AWS 決定ガイド

AWS CloudTrail または Amazon CloudWatch?

AWS CloudTrail または Amazon CloudWatch?: AWS 決定ガイド

Table of Contents

AWS CloudTrail または Amazon CloudWatch?

違いを理解し、自分に合ったものを選択する

目的	クラウド環境の可視性、セキュリティ、運用効率を維持するために、 AWS CloudTrail と Amazon CloudWatch のどちらが適切かを判断するのに役立ちます。
最終更新日	2024 年 9 月 20 日
対象サービス	• AWS CloudTrail • Amazon CloudWatch

序章

重要なビジネスワークロードを にデプロイするときは AWS クラウド、クラウド環境で可視性、セキュリティ、運用効率を維持することが重要です。対処すべき重要な領域がいくつかあります。

- 運用の透明性 — クラウド環境で誰が何をしているのかを追跡し、リソースのパフォーマンスをモニタリングします。
- セキュリティ保証 — セキュリティの脅威を示す可能性のある異常な API コールまたはリソース使用率を検出します。
- 規制コンプライアンス — 監査目的で、ユーザーアクティビティとインフラストラクチャの変更の詳細なログを維持します。
- パフォーマンス管理 — リソース使用率とアプリケーションパフォーマンスメトリクスのモニタリング。
- インシデント対応 — 運用上の問題をすばやく特定して対応するためのデータとアラート。
- コスト管理 — クラウド支出の管理に役立つリソースの使用状況に関するインサイト。
- 自動化 — 特定のイベントまたはパフォーマンスしきい値への自動応答。

AWS には、これらの問題に対処するのに役立つ 2 つの主要なサービスがあります。

- AWS CloudTrail は主にガバナンス、コンプライアンス、運用監査に焦点を当てています。 AWS 環境内で行われたすべての API コールがログに記録されます。主な特徴:

  - API コール、、 AWS マネジメントコンソール AWS SDKs、コマンドラインツール、その他の AWS サービスで実行されたアクションなど、すべての AWS アカウント アクティビティを追跡します。
  - 呼び出しを行ったユーザー、使用したサービス、影響を受けたリソースなど、すべてのアクションの詳細なログを提供します。
  - セキュリティ監査、ユーザーアクティビティの追跡、悪意のある可能性のあるアクションの特定に役立ちます。
- Amazon CloudWatch は、モニタリングおよびオブザーバビリティサービスであり AWS、オンプレミス、ハイブリッドのアプリケーションとインフラストラクチャのデータと実用的なインサイトを提供します。主な特徴は以下のとおりです。
  - メトリクス、ログ、アラームなど、 AWS で実行されている AWS リソースとアプリケーションをリアルタイムでモニタリングします。
  - システムパフォーマンス、エラー率、リソース使用率などに関する詳細なインサイトを提供します。
  - 特定の条件に基づいてアクション (リソースのスケーリングなど) をトリガーするアラームの設定を許可します。

どちらのサービスも堅牢で安全なクラウド環境にとって重要ですが、そのユースケースと機能はそれぞれ異なります。

これらのサービスの主な違いの概要を次に示します。

カテゴリ	CloudTrail	CloudWatch
主な目的	API アクティビティの追跡と監査	リアルタイムモニタリングとパフォーマンス管理
収集されるデータ	呼び出しを行ったユーザー、日時、影響を受けたリソースを含む API コールのログ	リソースのパフォーマンスとアプリケーションの動作に関連するメトリクス、ログ、イベント
ユースケース	環境におけるセキュリティ監査、コンプライアンス、変更の追跡	リソース使用率のモニタリング、アラームの設定、パフォーマンス管理

カテゴリ	CloudTrail	CloudWatch
セキュリティとコンプライアンス	詳細なアクティビティログを提供することで、セキュリティとコンプライアンスの要件を満たすのに役立ちます	セキュリティの異常についてシステムパフォーマンスをモニタリングし、運用の整合性を維持するのに役立ちます
ログの保持	過去 90 日間のイベント履歴。証跡とイベントデータストア (CloudTrail Lake を使用) を作成して、アクティビティの記録を 90 日以上保持できます。	リアルタイムのモニタリングとトラブルシューティングのための短期的なデータ保持
アラームと通知	主にアラームには使用されませんが、API アクティビティに基づいてアクションをトリガーできます	自動レスポンスを使用して、特定のメトリクスまたはログイベントのアラームの設定を有効にします
Integration	多くの場合、セキュリティ管理を強化するために AWS Config や IAM などのセキュリティサービスで使用されます。	幅広い AWS サービスと統合して包括的なモニタリングと自動化を実現
コストに関する考慮事項	生成および保存されたログの量に基づくコスト	モニタリングされるメトリクス、ログ、アラームの数に基づくコスト
データの詳細度	詳細な情報を含むすべての API コールの詳細なログを提供します。	リアルタイムモニタリング用の集計メトリクスとログデータを提供します
アクセスコントロール	ユーザーアクセス許可のアクセスパターンと変更を追跡できます	パフォーマンスメトリクスに基づいてリソースへのアクセスをモニタリングおよび最適化するのに役立ちます
リソースカバレッジ	AWS アカウント全体	個々の AWS リソース

カテゴリ	CloudTrail	CloudWatch
リアルタイム追跡	ほぼリアルタイム (5 分以内)	リアルタイムまたはほぼリアルタイム
視覚的表現	制限あり。他のツールでよく使用される	組み込みダッシュボードとグラフ作成

