Amazon RDS for MySQL と MariaDB のモニタリングとアラートのツールとベストプラクティス

AWS 規範ガイダンス

AWS 規範ガイダンス: Amazon RDS for MySQL と MariaDB のモニタリングとアラートのツールとベストプラクティス

Table of Contents

MySQL および MariaDB 用 Amazon RDS 用のモニタリングおよびアラートツールとベストプラクティス

イゴール・オブラドビッチ、アマゾンウェブサービス (AWS)

2023 年 6 月(ドキュメント履歴)

データベース監視は、データベースの可用性、パフォーマンス、および機能を測定、追跡、評価するプロセスです。監視および警告ソリューションにより、組織はデータベースサービス、ひいては関連するアプリケーションとワークロードの安全性、高性能、耐障害性、効率性を確保できます。AWS では、ワークロードのログ、メトリクス、イベント、トレースを収集して分析し、ワークロードの状態を把握し、時間の経過に伴う運用から洞察を得ることができます。

リソースを監視して、期待どおりに機能していることを確認し、顧客に影響が及ぶ前に問題を検出して修正できます。監視しているメトリクス、ログ、イベント、トレースを使用して、しきい値を超えたときにアラームを発生させる必要があります。

このガイドでは、Amazon リレーショナルデータベースサービス (Amazon RDS) データベースのデータベースオブザーバビリティとモニタリングツール、およびベストプラクティスについて説明します。このガイドでは MySQL と MariaDB データベースに焦点を当てていますが、ほとんどの情報は他の Amazon RDS データベースエンジンにも当てはまります。

このガイドは、ソリューションアーキテクト、データベースアーキテクト、データベースアーキテクト、データベース管理者、上級者を対象としていますDevOpsAWS クラウドで実行されているデータベースワークロードのモニタリングおよびオブザーバビリティソリューションの設計、実装、管理に従事するエンジニアやその他のチームメンバー。

目次

- 次のステップとリソース

概要

モニタリングとアラートは、 AWS Well-Architected Framework の 4 つの柱に含まれています。

- 運用上の優秀性の柱では、Amazon Relational Database Service (Amazon RDS) などのテレメトリと monitoring. AWS services を含めるようにワークロードを設計すると、ワークロードの内部状態 (メトリクス、ログ、イベント、トレースなど) を把握するために必要な情報が得られます。Amazon RDS データベースを運用するときは、データベースインスタンスの状態を把握し、運用イベントを検出し、計画されたイベントと計画外のイベントの両方に対応できるようにする必要があります。AWS には、組織やビジネスの成果がいつリスクにさらされているか、またはリスクにさらされている可能性があるかを判断するのに役立つモニタリングツールが用意されているため、適切なタイミングで適切なアクションを実行できます。
- パフォーマンス効率の柱では、パフォーマンス関連のメトリクスをリアルタイムで収集、集約、処理することで、Amazon RDS DB インスタンスなどの リソースのパフォーマンスをモニタリングする必要があることを規定しています。最適化されていない SQL クエリや不適切な設定パラメータなど、パフォーマンスの低下を特定し、その要因を修正できます。測定値が想定範囲外の場合、アラームを自動的に生成できます。アラームは、通知だけでなく、検出されたイベントに応じて自動アクションを開始するためにも使用することをお勧めします。収集したメトリクスを事前定義されたしきい値と照らし合わせて評価したり、機械学習アルゴリズムを使用して異常な動作を特定したりできます。例えば、CPU 使用率が増加する傾向を検出するには、一定期間にわたって`cpuUtilization.total`メトリクスを収集して分析できます。CPU 使用率がハード制限に達する前に、その異常を事前に警告することで、顧客に影響を与える前に問題を修正できます。
- 信頼性の柱は、モニタリングとアラートを重要として定義し、可用性の要件を満たしていることを確認します。モニタリングソリューションは、障害を効果的に検出できる必要があります。問題や障害が検出された場合、その主な目的はそれらの問題を警告することです。継続的なオブザーバビリティとモニタリングのプラクティスを実装することは、クラウド内の回復力のあるアーキテクチャにとって不可欠です。ワークロードを改善するには、ワークロードを測定し、ワークロードの状態と正常性を理解できる必要があります。障害、水平方向のスケーラビリティ、キャパシティープロビジョニングから自動復旧するための設計原則は、正確なモニタリングとアラートサービスによって異なります。
- セキュリティの柱では、予期しない設定変更や不要な設定変更、および予期しない動作の検出と防止について説明します。MariaDB 監査プラグインを使用して Amazon RDS for MySQL および MariaDB DB インスタンスを設定し、データベースに対して実行されるユーザーログインや特定のオペレーションなどのデータベースアクティビティを記録できます。 MariaDB プラグインは、データベースアクティビティのレコードをログファイルに保存します。ログファイルは、モニタリングツールやアラートツールに統合してインポートできます。ログファイルは、データベース内の

予期しない動作や疑わしい動作についてリアルタイムで分析されます。このような予期しない動作や疑わしい動作は、Amazon RDS DB インスタンスが侵害され、ビジネスに潜在的なリスクが及ぶことを示している可能性があります。モニタリングツールがそのようなイベントを検出すると、アラームがアクティブになり、セキュリティインシデントへの応答が開始されます。これにより、疑わしいアクティビティや悪意のあるアクティビティに対処できます。

ターゲットを絞ったビジネス成果

モニタリングとアラートのメカニズムにベストプラクティスを実装することで、アプリケーションとワークロード向けに、高パフォーマンス、耐障害性、効率、安全性、コスト最適化のインフラストラクチャを確保できます。メトリクス、イベント、トレース、ログをリアルタイムで収集、保存、視覚化するオブザーバビリティツールを使用して、データベースの状態とパフォーマンスの全体像を監視および分析できるため、関連する IT サービスの低下や中断を防ぐことができます。計画外のパフォーマンス低下やサービスの中断が依然として発生する場合は、モニタリングおよびアラートツールが問題、エスカレーション、対応、迅速な調査と解決をタイムリーに検出するのに役立ちます。クラウドデータベースワークロード向けの包括的なモニタリングおよびアラートソリューションは、以下のビジネス成果を達成するのに役立ちます。

- カスタマーエクスペリエンスを向上させます。信頼性の高いサービスにより、顧客のエクスペリエンスが向上します。データベースは、多くの場合、ウェブおよびモバイルアプリケーション、メディアストリーミング、支払い、 business-to-business (B2B) APIs、統合サービスなどのデジタルサービスの主要コンポーネントです。データベースでアラートをモニタリングして設定し、問題を迅速に検出し、効率的に調査し、ダウンタイムやその他の中断を最小限に抑えるためにできるだけ早く修正できる場合は、お客様のデジタルサービスの可用性、セキュリティ、パフォーマンスを向上させることができます。
- 顧客の信頼を構築する。 パフォーマンスを向上させ、ユーザーエクスペリエンスをスムーズにすることで、顧客の信頼を獲得できるため、プラットフォームのビジネスが増える可能性があります。例えば、信頼性の高いオンラインサービスを提供する支払い処理サービスプロバイダーは、顧客の信頼度とロイヤルティが高いことを期待できます。その結果、顧客が増え、保持率が向上し、請求可能なトランザクションが増加し、収益が増える新しい革新的なサービスが増えます。
- 財務上の損失を避けます。 データベースインフラストラクチャの予期しないダウンタイムは、アプリケーションを使用して顧客が実行するビジネストランザクションに影響を与える可能性があります。場合によっては、これにより多額の経済的損失が発生します。サービスレベルアグリーメント (SLAsに違反すると、顧客の信頼が失われ、その結果、収益が失われる可能性があります。また、高額なトライアルの法的基盤にもなり、顧客が責任と保証の契約に基づいて報酬を要求する可能性があります。ソフトウェア会社である Atlassian Corporation の調査によると、サービス停

止の平均コストは、ビジネスのタイプと規模に応じて、1 時間あたり 140,000 USD から 540,000 USD の範囲内です。安定したデータベース環境は、長期にわたる停止やビジネス損失を防ぐ上で重要です。

- 値を展開します。モニタリングとアラートのメカニズムは、可用性、耐障害性、信頼性、パフォーマンス、費用対効果、安全なデジタルサービスの設計、開発、運用に役立ちますが、最初のステップにすぎません。組織が時間の経過とともに拡張し、既存のクラウドワークロードを強化し、新しいサービスを導入することが必要になります。新しいサービスは、顧客にさらなる価値を提供し、ビジネスにより多くの収益をもたらすため、ビジネスの増加にフライホイール効果をもたらします。
- デベロッパーの生産性を向上させます。 生産的で効率的で、開発タスクで問題やボトルネックが発生しない開発者は、高品質の製品を短時間で提供できます。ただし、ソフトウェアエンジニアリングや IT 運用には複雑な課題がよくあるため、ワークロードとそのアーキテクチャの規模によってはこの複雑さが増します。分散アプリケーションのパフォーマンスと一貫性を分析するには、デベロッパーには相関メトリクスとトレースを提供できるツールが必要です。これらは、欠陥コードアーティファクトとインフラストラクチャコンポーネントをできるだけ早く特定し、エンドユーザーへの影響を判断するのに役立ちます。適切なモニタリングおよびアラートツールスイートは、デベロッパーがコーディングとテストをより適切かつ迅速に行えるようになります。
- 運用効率と効率を向上させます。 クラウドワークロードを大規模に運用する場合、パフォーマンスの向上がごくわずかであっても、数百万ドルの節約につながります。データベースをモニタリングし、メトリクス、イベント、ログ、トレースを分析することで、将来の容量ニーズを理解して予測し、AWS クラウドで利用できるコスト削減を活用できます。Amazon RDS ワークロードと運用の健全性を理解することは、イベントへの対応、問題の修正、改善の計画に役立ちます。

一般的なベストプラクティス

以下のベストプラクティスは、Amazon RDS ワークロードの状態を十分に把握し、運用イベントやモニタリングデータに応じて適切なアクションを実行するのに役立ちます。

- KPI を特定してください。望ましいビジネス成果に基づいて主要業績評価指標 (KPI) を特定します。KPI を評価してワークロードの成功を判断します。たとえば、コアビジネスが電子商取引である場合、望ましいビジネス成果の1つは、顧客が電子ショップを年中無休で利用できることです。そのビジネス上の成果を達成するには、eショップアプリケーションが使用するバックエンドの Amazon RDS データベースの可用性 KPI を定義し、ベースライン KPI を週単位で 99.99% に設定します。実際の可用性KPIをベースライン値と照らし合わせて評価すると、希望するデータベース可用性の 99.99% を満たし、24時間365日のサービスを提供することでビジネス上の成果を達成しているかどうかを判断できます。
- ワークロードメトリクスを定義します。Amazon RDS ワークロードの量と質を測定するワークロードメトリックスを定義します。メトリクスを評価して、ワークロードが望ましい結果を達成しているかどうかを判断し、ワークロードの状態を把握します。たとえば、Amazon RDS DB インスタンスの可用性 KPI を評価するには、DB インスタンスの稼働時間やダウンタイムなどのメトリックスを測定する必要があります。次に、これらのメトリックを使用して、次のようにアベイラビリティKPIを計算できます。

  ```
  availability = uptime / (uptime + downtime)
  ```

  メトリックは、時系列のデータポイントのセットを表します。指標にはディメンションを含めることもでき、分類や分析に役立ちます。
- ワークロードメトリクスを収集して分析します。Amazon RDS は、設定に応じてさまざまなメトリックスとログを生成します。これらの中には、DB インスタンスのイベント、カウンター、または次のような統計を表すものがあります。`db.Cache.innoDB_buffer_pool_hits`。その他のメトリックは、次のようなオペレーティングシステムから取得されます。`memory.Total`これは、ホストの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの合計メモリ量を測定します。監視ツールは、収集した指標を定期的かつ積極的に分析して傾向を特定し、適切な対応が必要かどうかを判断する必要があります。
- ワークロードメトリクスのベースラインを確立します。指標のベースラインを設定して、期待値を定義し、良い閾値と悪いしきい値を特定します。たとえば、次のようなベースラインを定義できます。`ReadIOPS`通常のデータベース操作では最大1,000になります。その後、このベースラインを比較したり、過剰使用率を特定したりできます。読み取りIOPSが2,000〜3,000の範囲にあること

が新しい指標で一貫して示されていれば、調査や介入、改善のきっかけとなる可能性のある偏差を特定したことになります。

- ワークロードの結果が危険にさらされている場合はアラートを出します。ビジネス上の成果が危険にさらされていると判断したら、警告を発します。そうすれば、顧客に影響が及ぶ前に問題に積極的に対処することも、インシデントの影響をタイムリーに軽減することもできます。
- ワークロードに予想されるアクティビティパターンを特定してください。メトリクスのベースラインに基づいて、ワークロードアクティビティのパターンを確立して予期しない動作を特定し、必要に応じて適切なアクションを実行してください。AWS提供する監視ツール統計アルゴリズムと機械学習アルゴリズムを適用して指標を分析し、異常を検出します。
- ワークロードの異常が検出されたらアラートを出します。Amazon RDS ワークロードの操作に異常が検出されたら、必要に応じて適切なアクションで対応できるようにアラートを発生させます。
- KPI と指標を見直し、改訂します。Amazon RDS データベースが定義済みの要件を満たしていることを確認し、ビジネス目標を達成するために改善の余地がある分野を特定します。測定した指標と評価した KPI の有効性を検証し、必要に応じて修正します。たとえば、データベース同時接続の最適な数の KPI を設定し、接続の試行と失敗に関するメトリクス、および作成され実行中のユーザースレッドを監視するとします。KPI ベースラインで定義されている接続数よりも多くのデータベース接続がある可能性があります。現在のメトリクスを分析することで結果を検出することはできますが、根本原因を特定できない場合があります。その場合は、メトリクスを修正し、テーブルロックのカウンターなどの監視手段を追加する必要があります。新しいメトリックは、データベース接続数の増加の原因が予期しないテーブルロックであるかどうかを判断するのに役立ちます。

モニタリングツール

オブザーバビリティ、モニタリング、アラートの各ツールを使用して、次の操作を行うことをお勧めします。

- Amazon RDS 環境のパフォーマンスに関するインサイトを取得する
- 予期しない動作や疑わしい動作を検出する
- 容量を計画し、Amazon RDS インスタンスの割り当てについて知識に基づいた意思決定を行う
- メトリクスとログを分析して潜在的な問題を事前に予測する
- ユーザーが影響を受ける前に問題をトラブルシューティングして解決するために、しきい値を超えたときにアラートを生成する

AWS が提供するクラウドネイティブのオブザーバビリティとモニタリングツールとサービス、無料のオープンソースソフトウェアソリューション、Amazon RDS DB インスタンスをモニタリングするための商用サードパーティーソリューションなど、さまざまなオプションとソリューションから選択できます。これらのツールの一部については、以下のセクションで説明します。

ニーズに最適なツールを判断するには、各ツールの特徴と機能を組織の要件と比較します。また、デプロイのしやすさ、設定と統合、ソフトウェアの更新とメンテナンス、デプロイの方法 (ハードウェアやサーバーレスなど) 、ライセンス、価格、および組織に固有のその他の要素についてツールを評価することをお勧めします。

セクション

Amazon RDS に含まれるツール

Amazon Relational Database Service (Amazon RDS) は、AWS クラウドのマネージドデータベースサービスです。Amazon RDS はマネージドサービスであるため、データベースバックアップ、オペレーティングシステム (OS) とデータベースソフトウェアのインストール、OS とソフトウェアのパッチ適用、高可用性セットアップ、ハードウェアライフサイクル、データセンターオペレーションなど、ほとんどの管理タスクから解放されます。 AWS また、 には、Amazon RDS DB インスタンスの完全なオブザーバビリティソリューションを構築できる包括的なツールセットも用意されています。

一部のモニタリングツールは、Amazon RDS サービスに含まれ、事前設定され、自動的に有効になります。新しい Amazon RDS インスタンスを起動するとすぐに、次の 2 つの自動ツールを使用できます。

- Amazon RDS インスタンスのステータスは、DB インスタンスの現在のヘルスに関する詳細を提供します。例えば、ステータスコードには、利用可能 、停止 、 の作成、バックアップ 、失敗 が含まれます。Amazon RDS コンソール、 AWS Command Line Interface （ AWS CLI ）、または Amazon RDS API を使用して、インスタンスのステータスを表示できます。詳細については、Amazon RDS ドキュメントの「Amazon RDS DB インスタンスのステータスの表示」を参照してください。
- Amazon RDS レコメンデーションは、DB インスタンス、リードレプリカ、DB パラメータグループに関する自動レコメンデーションを提供します。これらのレコメンデーションは、DB インスタンスの使用状況、パフォーマンスデータ、および設定を分析することで提供され、ガイダンスとして提供されます。例えば、エンジンバージョンの古いレコメンデーションでは、DB インスタンスがデータベースソフトウェアの最新バージョンを実行していないこと、および最新のセキュリティ修正やその他の改善点を活用できるように DB インスタンスをアップグレードする必要があることを提案しています。詳細については、Amazon RDS ドキュメントの「Amazon RDS レコメンデーションの表示」を参照してください。

CloudWatch 名前空間

Amazon RDS は、AWS で実行されるクラウドリソースとアプリケーションのモニタリングおよびアラートサービスである Amazon CloudWatch と統合されています。Amazon RDS は、DB インスタンスのオペレーション、使用率、パフォーマンス、ヘルスに関するメトリクス、ログファイル、トレース、イベントを自動的に収集し、長期保存、分析、アラート CloudWatch のために に送信します。

Amazon RDS for MySQL および Amazon RDS for MariaDB は、追加料金なしでデフォルトのメトリクスセットを CloudWatch 1 分間隔で に自動的に発行します。これらのメトリクスは、メトリクスのコンテナである 2 つの名前空間 に収集されます。

- AWS/RDS 名前空間には、DB インスタンスレベルのメトリクスが含まれます。例としては、`BinLogDiskUsage` (バイナリログが占めるディスク容量)、 `CPUUtilization` (CPU 使用率)、 `DatabaseConnections` (DB インスタンスへのクライアントネットワーク接続の数) などがあります。
- AWS/Usage 名前空間にはアカウントレベルの使用状況メトリクスが含まれており、Amazon RDS サービスクォータ 内で運用されているかどうかを判断するために使用されます。例としては、 `DBInstances` (AWS アカウントまたはリージョンの DB インスタンスの数)、`DBSubnetGroups` (AWS アカウントまたはリージョンの DB サブネットグループの数)、`ManualSnapshots` (AWS アカウントまたはリージョンで手動で作成されたデータベーススナップショットの数) などがあります。

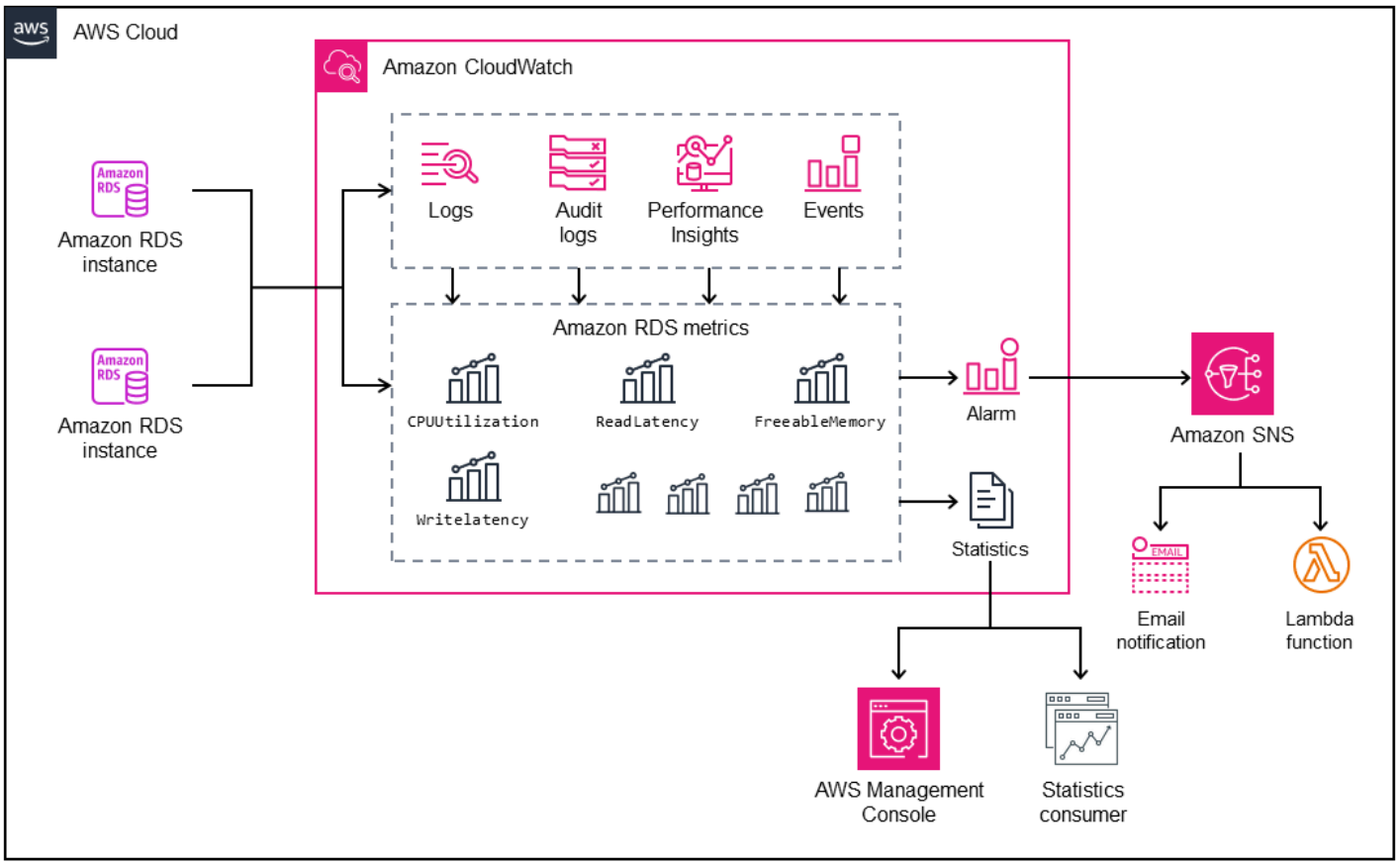
CloudWatch は、メトリクスデータを次のように保持します。

- 3 時間: 期間が 60 秒未満の高解像度カスタムメトリクスは 3 時間保持されます。3 時間後、データポイントは 1 分間のメトリクスに集約され、15 日間保持されます。
- 15 日間: 期間が 60 秒 (1 分) のデータポイントは 15 日間保持されます。15 日後、データポイントは 5 分間のメトリクスに集約され、63 日間保持されます。
- 63 日間: 300 秒 (5 分) のデータポイントは 63 日間保持されます。63 日後、データポイントは 1 時間のメトリクスに集約され、15 か月間保持されます。
- 15 か月: 3,600 秒 (1 時間) のデータポイントは 15 か月 (455 日) 利用できます。

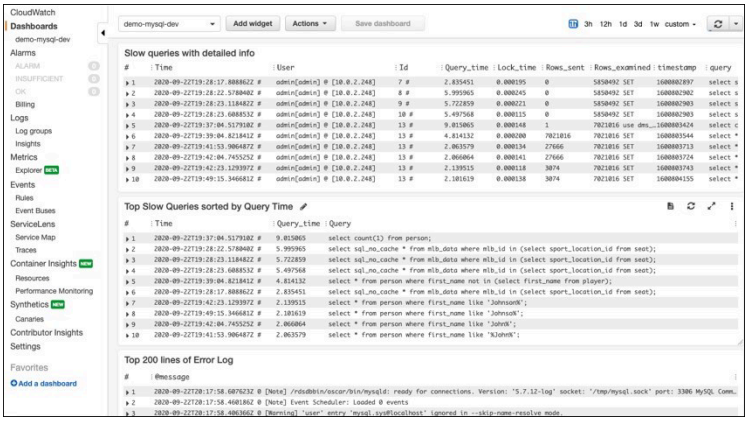
詳細については、 CloudWatch ドキュメントの「メトリクス」を参照してください。

CloudWatch アラームとダッシュボード

Amazon CloudWatch アラームを使用して、特定の Amazon RDS メトリクスを一定期間監視できます。例えば、 をモニタリングし`FreeStorageSpace`、メトリクスの値が設定したしきい値を超えた場合に 1 つ以上のアクションを実行できます。しきい値を 250 MB に設定し、空きストレージ領域が 200 MB (しきい値未満) の場合、アラームがアクティブになり、Amazon RDS DB インスタンスに追加のストレージを自動的にプロビジョニングするアクションをトリガーできます。アラームは、Amazon Simple Notification Service (Amazon SNS) を使用して DBA に通知 SMS を送信することもできます。次の図は、このプロセスを示したものです。

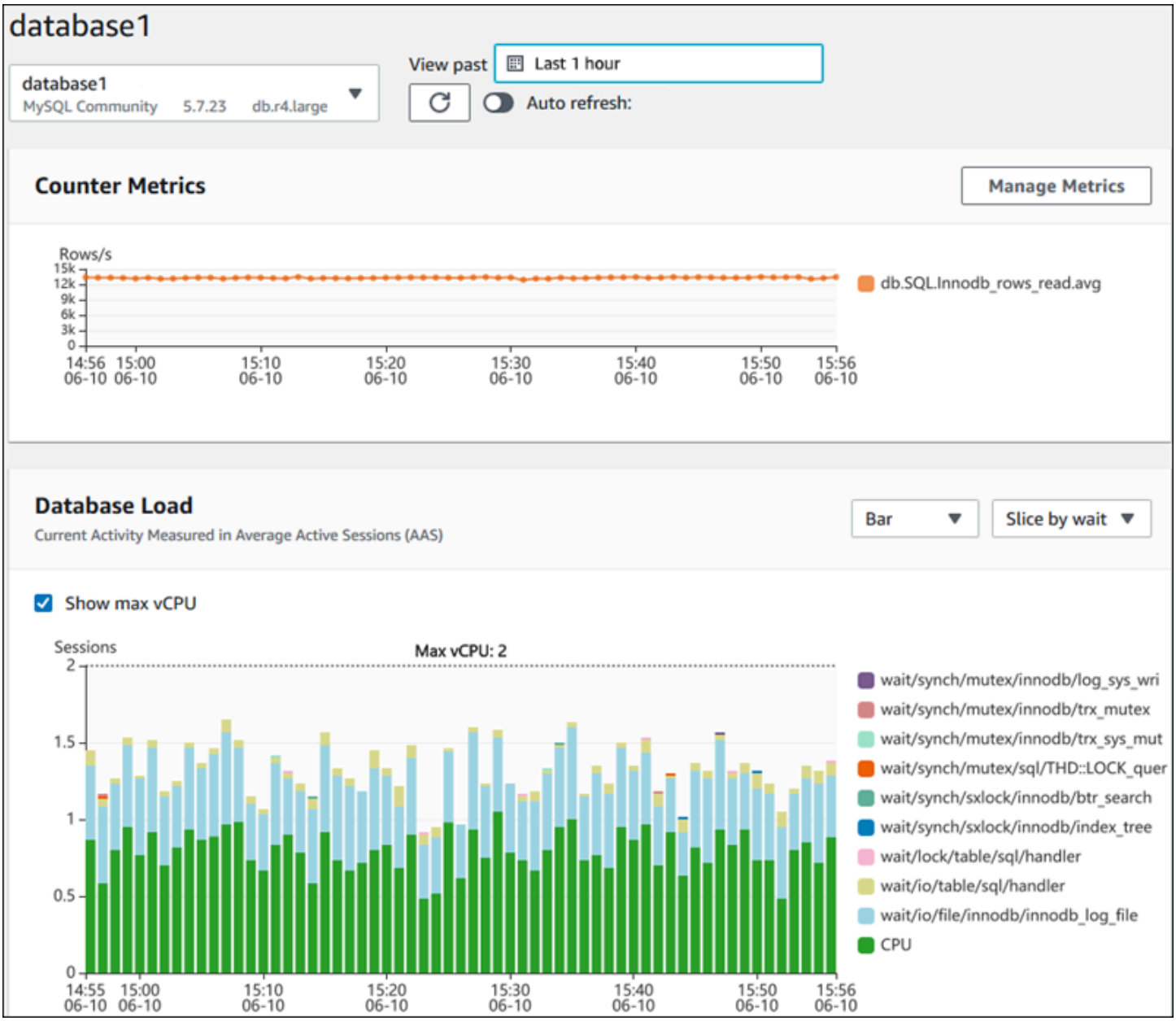


CloudWatch には、ダッシュボードも用意されています。ダッシュボードを使用して、メトリクスのカスタマイズされたビュー (グラフ) を作成、カスタマイズ、操作、保存できます。CloudWatch Logs Insights を使用して、スロークエリログとエラーログをモニタリングするためのダッシュボードを作成し、それらのログで特定のパターンが検出された場合にアラートを受信することもできます。次の画面は、ダッシュボードの例 CloudWatchを示しています。



「Amazon RDS Performance Insights」

Amazon RDS Performance Insights は、Amazon RDS のモニタリング機能を拡張するデータベースのパフォーマンス調整およびモニタリングツールです。DB インスタンスのロードを視覚化し、待機、SQL ステートメント、ホスト、またはユーザーでロードをフィルタリングすることで、データベースのパフォーマンスを分析するのに役立ちます。このツールは、ロック待機、高い CPU 使用率、I/O レイテンシーなど、DB インスタンスが持つ可能性のあるボトルネックのタイプを特定し、ボトルネックの原因となっている SQL ステートメントを特定するのに役立つ複数のメトリクスを 1 つのインタラクティブグラフに結合します。次の画面は、視覚化の例を示しています。



アカウント内の Amazon RDS DB インスタンスのメトリクスを収集するには、DB インスタンスの作成プロセス中に Performance Insights を有効にする必要があります。無料利用枠には、7 日間のパフォーマンスデータ履歴と 1 か月あたり 100 万件の API リクエストが含まれます。オプションで、より長い保持期間を購入できます。料金情報の詳細については、「Performance Insights の料金」を参照してください。

Performance Insights を使用して DB インスタンスをモニタリングする方法については、このガイドの後半にある DB インスタンスのモニタリングセクションを参照してください。

Performance Insights は、メトリクスを に自動的に発行します CloudWatch。Performance Insights ツールの使用に加えて、 CloudWatch が提供する追加機能を活用できます。Performance Insights メトリクスは、 CloudWatch コンソール、、 AWS CLIまたは CloudWatch API を使用して調べることができます。他のメトリクスと同様に、アラームを追加 CloudWatchすることもできます。例えば、DBAs への SMS 通知をトリガーしたり、DBLoadメトリクスが設定したしきい値を超えた場合に修正アクションを実行したりできます。Performance Insights メトリクスを既存の CloudWatch ダッシュボードに追加することもできます。

拡張モニタリング

拡張モニタリングは、Amazon RDS DB インスタンスが実行されている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キャプチャするツールです。これらのメトリクスは、CPU、メモリ、Amazon RDS および OS プロセス、ファイルシステム、ディスク I/O データなどに最大 1 秒の精度を提供します。これらのメトリクスには、Amazon RDS コンソール でアクセスして分析できます。Performance Insights と同様に、拡張モニタリングメトリクスは Amazon RDS から に配信され CloudWatch、分析用のメトリクスの長期保存、メトリクスフィルターの作成、 CloudWatch ダッシュボードへのグラフの表示、アラームの設定などの追加機能を利用できます。デフォルトでは、新しい Amazon RDS DB インスタンスを作成すると、拡張モニタリングは無効になります。この機能は、DB インスタンスを作成または変更するときに有効にできます。料金は、Amazon RDS から CloudWatch ログに転送されるデータの量とストレージレートに基づいています。詳細度と拡張モニタリングが有効になっている DB インスタンスの数に応じて、モニタリングデータの一部を CloudWatch Logs の無料利用枠に含めることができます。料金の詳細については、「Amazon CloudWatch 料金表」を参照してください。ツールの詳細については、「Amazon RDS ドキュメント」と「拡張モニタリングに関するよくある質問」を参照してください。

追加 AWS サービス

AWS は、Amazon RDS および とも統合されるいくつかのサポートサービスを提供し CloudWatch、データベースのオブザーバビリティをさらに強化します。これには、Amazon EventBridge、Amazon CloudWatch Logs、および が含まれます AWS CloudTrail。

- Amazon EventBridge は、Amazon RDS DB インスタンスを含むアプリケーションと AWS リソースからイベントを受信、フィルタリング、変換、ルーティング、配信できるサーバーレスイベントバスです。Amazon RDS イベントは、Amazon RDS 環境の変更を示します。例えば、DB インスタンスのステータスが Available から Stopped に変更されると、Amazon RDS はイベント を生成しますRDS-EVENT-0087 / The DB instance has been stopped。Amazon RDS は、イベントと CloudWatch にほぼリアルタイムでイベントを配信 EventBridge します。 EventBridge および CloudWatch イベントを使用して、特定の Amazon RDS イベントに関するアラートを送信するルールを定義し、イベントがルールに一致するときに実行されるアクションを自動化できます。修正アクションを実行できる AWS Lambda 関数や、DBAs や DevOps エンジニアにイベントを通知する E メールや SMS を送信できる Amazon SNS トピックなど、イベントに応じてさまざまなターゲットを使用できます。
- Amazon CloudWatch Logs は、Amazon RDS for MySQL、MariaDB DB インスタンス、 など、すべてのアプリケーション、システム、サービスからのログファイルのストレージを一元化する AWS サービスです AWS CloudTrail。DB インスタンスでこの機能を有効にすると、Amazon RDS は次のログを自動的に CloudWatch Logs に発行します。
  - エラーログ
  - スロークエリログ
  - 全般ログ
  - [監査ログ]

  CloudWatch Logs Insights を使用して、ログデータをクエリおよび分析できます。この機能には、定義したパターンに一致するログイベントの検索に役立つ専用のクエリ言語が含まれています。例えば、MySQL DB インスタンスのテーブルの破損を追跡するには、エラーログファイルのパターンをモニタリングします: "ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"。フィルタリングされたログデータはメトリクスに変換できます CloudWatch 。その後、メトリクスを使用して、グラフまたは表形式のデータを含むダッシュボードを作成したり、定義されたしきい値を超えた場合にアラームを設定したりできます。これは、予期しない動作や疑わしい動作が検出された場合に、自動的にモニタリング、アラートの送信、および是正措置を講じることができるため、監査ログを使用する場

合に特に便利です。 AWS マネジメントコンソール、、Amazon RDS API AWS CLI、または AWS SDK for CloudWatch Logs を使用して、データベースログにアクセスして管理できます。

- AWS CloudTrail は、AWS アカウントのユーザーおよび API アクティビティを口グに記録し、継続的にモニタリングします。Amazon RDS for MySQL または MariaDB DB インスタンスの監査、セキュリティモニタリング、運用上のトラブルシューティングに役立ちます。 CloudTrail は Amazon RDS と統合されています。すべてのアクションは口グに記録でき、Amazon RDS のユーザー、ロール、または AWS サービスによって実行されたアクションの記録 CloudTrail を提供します。例えば、ユーザーが新しい Amazon RDS DB インスタンスを作成すると、イベントが検出され、口グにはリクエストされたアクション (`"eventName": "CreateDBInstance"`) 、アクションの日時 ()`"requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}`、リクエストパラメータ (`"eventTime": "2022-07-30T22:14:06Z"`) などの情報が含まれます。によってログに記録されるイベントには、Amazon RDS コンソールからの呼び出しと、Amazon RDS API を使用するコードからの呼び出しの両方 CloudTrail が含まれます。

サードパーティーのモニタリングツール

シナリオによっては、Amazon RDS 用に AWS が提供するクラウドネイティブのオブザーバビリティおよびモニタリングツールの完全なスイートに加えて、他のソフトウェアベンダーのモニタリングツールを使用することもできます。このようなシナリオには、オンプレミスデータセンターで多数のデータベースが実行されているハイブリッドデプロイと、 で別のデータベースセットが実行されている場合がありますAWS クラウド。企業のオブザーバビリティソリューションを既に確立している場合は、既存のツールを引き続き使用し、AWS クラウドデプロイに拡張することをお勧めします。サードパーティーのモニタリングソリューションを設定する際の課題は、多くの場合、Amazon RDS がクラウドマネージドサービスとして課す保護にあります。例えば、データベースホストマシンへのアクセスが拒否されるため、DB インスタンスを実行するホストオペレーティングシステムにエージェントソフトウェアをインストールすることはできません。ただし、 CloudWatch およびその他の AWS クラウド サービス上に構築することで、多くのサードパーティーのモニタリングソリューションを Amazon RDS と統合できます。例えば、Amazon RDS メトリクス、ログ、イベント、トレースをエクスポートし、サードパーティーのモニタリングツールにインポートして、詳細な分析、可視化、アラートを行うことができます。これらのサードパーティーソリューションには、Prometheus、Grafana、Percona などがあります。

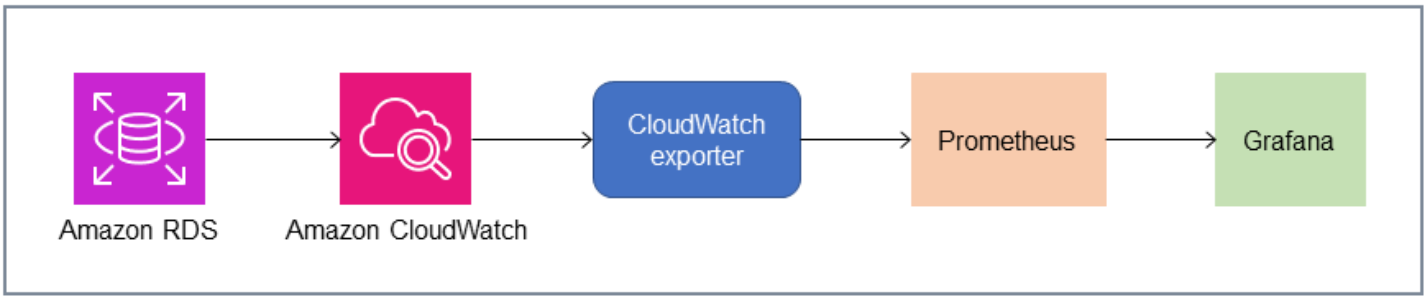
Prometheus と Grafana

Prometheus は、設定されたターゲットから特定の間隔でメトリクスを収集するオープンソースのモニタリングソリューションです。これは、あらゆるアプリケーションやサービスをモニタリングできる汎用モニタリングソリューションです。Amazon RDS DB インスタンスをモニタリングすると、は Amazon RDS からメトリクスを CloudWatch 収集します。次に、YACE Exporter や CloudWatch Exporter などのオープンソースエクスポーターを使用して、メトリクスを Prometheus サーバーにエクスポートします。

- YACE Exporter は、 CloudWatch API への 1 回のリクエストで複数のメトリクスを取得することで、データエクスポートタスクを最適化します。メトリクスが Prometheus サーバーに保存されると、サーバーはルール式を評価し、指定された条件が観測されたときにアラートを生成できます。
- CloudWatch Exporter は Prometheus によって公式に管理されています。 CloudWatch API を介して CloudWatch メトリクスを取得し、HTTP エンドポイントへの REST API リクエストを使用して、Prometheus と互換性のある形式で Prometheus サーバーに保存します。

エクスポーターを選択し、デプロイモデルを設計し、エクスポーターインスタンスを設定するときは、 CloudWatchと CloudWatch Logs のサービスおよび API クォータを検討してください。Prometheus サーバーへの CloudWatch メトリクスのエクスポートは CloudWatch API の上に実装されるためです。例えば、 CloudWatch Exporter の複数のインスタンスを 1 つの AWS アカウントおよびリージョンにデプロイして数百の Amazon RDS DB インスタンスをモニタリングすると、スロットリングエラー (ThrottlingException) とコード 400 エラーが発生する可能性があります。このような制限を克服するには、1 回のリクエストで最大 500 個の異なるメトリクスを収集するように最適化された YACE Exporter の使用を検討してください。さらに、多数の Amazon RDS DB インスタンスをデプロイするには、ワークロードを 1 つの に一元化し、各 のエクスポーターインスタンスの数を制限するのではなく、複数の AWS アカウント を使用することを検討する必要があります AWS アカウント。 AWS アカウント

アラートは Prometheus サーバーによって生成され、Alertmanager によって処理されます。このツールは、E メール、SMS、Slack などの正しい受信者へのアラートの重複排除、グループ化、ルーティング、または自動応答アクションの開始を処理します。Grafana と呼ばれる別のオープンソースツールでは、これらのメトリクスの視覚化が表示されます。Grafana は、高度なグラフ、動的ダッシュボード、アドホッククエリや動的ドリルダウンなどの分析機能など、豊富な視覚化ウィジェットを提供します。また、ログを検索および分析したり、メトリクスとログを継続的に評価したり、データがアラートルールに一致したときに通知を送信したりするためのアラート機能を含めたりすることもできます。



パーコナ

Percona Monitoring and Management (PMM) は、 MySQLMySQL および MariaDB 用の無料のオープンソースデータベースモニタリング、管理、オブザーバビリティソリューションです。 MariaDB PMM は、DB インスタンスとそのホストから数千のパフォーマンスメトリクスを収集します。ダッシュボード内のデータを視覚化するウェブ UI と、データベースヘルス評価の自動アドバイザーなどの追加機能を提供します。PMM を使用して Amazon RDS をモニタリングできます。ただし、PMM クライアント (エージェント) はホストにアクセスできないため、Amazon RDS DB インスタンスの基盤となるホストにはインストールされません。代わりに、このツールは Amazon RDS DB インスタンスに接続し、サーバー統計、INFORMATION_SCHEMA、sys スキーマ、パフォーマンススキーマをクエリし、 CloudWatch API を使用してメトリクス、ログ、イベント、トレースを取得します。PMM には AWS Identity and Access Management (IAM) ユーザーアクセスキー (IAM ロール) が必要で、モニタリングに使用できる Amazon RDS DB インスタンスを自動的に検出します。PMM ツールはデータベースモニタリング用にプロファイリングされ、Prometheus よりも多くのデータベース固有のメトリクスを収集します。PMM Query Analytics ダッシュボードを使用するには、クエリ分析エージェントが Amazon RDS にインストールされておらず、スロークエリログを読み取ることができないため、Performance Schema をクエリソースとして設定する必要があります。代わりに、MySQL および MariaDB DB インスタンスperformance_schemaから直接 をクエリしてメトリクスを取得します。 MariaDB PMM の目立つ機能の 1 つは、ツールがデータベース内で特定した問題について警告し、DBA に助言する機能です。 DBAs PMM には、一般的なセキュリティ脅威、パフォーマンスの低下、データ損失、データ破損を検出できる一連のチェックが用意されています。

これらのツールに加えて、Amazon RDS と統合できる市販のオブザーバビリティおよびモニタリングソリューションが市場にあります。例としては、Datadog Database Monitoring 、Dynatrace Amazon RDS Monitoring 、 AppDynamics Database Monitoring などがあります。

DB インスタンスモニタリング

あるDB インスタンスは Amazon RDS の基本的なビルディングブロックです。これは、クラウドで実行される独立したデータベース環境です。MySQL データベースと MariaDB データベースの場合、DB インスタンスはmysqldMySQL サーバーとも呼ばれるプログラムで、SQL パーサー、クエリオプティマイザー、スレッド/接続ハンドラー、システム変数、ステータス変数、1 つ以上のプラガブルストレージエンジンなどの複数のスレッドとコンポーネントが含まれています。各ストレージエンジンは、特定のユースケースをサポートするように設計されています。デフォルトかつ推奨されるストレージエンジンはInnoDBは、アトミシティ、コンシステンシー、アイソレーション、耐久性（ACID）モデルに準拠したトランザクション型の汎用リレーショナルデータベースエンジンです。InnoDB の機能インメモリ構造（バッファープール、変更バッファ、アダプティブハッシュインデックス、ログバッファ）およびオンディスク構造(テーブルスペース、テーブル、インデックス、UNDO ログ、REDO ログ、二重書き込みバッファファイル)。データベースが ACID モデルに厳密に準拠していることを確認するには、InnoDB ストレージエンジンは多数の機能を実装していますトランザクション、コミット、ロールバック、クラッシュリカバリ、行レベルのロック、マルチバージョン同時実行制御 (MVCC) などのデータを保護します。

DB インスタンスのこれらの内部コンポーネントはすべて連携して動作し、データの可用性、完全性、セキュリティを期待どおりの満足のいくパフォーマンスレベルに維持するのに役立ちます。ワークロードによっては、各コンポーネントや機能によって CPU、メモリ、ネットワーク、およびストレージサブシステムにリソースが必要となる場合があります。特定のリソースに対する需要の急増が、プロビジョニングされた容量またはそのリソースのソフトウェア制限（設定パラメータまたはソフトウェア設計によって課される）を超えると、DB インスタンスのパフォーマンスが低下したり、完全に利用できなくなったり壊れたりする可能性があります。そのため、これらの内部コンポーネントを測定して監視し、定義済みのベースライン値と比較し、監視値が期待値から逸脱した場合にアラートを生成することが重要です。

前に説明したように、別のものを使用できます道具MySQL インスタンスと MariaDB インスタンスを監視できます。Amazon RDS パフォーマンスインサイトとCloudWatchモニタリングとアラート用のツール。これらのツールは Amazon RDS と統合され、高解像度のメトリックスを収集し、最新のパフォーマンス情報をほぼリアルタイムで表示し、アラームを生成します。

お好みの監視ツールにかかわらず、次のことを推奨しますパフォーマンススキーマを有効にするMySQL インスタンスと MariaDB DB インスタンスにあります。ザ· パフォーマンススキーマはMySQL サーバー (DB インスタンス) の動作を低レベルで監視するためのオプション機能で、データベース全体のパフォーマンスへの影響を最小限に抑えるように設計されています。この機能は、を使用して管理できます。`performance_schema`パラメーター。このパラメータはオプションです

が、Amazon RDS Performance Insights が収集する高解像度 (1 秒) 単位のメトリクス、アクティブセッションメトリックス、待機イベント、その他の詳細で低レベルのモニタリング情報を収集するには、これを使用する必要があります。

セクション

- DB インスタンスのパフォーマンスインサイトメトリックス
- CloudWatchDB インスタンスのメトリックス
- パフォーマンスインサイトメトリクスの公開先CloudWatch

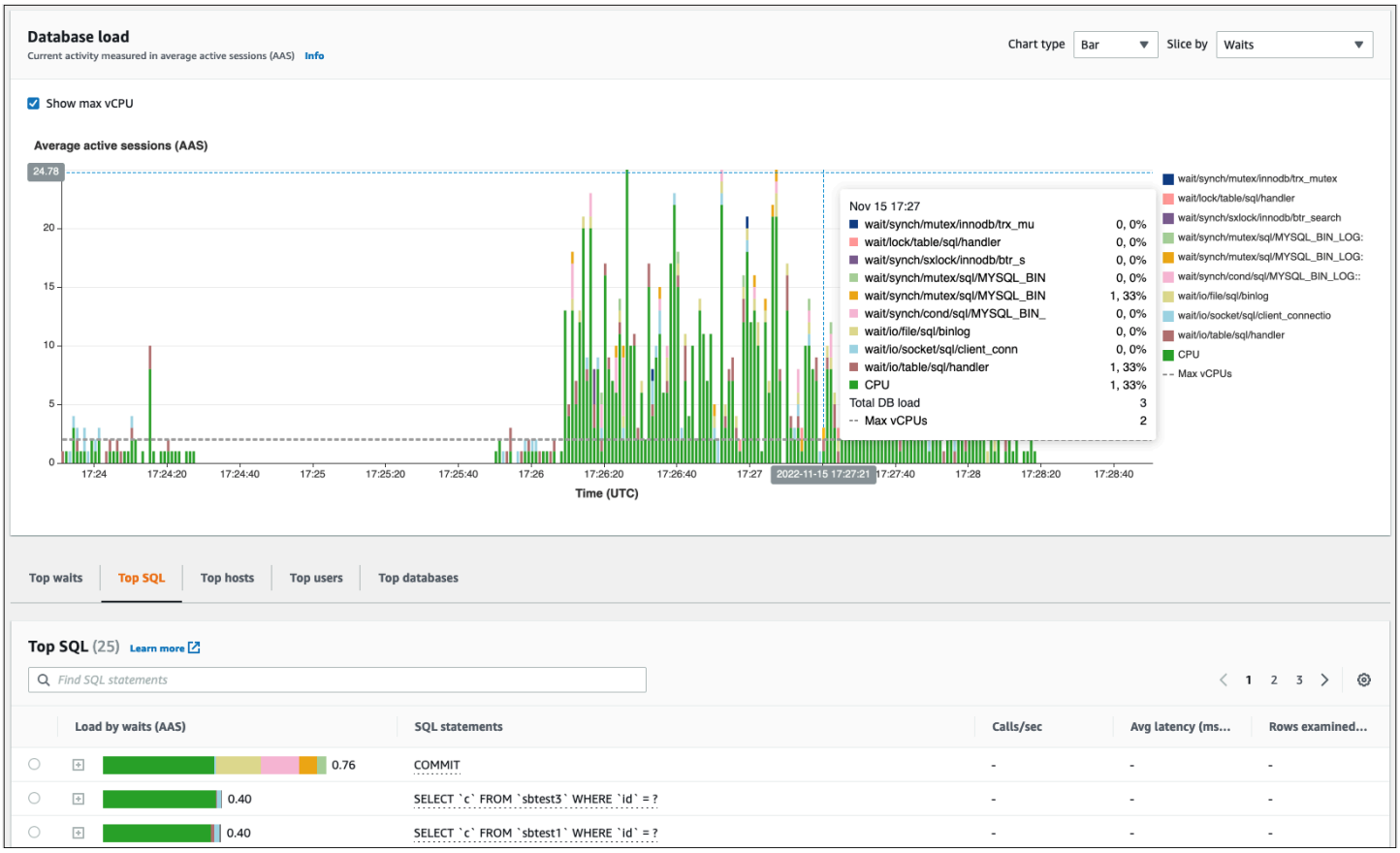
DB インスタンスのパフォーマンスインサイトメトリックス

パフォーマンスインサイトは、次のセクションで説明するように、さまざまなタイプのメトリックを監視します。

データベース負荷

データベースロード (DBLoad) は、データベース内のアクティビティレベルを測定するパフォーマンスインサイトの重要な指標です。1 秒ごとに収集され、自動的に Amazon に公開されます CloudWatch。平均アクティブセッション (AAS) における DB インスタンスのアクティビティを表します。AAS とは、SQL クエリを同時に実行しているセッションの数です。ザ・ DBLoadメトリックは、待機時間、SQL、ホスト、ユーザー、データベースの 5 つのディメンションのいずれかを使用して解釈できるという点で、他の時系列メトリックとは異なります。これらのディメンションはサブカテゴリですDBLoadメトリック。これらは次のように使用できますスライスバイデータベース負荷のさまざまな特性を表すカテゴリ。データベース負荷の計算方法の詳細については、を参照してください。データベースロードAmazon RDS のドキュメントに記載されています。

次の画面図は、パフォーマンスインサイトツールを示しています。



ディメンション

- 待機イベントは、データベースセッションが処理を続行するためにリソースまたは別の操作が完了するまで待機する条件です。次のような SQL ステートメントを実行する場合`SELECT * FROM big_table`また、このテーブルが割り当てられた InnoDB バッファープールよりもはるかに大きい場合は、セッションが待機する可能性が高くなります`wait/io/file/innodb/innodb_data_file`データファイルに対する物理的な I/O 操作によって発生する待機イベント。待機イベントは、パフォーマンスのボトルネックの可能性を示すため、データベース監視にとって重要な要素です。待機イベントは、セッション内で実行している SQL ステートメントが待機に最も時間を費やしているリソースと操作を示します。たとえば、`wait/synch/mutex/innodb/trx_sys_mutex`イベントは、データベースの使用率が高く、トランザクション数が多い場合に発生し、`wait/synch/mutex/innodb/buf_pool_mutex`イベントは、スレッドが InnoDB バッファープールのロックを取得してメモリ内のページにアクセスしたときに発生します。MySQL と MariaDB のすべての待機イベントの詳細については、を参照してください。待機イベント概要テーブルMySQL のドキュメントを参照してください。インストゥルメント名の解釈方法については、以下を参照してください。パフォーマンス・スキーマ・インストゥルメントの命名規則MySQL のドキュメントを参照してください。

- SQLデータベース全体の負荷に最も寄与している SQL 文が表示されます。ザ· 上部の寸法下にあるテーブルデータベースロードAmazon RDS パフォーマンスインサイトのグラフはインタラクティブです。SQL ステートメントに関連する待機イベントの詳細なリストを表示するには、のバーをクリックします。待機時間によるロード (AAS)コラム。リストから SQL ステートメントを選択すると、Performance Insightsは関連する待機イベントをデータベースロードのチャートとSQL ステートメントのテキストSQL テキストセクション。SQL 統計は、の右側に表示されます上部の寸法テーブル。
- ホスト接続しているクライアントのホスト名を表示します。このディメンションは、どのクライアントホストがほとんどの負荷をデータベースに送っているかを特定するのに役立ちます。
- ユーザデータベースにログインしているユーザーごとにデータベース負荷をグループ化します。
- [データベース]DB ロードを、クライアントが接続しているデータベースの名前でグループ化します。

カウンターメトリクス

カウンターメトリックスは累積的なメトリックスで、DB インスタンスの再起動時にのみ値が増加またはゼロにリセットされます。カウンタメトリックの値を以前の値に戻すことはできません。これらの指標は、単調に増加する単一のカウンターを表しています。

- ネイティブカウンターは Amazon RDS ではなくデータベースエンジンによって定義されるメトリックスです。例:
  - `SQL.Innodb_rows_inserted`InnoDB テーブルに挿入された行の数を表します。
  - `SQL.Select_scan`は、最初のテーブルのフルスキャンを完了したジョインの数を表します。
  - `Cache.Innodb_buffer_pool_reads`InnoDB エンジンがバッファープールから取得できず、ディスクから直接読み取る必要があった論理読み取りの数を表します。
  - `Cache.Innodb_buffer_pool_read_requests`論理的な読み取り要求の数を表します。

  すべてのネイティブメトリックの定義については、を参照してください。サーバーステータス変数MySQL のドキュメントを参照してください。
- 非ネイティブカウンターアマゾン RDS によって定義されています。これらのメトリックは、特定のクエリを使用して取得することも、計算に2つ以上のネイティブメトリックを使用して取得することもできます。非ネイティブのカウンターメトリックは、レイテンシー、比率、ヒット率を表すことができます。例:

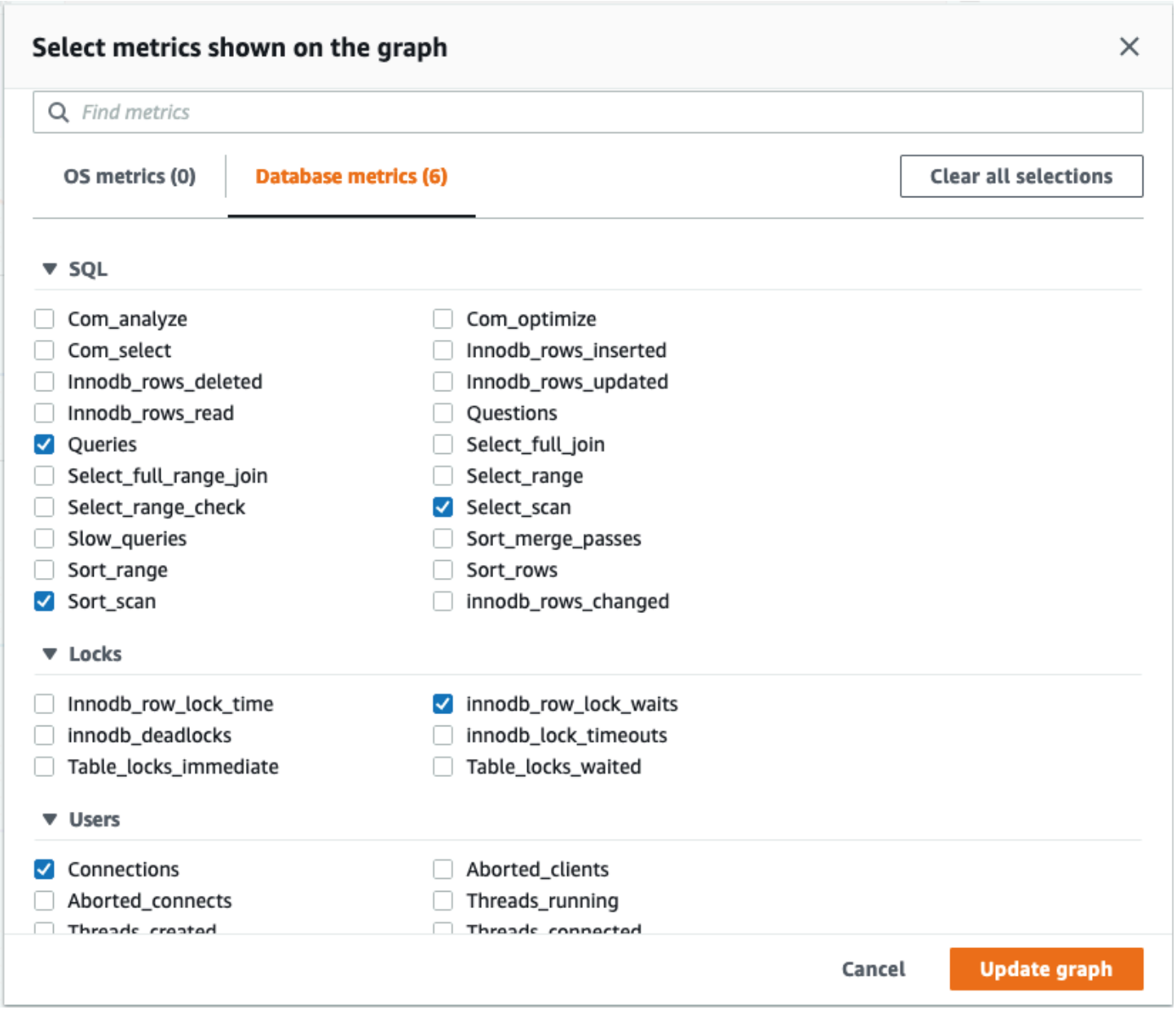
- Cache.innoDB_buffer_pool_hitsInnoDB がディスクを利用せずにバッファープールから取得できた読み取り操作の数を表します。ネイティブカウンターメトリックから次のように計算されます。

```
db.Cache.Innodb_buffer_pool_read_requests - db.Cache.Innodb_buffer_pool_reads
```

- IO.innoDB_datafile_writes_to_diskInnoDB データファイルのディスクへの書き込み操作の数を表します。キャプチャされるのはデータファイルに対する操作だけで、ロギングの二重書き込み操作ややり直し書き込み操作はキャプチャされません。次のように計算されます。

```
db.IO.Innodb_data_writes - db.IO.Innodb_log_writes - db.IO.Innodb_dblwr_writes
```

DB インスタンスのメトリクスをパフォーマンスインサイトダッシュボードで直接視覚化できます。選択指標の管理、選択してくださいデータベースメトリクスタブをクリックし、次の図に示すように、目的のメトリックを選択します。



を選択してくださいグラフを更新ボタンをクリックすると、次の図に示すように、選択したメトリックが表示されます。

SQL 統計

Performance Insightsは、クエリが実行されている1秒ごと、およびSQL呼び出しごとに、SQLクエリに関するパフォーマンス関連のメトリックを収集します。一般的に、パフォーマンスインサイトはSQL 統計情報ステートメントレベルとダイジェストレベルで ただし、MariaDB インスタンスとMySQL DB インスタンスの場合、統計はダイジェストレベルでのみ収集されます。

- ダイジェスト統計は、同じパターンであっても最終的にはリテラル値が異なるすべてのクエリを組み合わせた指標です。ダイジェストは、特定のリテラル値を変数に置き換えます。次に例を示します。

```
SELECT department_id, department_name FROM departments WHERE location_id = ?
```

- 統計を表す指標があります1 秒あたりダイジェストされた各 SQL ステートメントについて。たとえば、sql_tokenized.stats.count_star_per_sec1 秒あたりの呼び出し数 (つまり、SQL ステートメントが 1 秒間に何回実行されたか) を表します。

- パフォーマンスインサイトには、次のような指標も含まれています1 回の通話SQL ステートメントの統計情報。たとえば、`sql_tokenized.stats.sum_timer_wait_per_call`は、呼び出しごとの SQL ステートメントの平均レイテンシーをミリ秒単位で示します。

SQL 統計は、パフォーマンスインサイトダッシュボードのトップ SQLのタブ上部の寸法テーブル。

CloudWatchDB インスタンスのメトリックス

アマゾンCloudWatchAmazon RDS が自動的に公開するメトリックスも含まれています。にあるメトリックAWS/RDS名前空間はインスタンスレベルのメトリクスこれは、厳密な意味での DB インスタンスではなく、Amazon RDS (サービス) インスタンス (つまり、クラウドで実行されている独立したデータベース環境) を指しますmysqldプロセス。したがって、それらのほとんどはデフォルト指標厳密な定義では、OS メトリックのカテゴリに分類されます。例には以下が含まれます。`CPUUtilization`、`WriteIOPS`、`SwapUsage`、その他。それでも、MariaDB と MySQL に適用できる DB インスタンスメトリックスがいくつかあります。

- `BinLogDiskUsage`— バイナリログが占めるディスク容量の量。
- `DatabaseConnections`— DB インスタンスへのクライアントネットワーク接続の数。
- `ReplicaLag`— リードレプリカ DB インスタンスがソース DB インスタンスより遅れている時間。

パフォーマンスインサイトメトリクスの公開先CloudWatch

Amazon RDS パフォーマンスインサイトは DB インスタンスのメトリックスとディメンションのほとんどをモニタリングし、それらを DB インスタンスのパフォーマンスインサイトダッシュボードから利用できるようにします。AWS管理コンソール。このダッシュボードは、データベースのトラブルシューティングや根本原因の分析に適しています。ただし、パフォーマンス関連メトリックのアラームをパフォーマンスインサイト内に作成することはできません。Performance Insightsメトリッ

クに基づいてアラームを作成するには、それらのメトリックを次の場所に移動する必要があります CloudWatch。メトリクスを入力するCloudWatchまた、次のような高度な監視機能にもアクセスできますCloudWatch異常検知、メトリック演算、および統計また、メトリクスをPrometheusやGrafanaなどの外部モニタリングツールにエクスポートできます。

パフォーマンスインサイトメトリックスは自動的には公開されませんCloudWatch(以外DBロードメトリック)。パフォーマンスインサイトから DB インスタンスメトリックスをに公開するにはCloudWatch、使用できますパフォーマンスインサイト APIメトリクスを取得するには、CloudWatchAPIメトリクスを公開するにはCloudWatch。このプロセスを自動化するには、Lambda 関数を作成して Amazon でスケジュールできます。EventBridge指定した時間帯 (たとえば 2 分おき) に実行します。どのパフォーマンスインサイト指標を公開するかを指定できます。CloudWatch。Lambda 関数は、パフォーマンスインサイトが有効になっているすべての Amazon RDS インスタンスからそれらのメトリックスを取得し、そのメトリックスをに保存します。CloudWatch。このプロセスの詳細については、以下のブログ記事を参照してくださいパフォーマンスインサイトのカウンターメトリクスを配信するCloudWatch。

OS モニタリング

Amazon RDS for MySQL または MariaDB の DB インスタンスは Linux オペレーティングシステム上で実行され、基盤となるシステムリソース (CPU、メモリ、ネットワーク、ストレージ) を使用します。

```
MySQL [(none)]> SHOW variables LIKE 'version%';
+-------------------------+----------------------+
| Variable_name           | Value                |
+-------------------------+----------------------+
| version                 | 8.0.28               |
| version_comment         | Source distribution  |
| version_compile_machine | aarch64              |
| version_compile_os      | Linux                |
| version_compile_zlib    | 1.2.11               |
+-------------------------+----------------------+
5 rows in set (0.00 sec)
```

データベースと基盤となるオペレーティングシステムの全体的なパフォーマンスは、システムリソースの使用率に大きく依存します。たとえば、CPU はデータベースソフトウェアの命令を実行し、他のシステムリソースを管理するため、システムのパフォーマンスにとって重要なコンポーネントです。CPU が過剰に使用されている場合 (つまり、負荷が DB インスタンスにプロビジョニングされた量よりも多くの CPU パワーを必要とする場合)、この問題はデータベース、ひいてはアプリケーションのパフォーマンスと安定性に影響を与えます。

データベースエンジンはメモリの割り当てと解放を動的に行います。RAM に現在の作業を行うのに十分なメモリがない場合、システムはメモリページをディスク上のスワップメモリに書き込みます。ディスクは SSD NVMe テクノロジーをベースにしていても、メモリよりもはるかに低速であるため、メモリを過剰に割り当てるとパフォーマンスが低下します。メモリ使用率が高いと、追加のメモリをサポートするためにページファイルのサイズが大きくなるため、データベース応答の待ち時間が長くなります。メモリ割り当てが大きすぎて RAM とスワップメモリ領域の両方を使い果たしてしまうと、データベースサービスが使用できなくなり、ユーザに次のような エラーが表示されることがあります。`[ERROR] mysqld: Out of memory (Needed xyz bytes)`。

MySQL と MariaDB のデータベース管理システムは、ストレージ用のディスクで構成されるストレージサブシステムを利用します。オンディスク構造テーブル、インデックス、バイナリログ、やり直しログ、元に戻すログ、二重書き込みバッファファイルなど。したがって、データベースは、他の種類のソフトウェアとは対照的に、大量のディスクアクティビティを実行する必要があります。デー

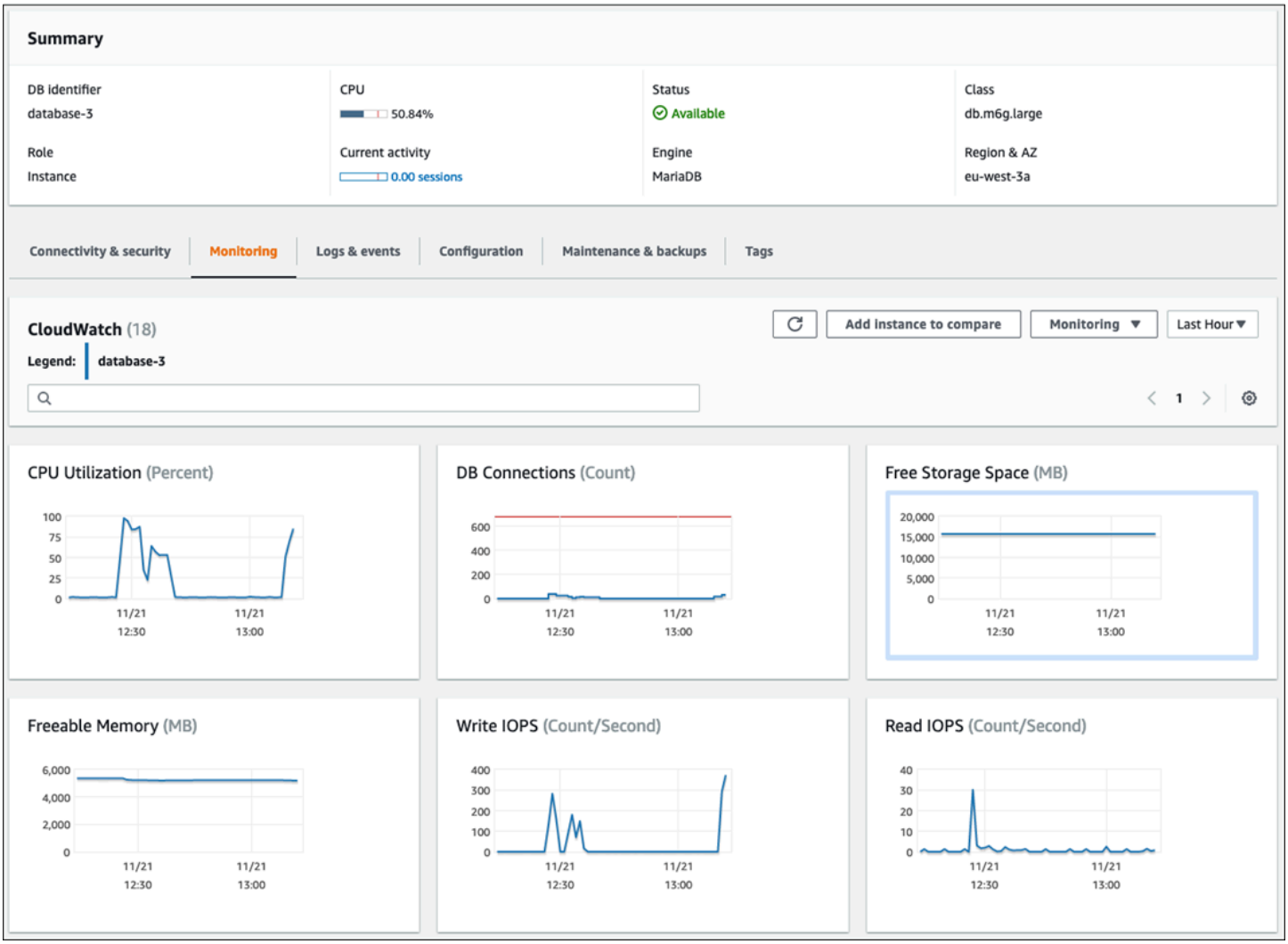
タベースを最適に運用するには、ディスク I/O の使用率とディスク容量の割り当てを監視および調整することが重要です。データベースがディスクがサポートする最大 IOPS またはスループットの制限に達すると、データベースのパフォーマンスが影響を受ける可能性があります。たとえば、インデックススキャンによってランダムアクセスが急増すると、1 秒間に大量の I/O 操作が発生し、最終的には基盤となるストレージの制限に達する可能性があります。フルテーブルスキャンでは IOPS の上限に達しないかもしれませんが、1 秒あたりのメガバイト単位の高スループットが発生する可能性があります。次のような エラーがあるため、ディスク容量の割り当てを監視してアラートを生成することが重要です。`OS error code 28: No space left on device`データベースが使用できなくなったり、破損したりする可能性があります。

Amazon RDS は、DB インスタンスが実行されているオペレーティングシステムのメトリックスをリアルタイムで提供します。Amazon RDS は 1 セットの OS メトリックスを自動的に公開しますCloudWatch。これらのメトリックスは Amazon RDS コンソールで表示および分析できます。CloudWatchダッシュボード、および選択したメトリックにアラームを設定できますCloudWatch。その例を以下に示します。

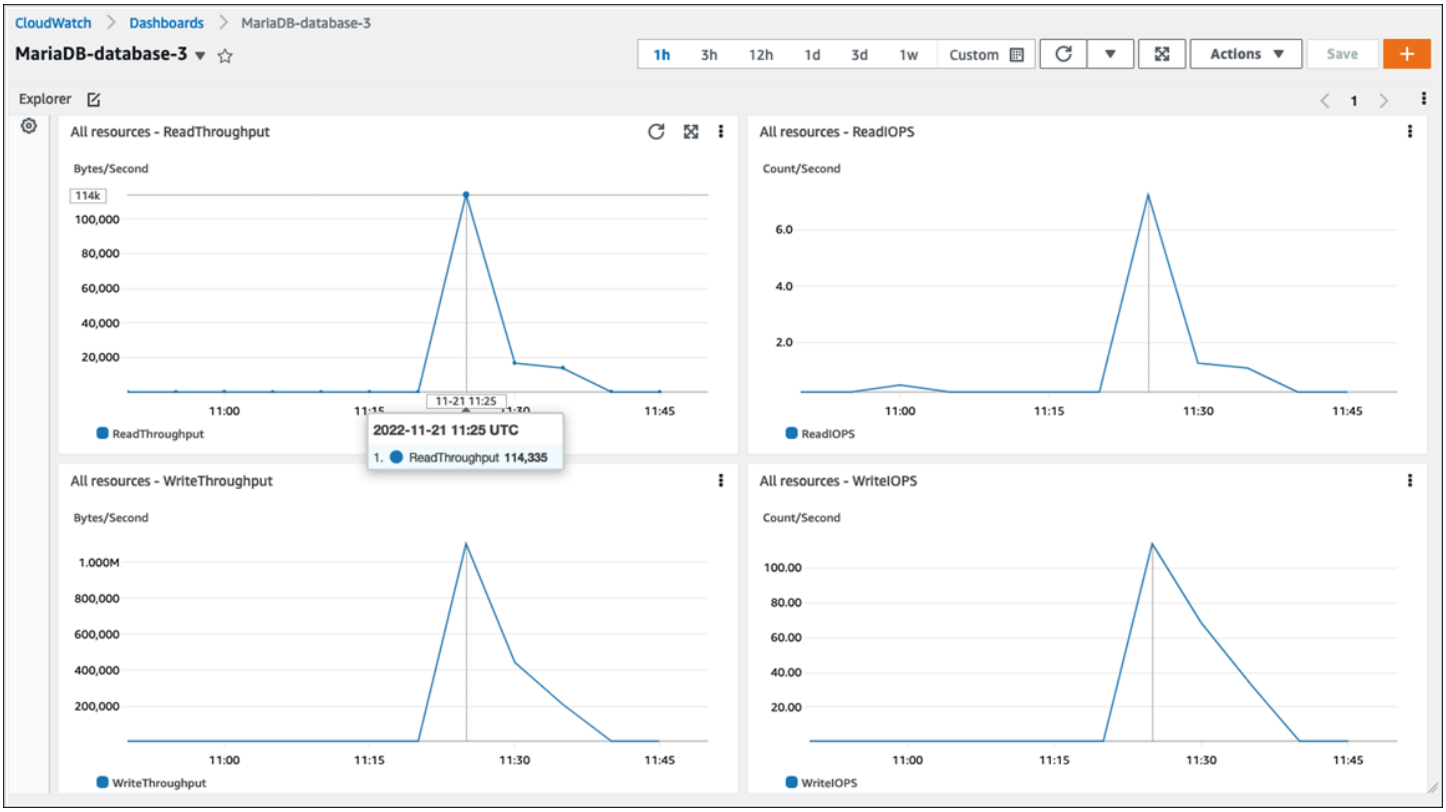
- `CPUUtilization`— CPU 使用率のパーセンテージ。
- `BinLogDiskUsage`— バイナリログが占めるディスク容量の量。
- `FreeableMemory`— 使用可能なランダム・アクセス・メモリの量。これは、の値を表しますMemAvailableのフィールド/proc/meminfo。
- `ReadIOPS`— 1 秒あたりのディスク読み取り I/O 操作の平均数。
- `WriteThroughput`— ローカルストレージの 1 秒あたりにディスクに書き込まれる平均バイト数。
- `NetworkTransmitThroughput`— DB ノード上の送信ネットワークトラフィック。データベーストラフィックと Amazon RDS トラフィックの両方をモニタリングとレプリケーションに使用します。

Amazon RDS が公開しているすべてのメトリックスの完全なリファレンスについては、以下を参照してください。CloudWatch、を参照してくださいアマゾンCloudWatchAmazon RDS のメトリックスAmazon RDS のドキュメントに記載されています。

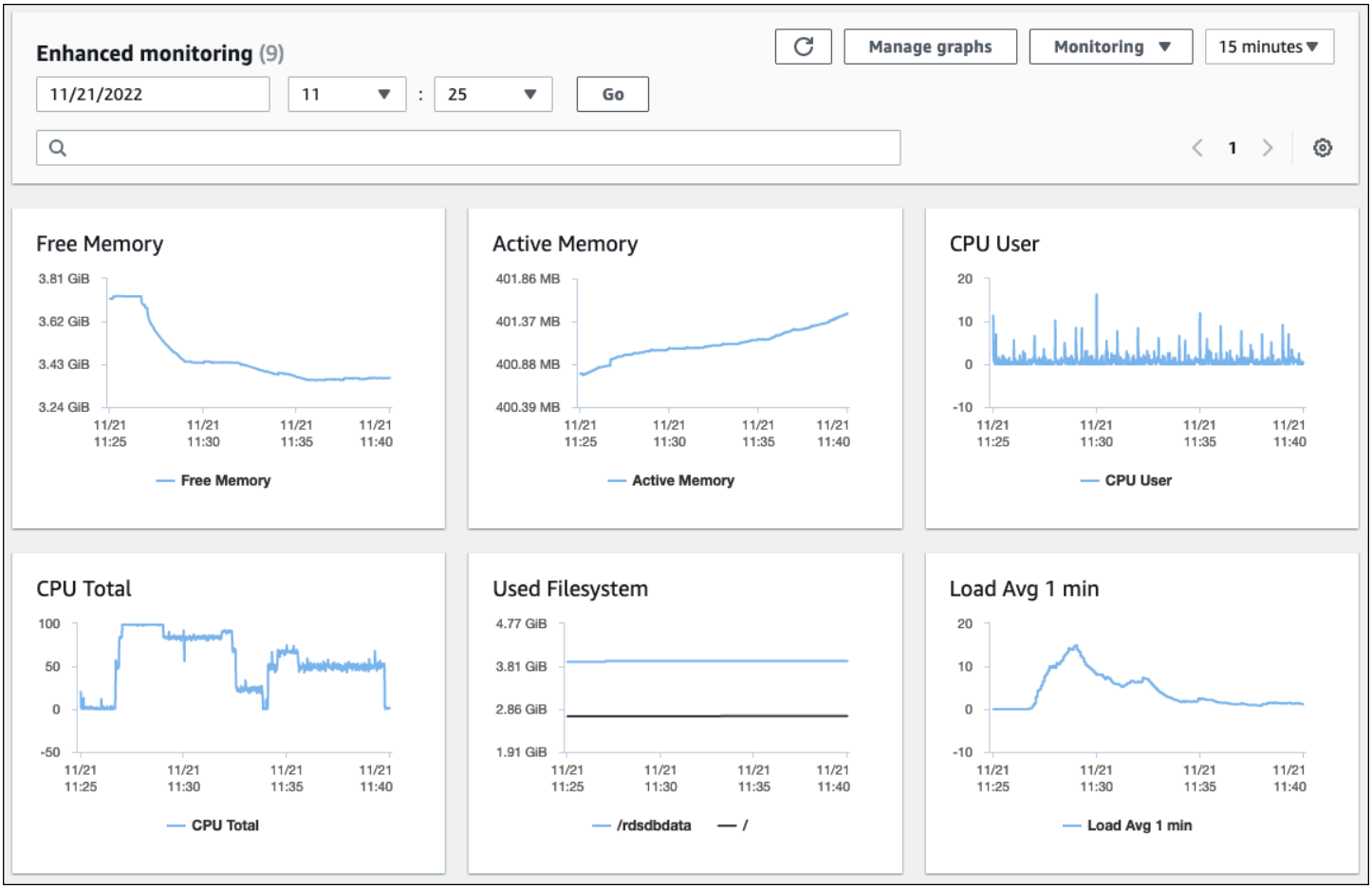
次のグラフは、次の例を示しています。CloudWatchAmazon RDS コンソールに表示される Amazon RDS のメトリックス。



次のグラフは、に表示される同様の指標を示していますCloudWatchダッシュボード。



もう 1 つの OS メトリックは次の方法で収集されます。モニタリングの強化アマゾン RDS 用。このツールを使用すると、リアルタイムのシステムメトリックスと OS プロセス情報が提供されるため、MariaDB 用 Amazon RDS および MySQL DB 用 Amazon RDS インスタンスの状態をより詳細に把握できます。あなたが拡張モニタリングを有効にするDB インスタンス上で必要な精度を設定すると、ツールはオペレーティングシステムのメトリックスとプロセス情報を収集します。これらの情報は、次の場所で表示および分析できます。アマゾン RDS コンソール、次の画面に示すように。



拡張モニタリングが提供する主な指標には次のものがあります。

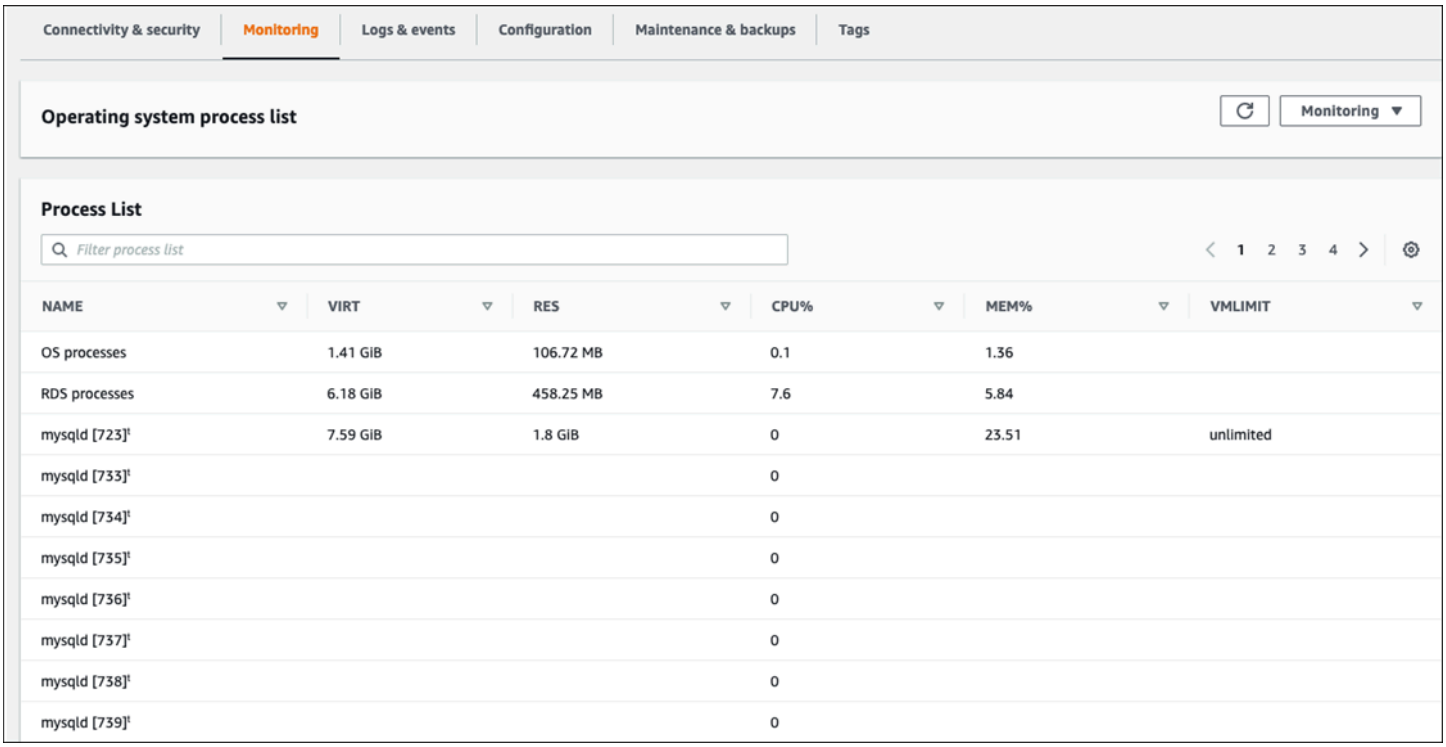
- `cpuUtilization.total`— 使用中の CPU の合計パーセンテージ。
- `cpuUtilization.user`— ユーザー・プログラムが使用している CPU の割合。
- `memory.active`— 割り当てられたメモリの量 (キロバイト単位) 。
- `memory.cached`— ファイル・システム・ベースのI/Oをキャッシュするために使用されるメモリの量。
- `loadAverageMinute.one`— 直近の 1 分間に CPU 時間を要求したプロセスの数。

メトリックの全リストについては、を参照してください。拡張モニタリングの OS メトリックAmazon RDS のドキュメントに記載されています。

Amazon RDS コンソールの OS プロセスリストには、DB インスタンスで実行されている各プロセスの詳細が表示されます。リストは次の 3 つのセクションに分かれています。

- OS プロセス– このセクションには、すべてのカーネルとシステムプロセスの概要がまとめられています。通常、これらのプロセスはデータベースのパフォーマンスにほとんど影響しません。
- RDS プロセス— このセクションでは、その概要を示します。AWSAmazon RDS DB インスタンスをサポートするために必要なプロセス。たとえば、Amazon RDS 管理エージェント、モニタリングおよび診断プロセス、および同様のプロセスが含まれます。
- RDS チャイルドプロセス— このセクションでは、DB インスタンスをサポートする Amazon RDS プロセスの概要を示します。この場合は`mysqld`プロセスとそのスレッド。ザ· `mysqld`スレッドは親スレッドの下にネストされて表示される`mysqld`プロセス。

次の画面図は、Amazon RDS コンソールの OS プロセスリストを示しています。

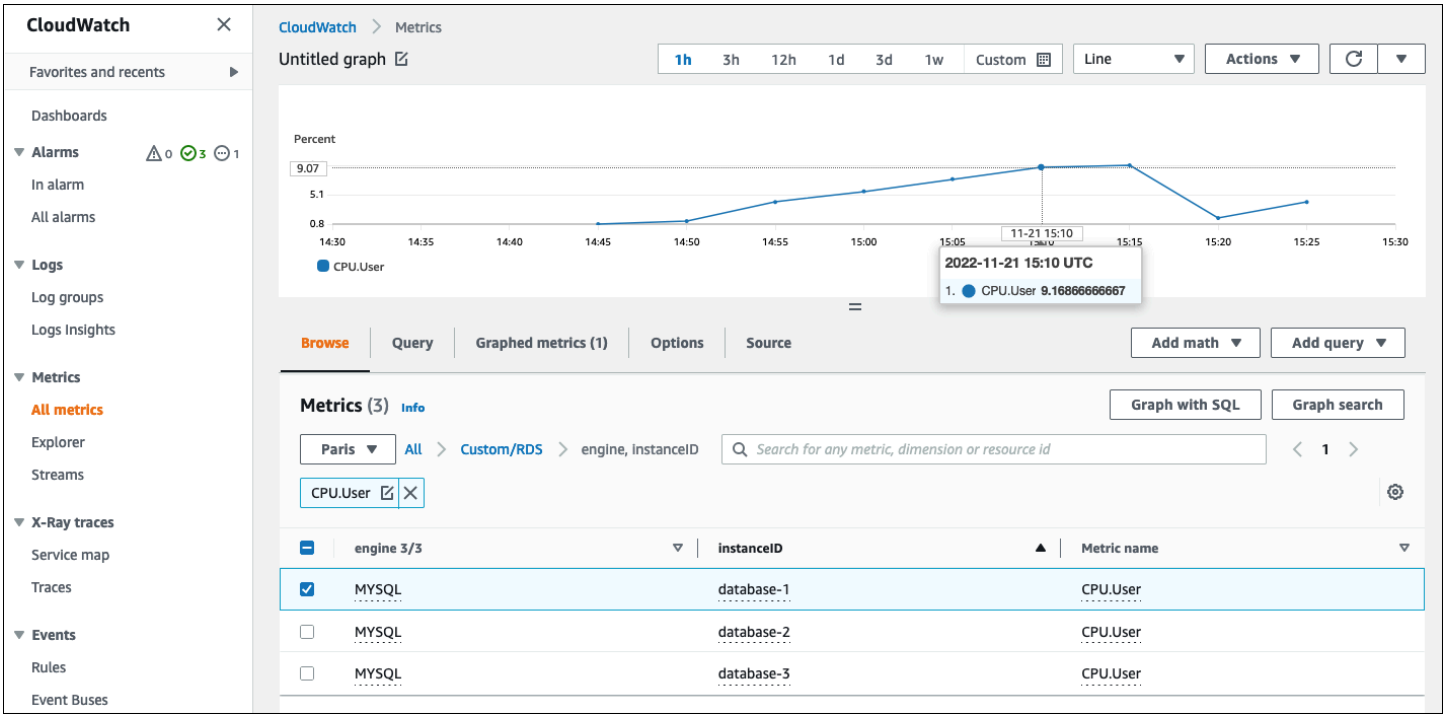


Amazon RDS は、拡張モニタリングからお客様にメトリックスを配信しますCloudWatchログアカウント。Amazon RDS コンソールに表示されるモニタリングデータは、から取得されます。CloudWatchログ。あなたもできますDB インスタンスのメトリックスをログストリームとして取得するからCloudWatchログ。これらのメトリックは JSON 形式で保存されます。以下から拡張モニタリングの JSON 出力を使用できます。CloudWatch選択した監視システムにログインします。

にグラフを表示するにはCloudWatchダッシュボードを作成して、メトリックが定義済みのしきい値を超えた場合にアクションを開始するアラームを作成するには、次の場所でメトリックフィルターを作成する必要がありますCloudWatchからCloudWatchログ。詳細な手順については、を参照して

ください。AWS リポスト拡張モニタリングをフィルタリングする方法についてCloudWatchAmazon RDS の自動カスタムメトリックスを生成するためのログ。

次の例は、カスタム指標を示しています。CPU.UserにCustom/RDS名前空間。このカスタムメトリックは、以下をフィルタリングすることによって作成されます。cpuUtilization.userからのモニタリング指標の強化CloudWatchログ。



メトリックが利用可能になったらCloudWatchリポジトリ、で表示、分析できますCloudWatchダッシュボードにさらに計算やクエリ操作を適用し、アラームを設定してこの特定のメトリックを監視し、観測値が定義済みのアラーム条件と一致しない場合にアラートを生成します。

イベント、ログ、監査証跡

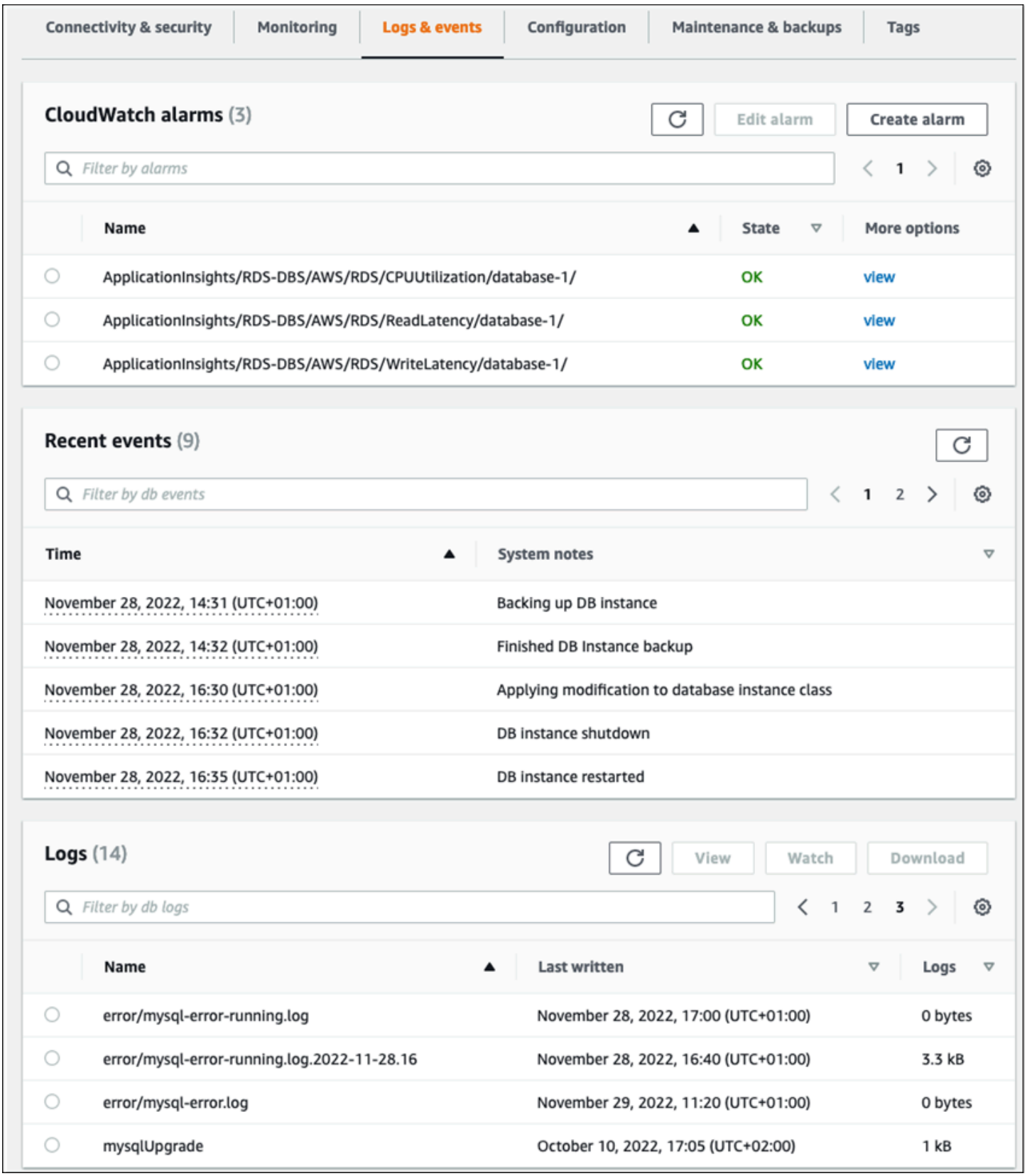
モニタリングDB インスタンスメトリクスそしてOS メトリクス、傾向を分析し、メトリックスをベースライン値と比較し、値が定義済みのしきい値を超えたときにアラートを生成することはすべて必要であり、Amazon RDS DB インスタンスの信頼性、可用性、パフォーマンス、およびセキュリティの達成と維持に役立つベストプラクティスでもあります。ただし、完全なソリューションでは、MySQL および MariaDB データベースのデータベースイベント、ログファイル、監査証跡も監視する必要があります。

セクション

- アマゾン RDS イベント
- データベースログ
- 監査証跡

アマゾン RDS イベント

アンアマゾン RDS イベントAmazon RDS 環境の変更を示しています。たとえば、DB インスタンスのステータスが次のように変化した場合開始に利用可能、Amazon RDS がイベントを生成しますRDS-EVENT-0088 The DB instance has been started。Amazon RDS はアマゾンにイベントを配信しますEventBridgeほぼリアルタイムで。Amazon RDS コンソールからイベントにアクセスできます。AWS CLIコマンドイベントの説明、または Amazon RDS API オペレーションDescribeEvents。次の画面図は、Amazon RDS コンソールに表示されるイベントとログを示しています。


Connectivity & security
Monitoring
Logs & events
Configuration
Maintenance & backups
Tags
CloudWatch alarms (3)
Edit alarm
Create alarm
Filter by alarms
1
Name
State
More options
ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/
OK
view
Recent events (9)
Filter by db events
1
2
Time
System notes
November 28, 2022, 14:31 (UTC+01:00)
Backing up DB instance
November 28, 2022, 14:32 (UTC+01:00)
Finished DB Instance backup
November 28, 2022, 16:30 (UTC+01:00)
Applying modification to database instance class
November 28, 2022, 16:32 (UTC+01:00)
DB instance shutdown
November 28, 2022, 16:35 (UTC+01:00)
DB instance restarted
Logs (14)
View
Watch
Download
Filter by db logs
1
2
3
Name
Last written
Logs
error/mysql-error-running.log
November 28, 2022, 17:00 (UTC+01:00)
0 bytes
error/mysql-error-running.log.2022-11-28.16
November 28, 2022, 16:40 (UTC+01:00)
3.3 kB
error/mysql-error.log
November 29, 2022, 11:20 (UTC+01:00)
0 bytes
mysqlUpgrade
October 10, 2022, 17:05 (UTC+02:00)
1 kB

Amazon RDS は、DB インスタンスイベント、DB パラメータグループイベント、DB セキュリティグループイベント、DB スナップショットイベント、RDS プロキシイベント、青/緑のデプロイイベントなど、さまざまな種類のイベントを発生させます。情報には次のものが含まれます。

- ソース名とソースタイプ。例:`"SourceIdentifier": "database-1", "SourceType": "db-instance"`
- イベントの日付と時刻。例:`"Date": "2022-12-01T09:20:28.595000+00:00"`
- イベントに関連するメッセージ。例:`"Message": "Finished updating DB parameter group"`
- イベントカテゴリ。例:`"EventCategories": ["configuration change"]`

詳細なリファレンスについては、を参照してください。Amazon RDS イベントカテゴリとイベントメッセージAmazon RDS のドキュメントに記載されています。

Amazon RDS イベントを監視することをお勧めします。これらのイベントは DB インスタンスの可用性のステータスの変化、設定の変更、リードレプリカのステータスの変更、バックアップとリカバリのイベント、フェイルオーバーアクション、障害イベント、セキュリティグループの変更、その他多くの通知を示すためです。たとえば、データベースのパフォーマンスと耐久性を高めるためにリードレプリカ DB インスタンスを設定している場合は、以下の Amazon RDS イベントをモニタリングすることをお勧めします。リードレプリカDB インスタンスに関連するイベントカテゴリ。これは、次のようなイベントが原因です`RDS-EVENT-0057 Replication on the read replica was terminated`リードレプリカがプライマリ DB インスタンスと同期しなくなったことを示します。このようなイベントが発生したことを担当チームに通知することで、問題をタイムリーに軽減できる可能性があります。アマゾンEventBridgeおよびその他の AWS サービスAWS Lambda、Amazon シンプルキューサービス (Amazon SQS)、および Amazon シンプル通知サービス (Amazon SNS) は、データベースの可用性の問題やリソースの変更などのシステムイベントへの応答を自動化するのに役立ちます。

Amazon RDS コンソールでは、過去 24 時間のイベントを取得できます。使用する場合AWS CLIまたは Amazon RDS API でイベントを表示する場合は、以下を使用して過去 14 日間のイベントを取得できます。イベントの説明コマンドは以下の通りです。

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
```

```
            "Message": "CloudWatch Logs Export enabled for logs [audit, error, general,
 slowquery]",
            "EventCategories": [],
            "Date": "2022-12-01T09:20:28.595000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        },
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

指定した有効期限まで、または永続的にイベントを長期間保存したい場合は、CloudWatch口グAmazon RDS によって生成されたイベントに関する情報を記録します。このソリューションを実装するには、Amazon SNS トピックを使用して Amazon RDS イベント通知を受け取り、Lambda 関数を呼び出してイベントを記録します。CloudWatch口グ。

1. イベントで呼び出される Lambda 関数を作成し、イベントの情報を次のように記録します。CloudWatch口グ。CloudWatchLogs は Lambda と統合されており、以下を使用してイベント情報を簡単に記録できます。印刷ファンクションへstdout。
2. Lambda 関数 (set) へのサブスクリプションによる SNS トピックの作成プロトコル(Lambda) に移動し、次のように設定します終点前のステップで作成した Lambda 関数の Amazon リソースネーム (ARN) に送信します。
3. Amazon RDS イベント通知を受信するように SNS トピックを設定します。詳細な手順については、を参照してください。AWSRe: 記事を投稿するAmazon SNS トピックに Amazon RDS 通知を受信させる方法について説明しています。
4. Amazon RDS コンソールで、新しいイベントサブスクリプションを作成します。セットターゲットARN に移動し、以前に作成した SNS トピックを選択します。セットソースタイプそして含めるイベントカテゴリあなたの要件に応じて。詳細については、を参照してください。Amazon RDS イベント通知の購読Amazon RDS のドキュメントに記載されています。

データベースログ

MySQL および MariaDB データベースは、監査やトラブルシューティングに使用できるログを生成します。それらのログは以下のとおりです。

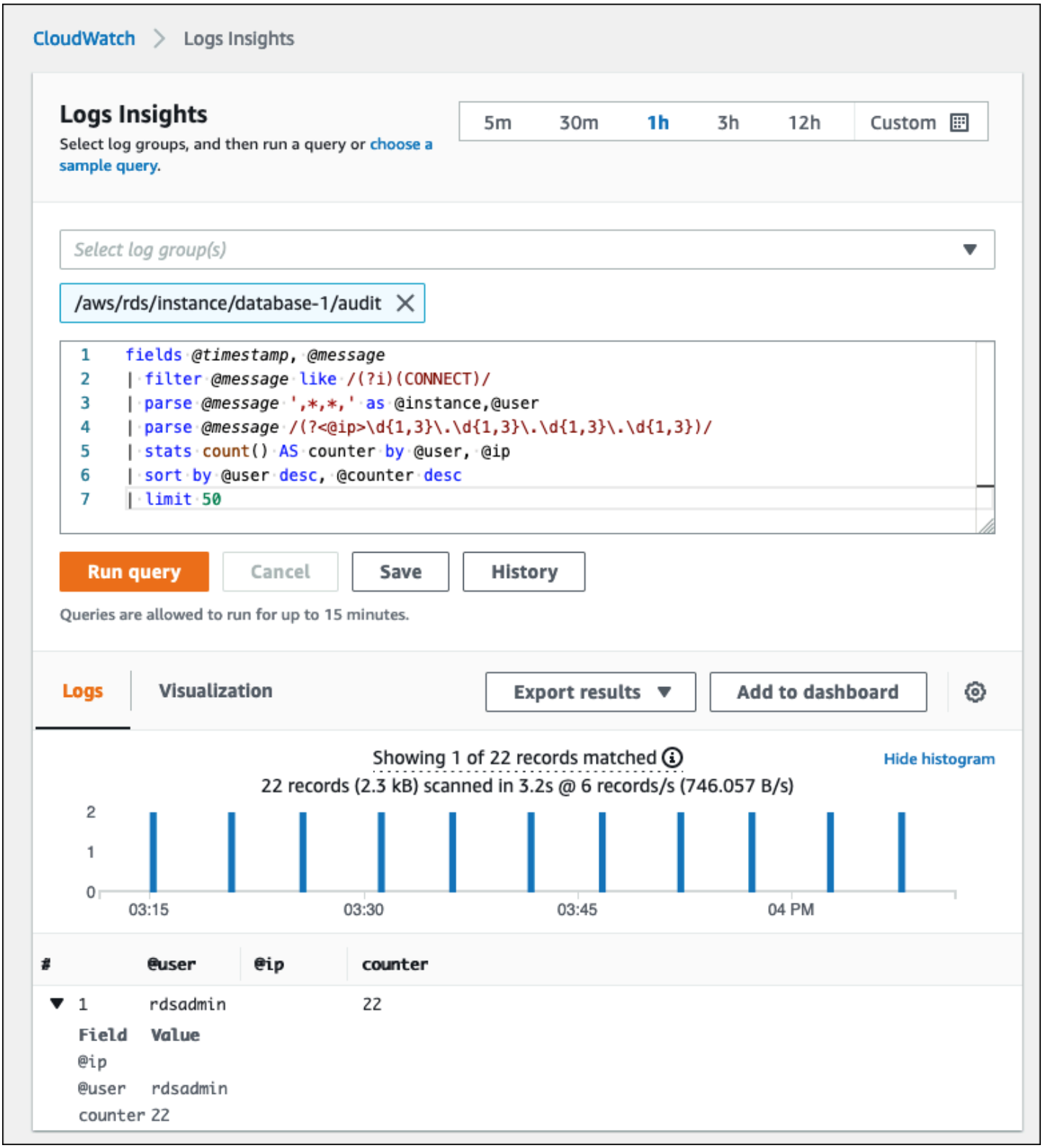
- 監査— オーディットトレイルは、サーバーのアクティビティを記録するレコードのセットです。クライアントセッションごとに、サーバーに接続したユーザー (ユーザー名とホスト)、実行されたクエリ、アクセスされたテーブル、および変更されたサーバー変数を記録します。
- エラー— このログにはサーバの (mysqld) 起動時間とシャットダウン時間、およびサーバーの起動時とシャットダウン時、およびサーバーの実行中に発生するエラー、警告、メモなどの診断メッセージ。
- 全般— このログには、次のアクティビティが記録されますmysqldこれには、各クライアントの接続アクティビティと切断アクティビティ、およびクライアントから受信した SQL クエリが含まれます。一般的なクエリログは、エラーが疑われ、クライアントの送信先を正確に知りたい場合に非常に役立ちます。mysqld。
- スロークエリ— このログには、実行に時間がかかった SQL クエリの記録が記録されます。

ベストプラクティスとして、Amazon RDS からアマゾンにデータベースログをパブリッシュ CloudWatchログ。とCloudWatchログでは、ログデータをリアルタイムで分析し、耐久性の高いストレージにデータを保存し、次の方法でデータを管理できます。CloudWatchログエージェント。できますデータベースログにアクセスして監視するAmazon RDS コンソールから。使用することもできますCloudWatchLogs Insightsでログデータをインタラクティブに検索、分析できますCloudWatchログ。次の例は、何回かを確認する監査ログのクエリを示しています。CONNECTイベント、接続者、接続元のクライアント (IP アドレス) がログに表示されます。監査ログからの抜粋は次のようになります。

```
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,CONNECT,,,0,SOCKET
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,DISCONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,CONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,DISCONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,CONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,DISCONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,CONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,DISCONNECT,,,0,SOCKET
```

ログインサイトクエリの例では、次のことがわかります。rdsadminからデータベースに接続localhost次の図に示すように、5 分おきに、合計 22 回です。これらの結果は、アクティビティ

がモニタリングシステム自体などの内部の Amazon RDS プロセスから発生したことを示しています。



ログイベントには、MySQL や MariaDB DB インスタンスに関連する操作に関する警告やエラーなど、カウントしたい重要なメッセージが含まれることがよくあります。たとえば、操作が失敗した場合、エラーが発生し、次のようにエラーログファイルに記録されます。`ERROR 1114 (HY000): The table zip_codes is full`。これらのエントリを監視して、エラーの傾向を把握したい場合があります。できますカスタム作成CloudWatchフィルターを使用した Amazon RDS ログのメトリックスAmazon RDS データベースログの自動モニタリングを可能にし、特定のログで特定のパターンを監視し、予想される動作に違反した場合にアラームを生成できるようにします。例えば、ロググループのメトリックスフィルタを作成`/aws/rds/instance/database-1/error`エラーログを監視して検索します特定のパターン、など`ERROR`。を設定フィルターパターンに`ERROR`そしてメトリック値に`1`。フィルターは、そのキーワードを含むすべてのログレコードを検出します。`ERROR`そして、「ERROR」を含むログイベントごとにカウントが 1 ずつ増えます。フィルターを作成したら、MySQL または MariaDB のエラーログでエラーが検出された場合に通知するアラームを設定できます。

スロークエリログとエラーログの監視について詳しくは、CloudWatchダッシュボードと使用CloudWatchログインサイト (ブログ記事を参照)アマゾンの作成CloudWatchAmazon RDS とAmazon Aurora MySQL をモニタリングするためのダッシュボード。

監査証跡

監査証跡 (または監査ログ) には、AWS アカウント内のイベントに関するセキュリティ関連の時系列記録が記録されます。これには、データベースやクラウド環境に影響を与えた一連のアクティビティの証拠となる Amazon RDS のイベントが含まれます。Amazon RDS for MySQL または MariaDB では、オーディットトレイルを使用するには以下が必要です。

- DB インスタンス監査ログの監視
- での Amazon RDS API 呼び出しのモニタリングAWS CloudTrail

Amazon RDS DB インスタンスの場合、監査の目的には通常、以下が含まれます。

- 以下の事項に対するアカウンタビリティの有効化
  - パラメータまたはセキュリティ設定に対して行われた変更
  - データベーススキーマ、テーブル、または行で実行されるアクション、または特定のコンテンツに影響するアクション
- 侵入検知と調査
- 不審なアクティビティの検出と調査

- 権限に関する問題の検出 (たとえば、一般ユーザーまたは特権ユーザーによるアクセス権の乱用を特定するため)

データベースオーディットトレイルは、次のような一般的な質問に答えようとします。データベース内の機密データを閲覧または変更したのは誰ですか? これはいつ起こったのですか ? 特定のユーザーはどこからデータにアクセスしましたか? 特権ユーザーは無制限アクセス権を悪用しましたか?

MySQL と MariaDB はどちらも、MariaDB 監査プラグインを使用して DB インスタンスの監査証跡機能を実装しています。このプラグインは、データベースにログオンするユーザーやデータベースに対して実行されるクエリなどのデータベースアクティビティを記録します。データベースのアクティビティのレコードはログファイルに保存されます。監査ログにアクセスするには、DB インスタンスは `MARIADB_AUDIT_PLUGIN` オプションを指定してカスタムオプショングループを使用する必要があります。詳細については、を参照してください。MySQL 用の MariaDB 監査プラグインのサポートAmazon RDS のドキュメントに記載されています。監査ログのレコードは、プラグインで定義されている特定の形式で保存されます。監査ログ形式の詳細については、MariaDB サーバーのドキュメンテーション。

ザのAWS クラウドお客様用のオーディットトレイルAWSアカウントはAWS CloudTrailサービス。CloudTrailAmazon RDS の API 呼び出しをイベントとしてキャプチャします。Amazon RDS のすべてのアクションがログに記録されます。CloudTrailユーザー、ロール、または別のユーザーによって実行された Amazon RDS のアクションの記録を提供しますAWSサービス。イベントには、で実行されたアクションが含まれますAWS管理コンソール、AWS CLI、およびAWSSDK と API。

例

一般的な監査シナリオでは、組み合わせる必要がある場合がありますAWS CloudTrailデータベース監査ログと Amazon RDS イベントモニタリングを含む証跡 たとえば、Amazon RDS DB インスタンスのデータベースパラメータを使用するシナリオがあるかもしれません (たとえば、`database-1`) が変更されたので、誰が変更したか、何が変更されたか、いつ変更されたかを特定することがあなたの仕事です。

タスクを実行するには、次の手順に従います。

1. データベースインスタンスに発生した Amazon RDS イベントを一覧表示しますdatabase-1そして、そのカテゴリにイベントがあるかどうかを判断しますconfiguration changeそれにはメッセージがありますFinished updating DB parameter group。

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
```

```
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

2. DB インスタンスが使用している DB パラメータグループを特定してください。

```
$ aws rds describe-db-instances --db-instance-identifier database-1 --query
 'DBInstances[*].[DBInstanceIdentifier,Engine,DBParameterGroups]'
[
    [
        "database-1",
        "mariadb",
        [
            {
                "DBParameterGroupName": "mariadb10-6-test",
                "ParameterApplyStatus": "pending-reboot"
            }
        ]
    ]
]
```

3. を使うAWS CLI検索するにはCloudTrailイベントその地域ではdatabase-1は、ステップ 1 で発見された Amazon RDS イベントの前後の期間にデプロイされ、その場所にはデプロイされますEventName=ModifyDBParameterGroup。

```
$ aws cloudtrail --region eu-west-3 lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=ModifyDBParameterGroup --start-time
 "2022-12-01, 09:00 AM" --end-time "2022-12-01, 09:30 AM"

{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Role1",
                "accountId": "111122223333",
                "userName": "User1"
            }
        }
    },
    "eventTime": "2022-12-01T09:18:19Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "ModifyDBParameterGroup",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "parameters": [
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_log_buffer_size",
                "parameterValue": "8388612"
            },
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_write_io_threads",
                "parameterValue": "8"
            }
        ],
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "responseElements": {
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "requestID": "fdf19353-de72-4d3d-bf29-751f375b6378",
    "eventID": "0bba7484-0e46-4e71-93a8-bd01ca8386fe",
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
```

```
    "sessionCredentialFromConsole": "true"
}
```

ザのCloudTrailイベントはそれを明らかにしますUser1ロール付きRole1からAWSアカウント111122223333 が DB パラメータグループを変更しましたmariadb10-6-test、DB インスタンスで使用されていたものdatabase-1オン2022-12-01 at 09:18:19 h。2 つのパラメータが変更され、次の値に設定されました。

- innodb_log_buffer_size = 8388612
- innodb_write_io_threads = 8

[追加]CloudTrailそしてCloudWatchログ機能

過去 90 日間に発生した運用上およびセキュリティ上のインシデントのトラブルシューティングには、以下を参照してください。イベント履歴にCloudTrailコンソール。保存期間を延長して追加のクエリ機能を利用するには、AWS CloudTrail湖。とAWS CloudTrailLake では、イベントデータをイベントデータストアに最大 7 年間保存できます。さらに、このサービスは複雑な SQL クエリをサポートしているため、単純なキー値検索によるビューよりも詳細でカスタマイズ可能なイベントビューが提供されます。イベント履歴。

オーディットトレイルを監視し、アラームを設定し、特定のアクティビティが発生したときに通知を受け取るには、構成しますCloudTrailトレイルレコードの送信先はCloudWatchログ。トレイルレコードが次のように保存された後CloudWatchログ:メトリックフィルターを定義して、ログイベントを評価して用語、フレーズ、または値に一致するように評価したり、メトリックスフィルターにメトリックを割り当てたりできます。さらに、作成することができますCloudWatch指定したしきい値と期間に従って生成されるアラーム。たとえば、担当チームが適切なアクションを実行できるように、担当チームに通知を送信するアラームを設定できます。アラームへの対応アクションが自動的に実行されるように CloudWatch を設定することもできます。

アラート

アラートは、ITインフラストラクチャとITサービスのセキュリティ、可用性、パフォーマンス、信頼性に関する最も重要な情報源の1つです。継続的なセキュリティ脅威、システム停止、パフォーマンスの問題、またはシステム障害についてITチームに通知し、通知します。

情報技術インフラストラクチャライブラリ（ITIL）、特にITサービス管理（ITSM）プラクティスは、監視、イベント管理、およびインシデント管理のベストプラクティスの中心に自動アラートを設定しています。

インシデントアラートとは、監視ツールがアラートを生成して、IT環境の変更、リスクの高いアクション、または障害について、チームや自動化ツール（自動的にアクション可能なアイテム用）に通知することです。ITアラートは、重大なインシデントにつながる可能性のあるシステム停止や変更に対する防御の最前線です。システムを自動的に監視し、システム停止や危険な変更に関するアラートを生成することで、ITチームはダウンタイムを最小限に抑え、それに伴う高額なコストを削減できます。

ベストプラクティスとして、AWS適切に設計されたフレームワークでは、モニタリングを使用してアラームベースの通知を生成する、およびプロアクティブな監視とアラーム。使用CloudWatchまたはサードパーティの監視サービスを使用して、メトリックが予想範囲外になったときにアラームを設定することもできます。

アラート管理の目的は、ロギング、分類、アクションの定義と実装、終了、インシデント後のレビュー活動を通じて、IT関連のイベントやインシデントを処理するための効率的で標準化された手順を確立することです。

セクション

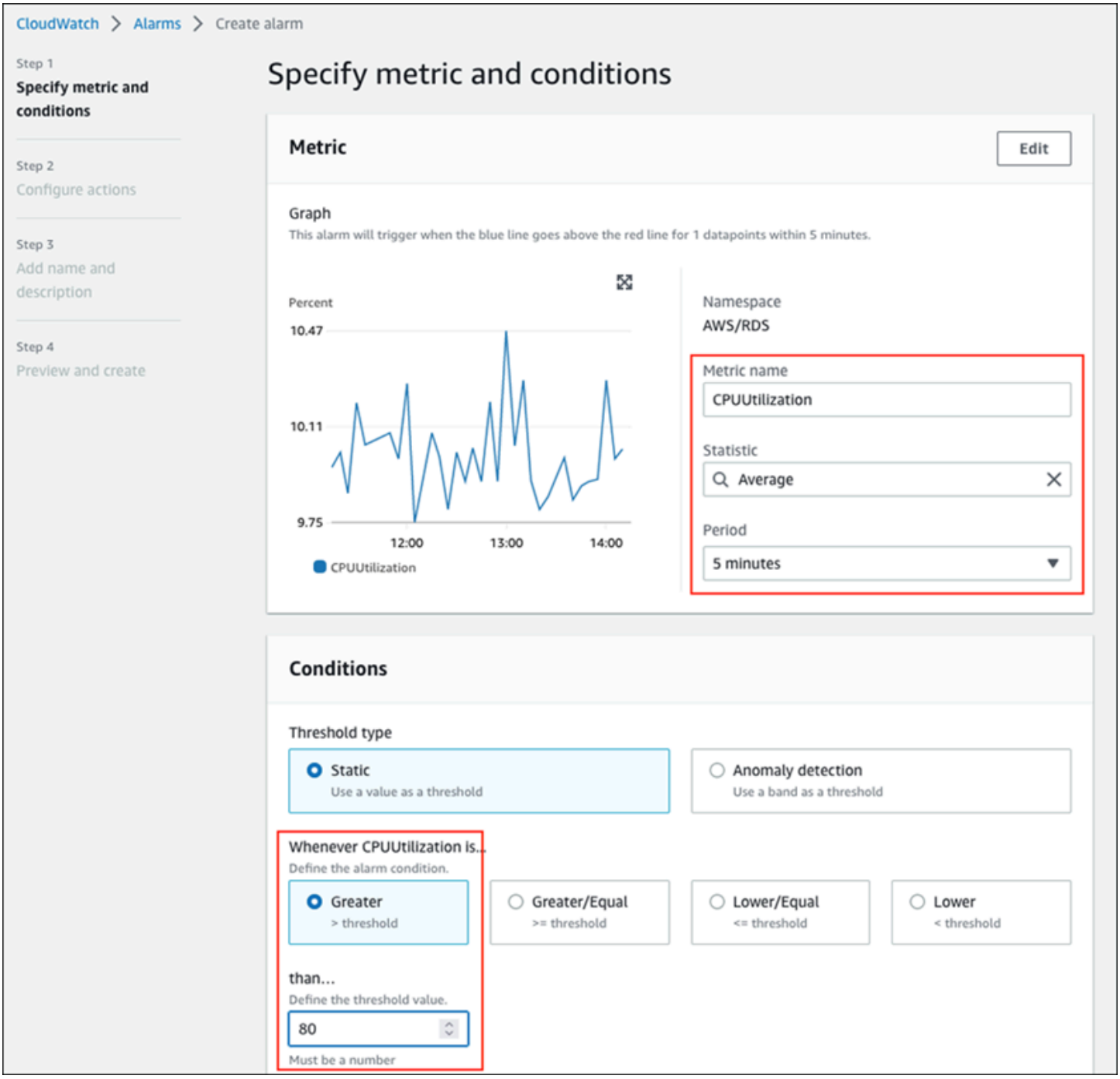
- CloudWatch のアラーム
- EventBridgeルール
- アクションの指定、アラームの有効化と無効化

CloudWatch アラーム

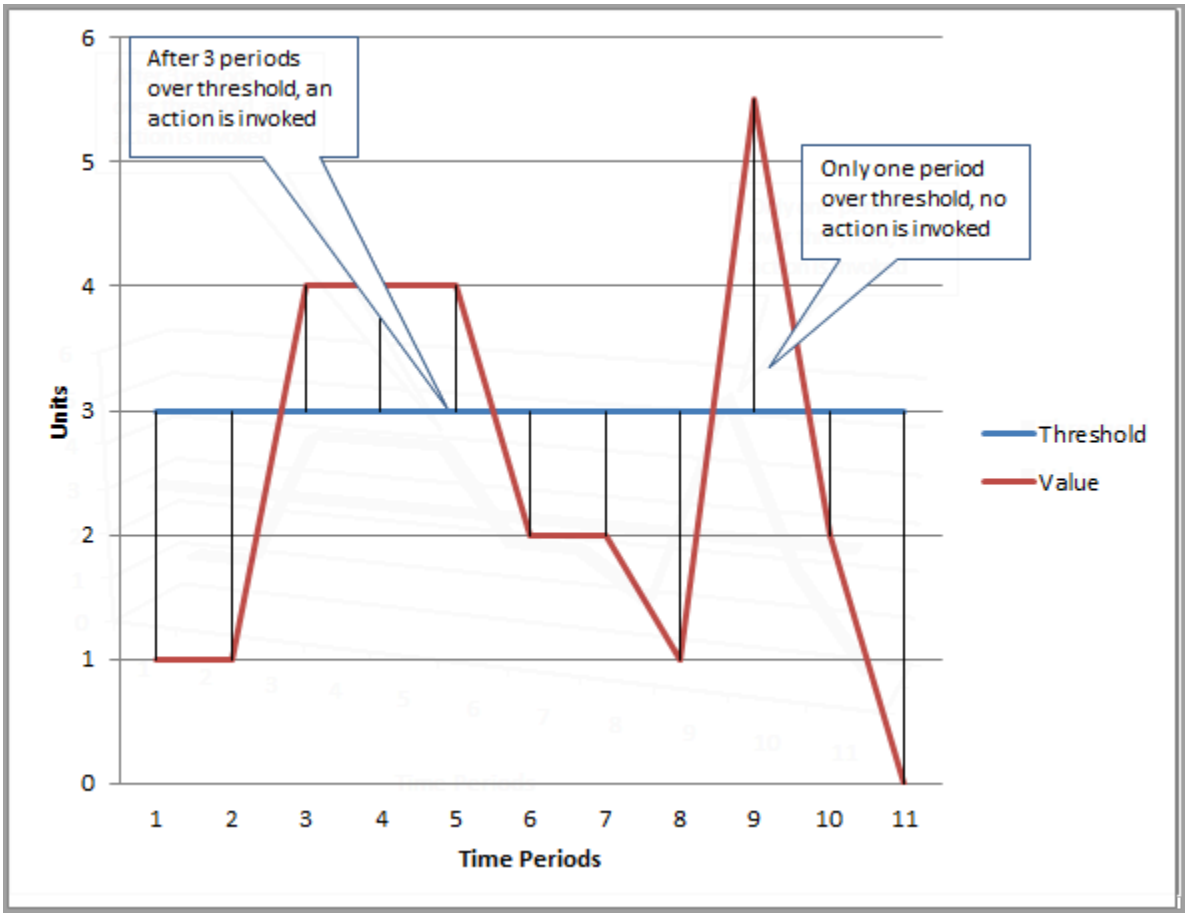
Amazon RDS DB インスタンスを運用する場合、さまざまな種類のメトリックス、イベント、トレースをモニタリングしてアラートを生成する必要があります。MySQL および MariaDB データベースの場合、重要な情報源は以下のとおりです。DB インスタンスメトリクス、OS メトリクス、イベン

ト、ログ、監査証跡。を使用することをおすすめしますCloudWatchアラーム指定した期間にわたって 1 つのメトリクスを監視できます。

次の例は、を監視するアラームを設定する方法を示していますCPUUtilizationすべての Amazon RDS DB インスタンスのメトリックス (CPU 使用率) 5 分間の評価期間中にいずれかの DB インスタンスの CPU 使用率が 80% を超えた場合にアラームがトリガーされるように設定します。



つまり、アラームはALARM5 分以上にわたって CPU 使用率が高い (80% を超える) データベースがあるかどうかを明記してください。アラームは、に残っていますOKCPU の使用率が短期間で 80% を超えることがあり、その後再びしきい値を下回った場合の状態です。次のグラフは、この口ジックを示しています。



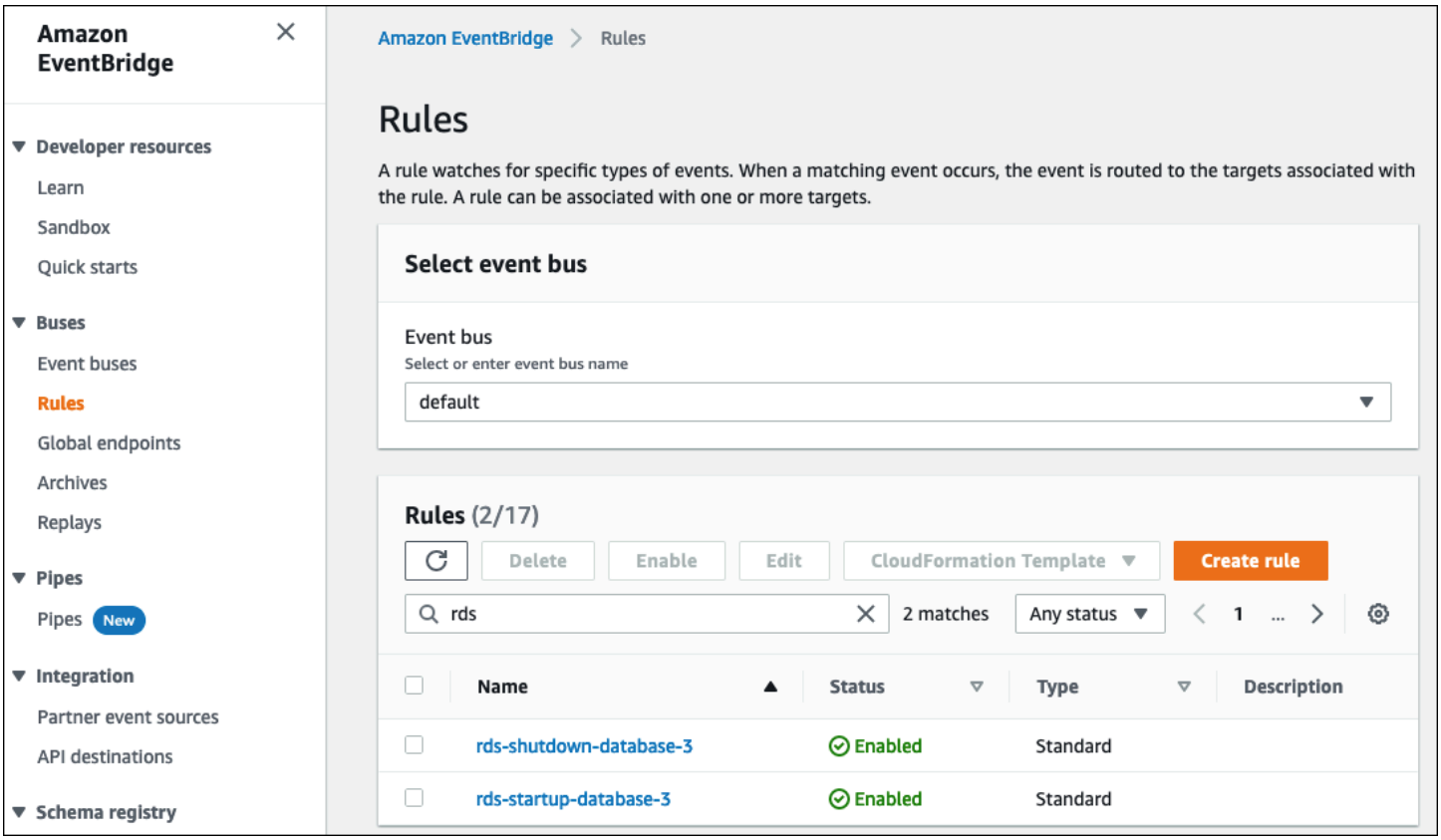
CloudWatchアラームはメトリックアラームと複合アラームをサポートします。

- あるメトリックアラームシングルを見るCloudWatchメトリック。メトリックに対して数式を実行できます。メトリックスアラームは Amazon SNS メッセージを送信できます。このメッセージは、特定のしきい値に対するメトリクスの値に基づいて、さまざまな期間にわたって 1 つ以上のアクションを実行できます。
- ある複合アラームルール表現に基づいており、複数のアラームの状態を評価して、ALARMルールのすべての条件が満たされている場合にのみステートしてください。複合アラームは通常、不要なアラートの数を減らすために使用されます。たとえば、アクションを実行しないように設定された複数のメトリックアラームを含む複合アラームがある場合があります。複合アラームは、複合内の個々のメトリックアラームがすべてすでに存在している場合にアラートを送信します。ALARM

CloudWatchアラームは監視のみCloudWatch指標。エラー、スロークエリ、または一般ログに基づいてアラームを作成する場合は、作成する必要がありますCloudWatchログからのメトリックス。これについては、前述のとおりに行うことができます。OS モニタリングそしてイベント、ログ、監査証跡セクション、フィルターを使用してログイベントからメトリクスを作成。同様に、拡張モニタリングのメトリックについてアラートを出すには、でメトリックスフィルターを作成する必要がありますCloudWatchからCloudWatchログ。

EventBridgeルール

アマゾン RDS イベントアマゾンに配送されますEventBridge、そして使用できますEventBridgeルールそれらの出来事に対応するためです たとえば、次のように作成できますEventBridge次の画面に示すように、特定の DB インスタンスが 1 つ停止または起動した場合に通知してアクションを実行するルール。

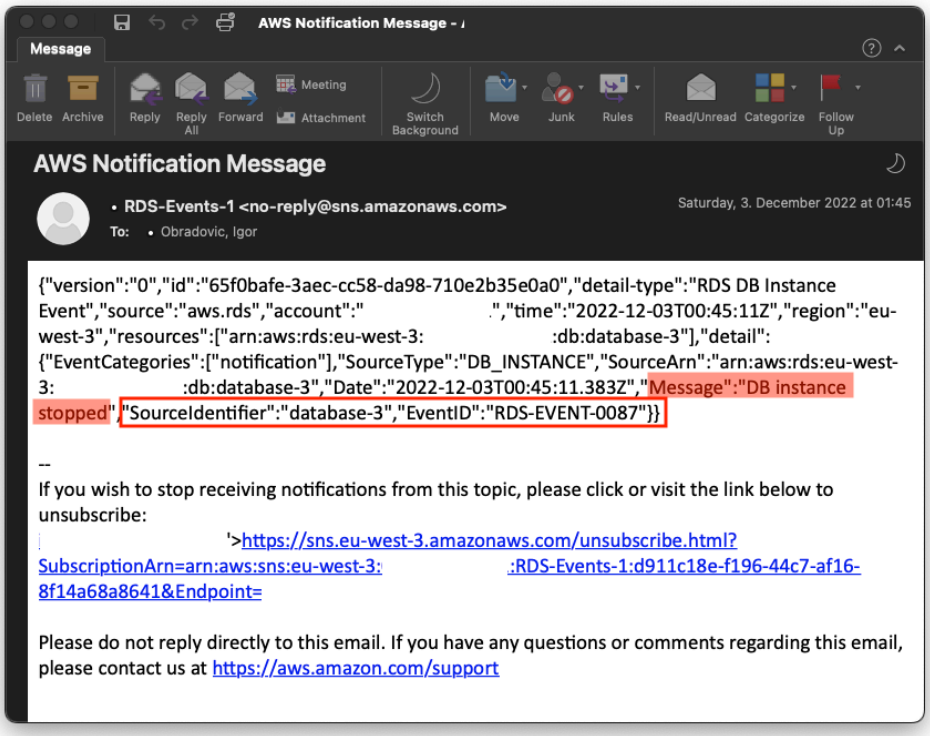


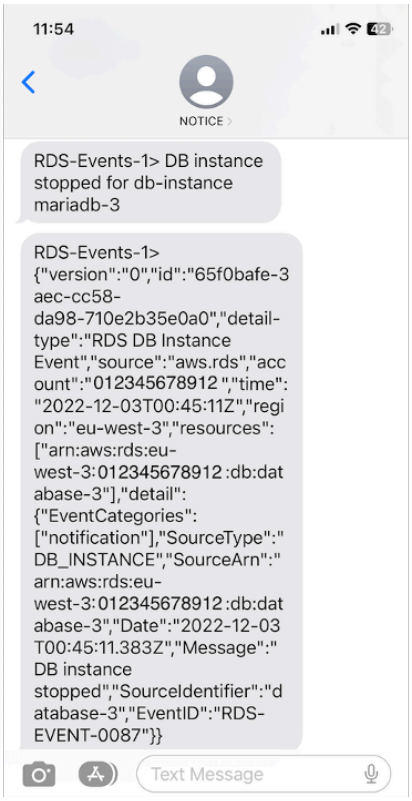
検出するルールThe DB instance has been stoppedイベントには Amazon RDS イベント IDがありますRDS-EVENT-0087、そこで設定したのがEvent Patternルールのプロパティ:

```
{
  "source": ["aws.rds"],
```

```
  "detail-type": ["RDS DB Instance Event"],
  "detail": {
    "SourceArn": ["arn:aws:rds:eu-west-3:111122223333:db:database-3"],
    "EventID": ["RDS-EVENT-0087"]
  }
}
```

このルールは DB インスタンスを監視しますdatabase-3のみ、そして監視しますRDS-EVENT-0087イベント。いつEventBridgeイベントを検出し、イベントを「」と呼ばれるリソースまたはエンドポイントに送信しますターゲット。ここで、Amazon RDS インスタンスが停止した場合に実行するアクションを指定できます。SNS トピック、Amazon シンプルキューサービス (Amazon SQS) キューなど、さまざまなターゲットにイベントを送信できます。AWS Lambda機能、AWS Systems Managerオートメーション、およびAWS Batchジョブ、Amazon API Gateway、インシデントマネージャーの対応計画、次の機能AWS Systems Manager、その他多数。たとえば、通知メールと SMS を送信する SNS トピックを作成し、その SNS トピックをターゲットとして割り当てることができます。EventBridge規則。Amazon RDS DB インスタンスの場合database-3停止されました。Amazon RDS がイベントを配信しますRDS-EVENT-0087にEventBridge、検出される場所。EventBridge次に、SNS トピックであるターゲットを呼び出します。SNS トピックは、電子メール (次の図を参照) と SMS を送信するように設定されています。





アクションの指定、アラームの有効化と無効化

を使用できますCloudWatchアラーム:アラームが次のモードに切り替わったときに実行するアクションを指定しますOK、ALARM、およびINSUFFICIENT_DATA州。CloudWatchには、SNS トピックとの統合が組み込まれています。また、Amazon Elastic Compute Cloud (Amazon EC2) アクションや Amazon EC2 Auto Scaling グループアクションなど、Amazon RDS メトリックスには適用されない追加のアクションカテゴリがいくつか組み込まれています。EventBridge通常、Amazon RDS メトリックスでアラームがトリガーされたときにアクションを実行するルールを記述したり、ターゲットを定義したりするために使用されます。CloudWatchイベントを送信EventBridge毎回CloudWatchアラームの状態が変わります。これらのアラーム状態変更イベントを使用して、以下のイベントターゲットをトリガーできます。EventBridge。詳細については、を参照してください。アラームイベントとEventBridgeにCloudWatchドキュメンテーション。

また、アラームを管理する必要がある場合もあります。たとえば、計画された構成変更やテスト中にアラームを自動的に無効にし、計画されたアクションが終了したらアラームを再度有効にする場合などです。たとえば、ダウンタイムを必要とするデータベースソフトウェアのアップグレードを予定していて、データベースが使用できなくなった場合にアクティブになるアラームがある場合は、API アクションを使用してアラームを無効または有効にできます。DisableAlarmActionsそしてEnableAlarmActions、またはdisable-alarm-actionsそしてenable-alarm-actionsのコマンドAWS CLI。アラームの履歴は、で確認することもできますCloudWatchコンソールまたはを使用してDescribeAlarmHistoryAPI アクションまたはdescribe-alarm-historyのコマンドAWS CLI。CloudWatchアラーム履歴を 2 週間保存します。にCloudWatchコンソール、選択できますお気に入りと最近のものナビゲーションペインのメニューで、お気に入りのアラームや最近使用したアラームを設定したり、アクセスしたりできます。

次のステップとリソース

リレーショナルデータベースをに移行する方法の詳細についてはAWS クラウド、次のストラテジーを参照してくださいAWS規範ガイダンスのウェブサイト:

- リレーショナルデータベースの移行戦略

探索できますデータベース移行パターンにとってstep-by-stepで実行されている特定のリレーショナルデータベースに関する説明AWS クラウドこれには、監視、移行、およびデータ管理に関連するタスクが含まれます。

そのページのフィルターを使用して、次の方法でパターンを検索します。AWSサービス (たとえば、Amazon RDS や Amazon Aurora への移行)、ワークロード別 (MySQL や MariaDB データベースを含むオープンソースなど)、または計画的な使用状況 (本番環境またはパイロット)

その他のリソースについては、以下を参照してください。

- Amazon リレーショナルデータベースサービスユーザーガイド
- アマゾンCloudWatchユーザーガイド
- アマゾン RDS に関するよくある質問
- パフォーマンスインサイトに関するよくある質問
- Amazon RDS パフォーマンスインサイトのカウンターメトリックスを Amazon を使用するサードパーティのアプリケーションパフォーマンス監視サービスプロバイダーに配信CloudWatchメトリックスストリーム(AWSブログ投稿)
- アマゾンの作成CloudWatchAmazon RDS と Amazon Aurora MySQL をモニタリングするためのダッシュボード(AWSブログ投稿)
- パフォーマンスインサイトによる MySQL 用 Amazon RDS のチューニング(AWSブログ投稿)

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
更新した情報	エクスポーターに関する情報を更新し、エクスポーターを選択するためのガイドラインを追加しました。	2024 年 6 月 13 日
初版発行	—	2023 年 6 月 30 日

AWS 規範的ガイダンスの用語集

以下は、 AWS 規範的ガイダンスが提供する戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: オンプレミスの Oracle データベースを AWS クラウドの Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: AWS クラウドの EC2 インスタンスでオンプレミスの Oracle データベースを Oracle に移行します。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。この移行シナリオは、オンプレミス環境と 間の仮想マシン (VM) の互換性とワークロードの移植性 AWSをサポートする VMware Cloud on に固有のものです AWS。 AWSのVMware Cloud にインフラを移行する際、オンプレミスのデータセンターから VMware Cloud Foundation のテクノロジーを使用することができます。例: Oracle データベースをホストするハイパーバイザーを VMware Cloud on に再配置します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したい

アプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。

- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「マネージドサービス」を参照してください。

ACID

「原子性、一貫性、分離性、耐久性」を参照してください。

アクティブ - アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。アクティブ/パッシブ移行よりも柔軟性がありますが、より多くの作業が必要です。

アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行の方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

行のグループを操作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例としては、 SUMや などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーションコントロール

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の需要要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」を参照してください。

AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 の ABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行 AWS するための効率的で効果的な計画を立てるのに役立つ、 のガイドラインとベストプラクティスのフレームワーク。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを編成します。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、組織がクラウド導入を成功させるための準備に役立つ、人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool （ AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「事業継続計画」を参照してください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントのData in a behavior graphを参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネス も参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンは 1 つの環境 (青) で実行し、新しいアプリケーションバージョンは他の環境 (緑) で実行します。この戦略は、影響を最小限に抑えながら迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティやインタラクションをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボット と呼ばれる他のボッ

トの中には、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

マルウェアに感染し、ボットのヘルダーまたはボットオペレーター と呼ばれる、単一関係者の管理下にあるボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチについて (GitHub ドキュメント) 」を参照してください。

ブレークグラスアクセス

例外的な状況や承認されたプロセスを通じて、ユーザーが通常アクセス許可を持たない AWS アカウント にすばやくアクセスできるようになります。詳細については、 Well-Architected ガイダンスの「ブレークグラスプロシージャの実装」インジケータ AWS を参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 の ビジネス機能を中心に組織化 セクションを参照してください。

ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンの低速かつ増分的なリリース。確信できたら、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「データキャプチャの変更」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストします。AWS Fault Injection Service （ AWS FIS ） を使用して、 AWS ワークロードに負荷をかけてレスポンスを評価する実験を実行できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、ローカルでデータを暗号化します。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウドエンタープライズ戦略ブログのCCoE の投稿」を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的にエッジコンピューティングテクノロジーに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」 を参照してください。

導入のクラウドステージ

組織が AWS クラウドに移行する際に通常実行する 4 つのフェーズ：

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 クラウド AWS エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略とどのように関連しているかについては、 AWS 「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、 GitHub または が含まれます AWS CodeCommit。コードの各バージョンはブランチと呼ばれます。マイクロサー

ビスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker は CV の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定した状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンに、または組織全体に 1 つのエンティティとしてデプロイできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性

の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、データ分類を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元化された管理とガバナンスにより、分散型の分散型データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待されるネットワークから信頼できるリソースにアクセスしていることを確認できます。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには通常、大量の履歴データが含まれており、クエリや分析によく使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせる。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

ディープラーニング

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

defense-in-depth

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を に採用するときは AWS、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。例えば、 defense-in-depth アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS Organizations ドキュメントのAWS Organizationsで使用できるサービスを参照してください。

デプロイメント

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、Implementing security controls on AWSのDetective controlsを参照してください。

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマ では、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けに一般的に使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

災害によるダウンタイムとデータ損失を最小限に抑えるために使用する戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法の詳細については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差の追跡。例えば、 AWS CloudFormation を使用してシステムリソース のドリフトを検出したり、 を使用して AWS Control Tower ガバナンス要件への準拠に影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティング と比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を短縮できます。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティングプロセス。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (アカウンティング、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service （ AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。例えば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイド を参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

スタースキーマ の中央テーブル。事業運営に関する定量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 種類の列が含まれます。

フェイルファスト

頻繁で段階的なテストを使用して開発ライフサイクルを短縮する哲学。これはアジャイルアプローチの重要な部分です。

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を向上させるアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界です。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性：AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

段階的なアプローチを使用するのではなく、変更データキャプチャによる継続的なデータレプリケーションを使用して、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

G

Geo Blocking

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

Amazon では CloudFront、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、 CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装

されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは、 AWS Config、、Amazon AWS Security Hub、GuardDuty、Amazon Inspector AWS Trusted Advisor、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

ハイアベイラビリティ (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外で行われます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1～4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「産業モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャ よりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS Well-Architected フレームワークの「変更不可能なインフラストラクチャを使用したデプロイ」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からのネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリ

ケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

接続、リアルタイムデータ、自動化、分析、AI/ML の進歩を通じて、 のビジネスプロセスのモダナイゼーションを指すために 2016 年に Klaus Schwab によって導入された用語。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

産業分野における IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「Building an industrial Internet of Things (IIoT) digital transformation strategy」を参照してください。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「AWS を使用した機械学習モデルの解釈」を参照してください。

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、オペレーション統合ガイド を参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロー

ドとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、安全でスケーラブルなマルチアカウント AWS 環境のセットアップ を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの最小特権アクセス許可を適用するを参照してください。

リフトアンドシフト

「7 R」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアンネス も参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティまたはプライバシーを侵害するように設計されているソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスにつながる

可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス がインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得します。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、 マネージドサービスの例です。これらは抽象化されたサービス とも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。このソフトウェアシステムは、加工品を現場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整のために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。詳細については、 AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

内の組織の一部である管理アカウント AWS アカウント を除くすべての AWS Organizations。アカウントが組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量の machine-to-machine (M2M) 通信プロトコル。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロ

イ、再利用可能なコード、回復力などがあります。詳細については、AWS 「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドへの移行のための強固な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、オペレーション、ビジネスアナリストと所有者、移行エンジニア、デベロッパー、スプリントに取り組む DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例には、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: Application Migration Service を使用して Amazon EC2 AWS への移行をリホストします。

Migration Portfolio Assessment (MPA)

AWS クラウドに移行するためのビジネスケースを検証するための情報を提供するオンラインツール。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイド を参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを AWS クラウドに移行するために使用されるアプローチ。詳細については、この用語集の「7 Rs エントリ」と「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定された

ギャップに対処するためのアクションプランが得られます。詳細については、AWS クラウドでのアプリケーションのモダナイゼーションの準備状況を評価するを参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、モノリスをマイクロサービスに分解する を参照してください。

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

変更可能なインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。Well-Architected AWS Framework では、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「 オペレーション統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業オートメーション用の machine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。詳細については、 AWS Well-Architected フレームワークの「運用準備状況レビュー (ORR)」を参照してください。

運用テクノロジー (OT)

産業運用、機器、インフラストラクチャを制御するために物理環境と連携するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 トランスフォーメーションの主要な焦点です。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイド を参照してください。

組織の証跡

の組織 AWS アカウント 内のすべての のすべてのイベントをログ AWS CloudTrail に記録する、によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウントに作成され、各アカウントのアクティビティを追跡します。詳細については、 ドキュメントの「組織の証跡の作成」を参照してください。 CloudTrail

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードから、このフレームワークは人材アクセラレーション と呼ばれます。詳細については、OCM ガイド を参照してください。

オリジンアクセスコントロール (OAC)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。OAC は、すべての のすべての S3 バケット AWS リージョン、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUTおよび DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。OAI を使用すると、 は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。OACも併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用技術」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されるネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

個人を特定できる情報を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

アクセス許可の定義 (アイデンティティベースのポリシー を参照) 、アクセス条件の指定 (リソースベースのポリシー を参照) 、または の組織内のすべてのアカウントに対する最大アクセス許可の定義 AWS Organizations (サービスコントロールポリシー を参照) が可能なオブジェクト。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行準備状況ガイド」を参照してください。

述語

`true` または を返すクエリ条件。`false`通常は `WHERE`句にあります。

述語のプッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、Implementing security controls on AWSのPreventative controlsを参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM ロール AWS アカウント、またはユーザーのルートユーザーです。詳細については、IAM ドキュメントのロールに関する用語と概念内にあるプリンシパルを参照してください。

プライバシーバイデザイン

エンジニアリングプロセス全体を通してプライバシーを考慮に入れたシステムエンジニアリングのアプローチ。

プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠のリソースのデプロイを防止するように設計されたセキュリティコントロール。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「 コントロールリファレンスガイド」および「 でのセキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長、成熟、縮小、削除まで、ライフサイクル全体にわたる製品のデータとプロセスの管理。

本番環境

「環境」を参照してください。

プログラミング可能ロジックコントローラー (NAL)

製造では、マシンをモニタリングし、承認プロセスを自動化する、信頼性が高く、適応性の高いコンピュータです。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES では、マイクロサービスは他のマイクロサービスがサブスクライブできるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

SQL リレーショナルデータベースシステムのデータにアクセスするために使用する手順などの一連のステップ。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設

定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

再構築

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 R」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の から分離され、独立しています。詳細については、AWS リージョン 「 を使用できるアカウントを指定する」を参照してください。

回帰

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 R」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 R」を参照してください。

プラットフォーム変更

「7 R」を参照してください。

再購入

「7 R」を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。で障害耐性を計画する場合、高可用性とディザスタリカバリが一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド 「レジリエンス」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任

(A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 R」を参照してください。

廃止

「7 R」を参照してください。

ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能により、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは にログイン AWS

Management Console したり AWS API オペレーションを呼び出したりでき、組織内のすべてのユーザーを IAM で作成する必要はありません。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視コントロールとデータ収集」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

では AWS Secrets Manager、暗号化された形式で保存されるパスワードやユーザー認証情報などの機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値は、バイナリ、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「シークレット」を参照してください。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、予防的 、検出的 、???応答的 、プロアクティブ の 4 つの主なタイプがあります。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポン

スアクションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先にあるデータの、それを受け取る AWS のサービス による暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS 全般のリファレンスの「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータ によって測定される、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、お客様はクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

「セキュリティ情報とイベント管理システム」を参照してください。

単一障害点 (SPOF)

システムを中断させる可能性のあるアプリケーションの単一の重要なコンポーネントの障害。

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

split-and-seed モデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、「」の「アプリケーションをモダナイズするための段階的アプローチ AWS クラウド」を参照してください。

SPOF

単一障害点 を参照してください。

star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用するように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズを参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視コントロールとデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと生産オペレーションをモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーインタラクションをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

T

タグ

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数 のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパター

ンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations とそのアカウントで組織内でタスクを実行するために指定するサービスへのアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 AWS Organizations を他の AWS のサービスで使用する AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 つのピザを食べることができる小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどのタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「書き込み 1 回」を参照し、多くの を読み取ります。

WQF

「AWS ワークロード認定フレームワーク」を参照してください。

Write Once, Read Many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャはイミュータブルな と見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性 を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

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。