CloudTrail と CloudWatch の違い

CloudTrail と CloudWatch の違いについては、いくつかの主要分野をご覧ください。

Primary purpose

AWS CloudTrail

- 内のすべての API アクティビティの包括的な監査証跡を提供します AWS アカウント。誰が、いつ、どこで何をしたかを記録することに重点を置いています。これには、 AWS マネジメントコンソール、 AWS SDKs、コマンドラインツール、およびその他の AWS サービスを通じて実行されたアクションが含まれます。CloudTrail は、「誰がこの EC2 インスタンスを終了したか」などの質問に回答します。または「この IAM ポリシーにどのような変更が行われましたか？」

Amazon CloudWatch

- リソースとアプリケーションの動作 AWS 状態とパフォーマンスをモニタリングします。CloudWatch は、メトリクスの収集と追跡、ログファイルの収集とモニタリング、アラームの設定を行います。これは、アプリケーションのパフォーマンスを理解し、システム全体のパフォーマンスの変化に対応するのに役立ちます。CloudWatch はAmazon EC2 インスタンスの CPU 使用率が高すぎますか？」などの質問に回答します。または「Lambda 関数が生成するエラーの数」

[概要]

CloudTrail は、セキュリティとコンプライアンスに関するユーザーアクティビティの追跡と監査に役立ちますが、CloudWatch はシステムパフォーマンスと運用状態のモニタリングと最適化に

関するものです。どちらのツールも、クラウド環境の管理において、それぞれ異なるが補完的な役割を担います。

Data collected

AWS CloudTrail

- AWS 環境内のすべての API アクティビティの詳細なログのキャプチャに焦点を当てます。これには、API コールを行ったユーザー、実行日時、実行されたアクション、および関連するリソースに関する情報が含まれます。CloudTrail のログは、変更の追跡、コンプライアンスの確保、セキュリティインシデントの調査に不可欠な包括的な監査証跡を提供します。

Amazon CloudWatch

- AWS リソースとアプリケーションからパフォーマンスと運用データを収集します。これには、CPU 使用率、メモリ使用率、ネットワークトラフィック、アプリケーションログなどのメトリクスと、定義できるカスタムメトリクスが含まれます。CloudWatch によって収集されたデータは、リアルタイムのモニタリング、パフォーマンスの最適化、および特定の条件に基づいて自動アクションをトリガーするアラームの設定に使用されます。

[概要]

CloudTrail は監査とセキュリティの目的でユーザーアクティビティと API の使用に関連するデータを収集し、CloudWatch はメトリクスとログを収集してシステムパフォーマンスと運用状態をモニタリング、管理、最適化します。どちらも重要なインサイトを提供しますが、クラウド管理のさまざまな側面を提供します。

Use cases

AWS CloudTrail

- 主にセキュリティ監査、コンプライアンス、運用監査に使用されます。CloudTrail は、 AWS 環境内の API コールとユーザーアクティビティの詳細な記録を提供するため、変更の追跡、セキュリティインシデントの調査、組織が規制要件を満たしていることの確認に不可欠です。例えば、CloudTrail は、特定のリソースにアクセスしたユーザーをモニタリングしたり、設定に加えられた変更を追跡したり、複数の にわたるアクティビティを監査したりするシナリオに役立ちます AWS アカウント。

Amazon CloudWatch

- リアルタイムのモニタリング、パフォーマンス管理、運用効率を実現するように設計されています。CloudWatch は、メトリクス、ログ、イベントを収集して追跡することで、 AWS リソースとアプリケーションのヘルスをモニタリングするために使用されます。CloudWatch では、リソースのスケーリングや、特定のしきい値に達したときの通知の送信など、自動アクションをトリガーするアラームを設定できます。CloudWatch のユースケースには、アプリケーションのパフォーマンスのモニタリング、リソース使用率の管理、異常の検出、ダウンタイムを防ぐためにシステムが最適に動作していることの確認などがあります。

Security and compliance

AWS CloudTrail

- AWS 環境でセキュリティとコンプライアンスを維持する上で重要です。CloudTrail は、呼び出しの実行者、実行日時、実行されたアクションなど、すべての API コールの包括的な監査証跡を提供します。この詳細なログ記録は、コンプライアンス基準を満たし、セキュリティ監査を実施し、インシデントを調査するために不可欠です。ユーザーアクティビティとリソースの変更を追跡することで、CloudTrail は説明責任と透明性を確保するのに役立ちます。これは多くの規制フレームワークの主要な要件です。

Amazon CloudWatch

- 運用上の異常を検出できるようにすることで、セキュリティ上の役割を果たします。例えば、CloudWatch を使用して、ネットワークトラフィックの異常なスパイクや CPU 使用率など、潜在的なセキュリティ問題を示すメトリクスをモニタリングできます。さらに、CloudWatch は特定のしきい値に達したときにアラームと自動応答をトリガーできるため、プロアクティブなインシデント管理が可能になります。CloudWatch でキャプチャされたログは、セキュリティインシデントのコンテキストを理解するために不可欠な運用イベントを追跡するためにも使用できます。

[概要]

CloudTrail は、コンプライアンスに必要な監査ログを提供します。一方、CloudWatch は、セキュリティの脅威を検出して対応するのに役立つリアルタイムのモニタリングを提供し、安全で準拠したクラウド環境に貢献します。

Log retention

AWS CloudTrail

- デフォルトでは、CloudTrail イベント履歴には、アカウントの過去 90 日間の管理イベントが記録されます。
- ユーザーは、S3 バケットにログを無期限に保存するための証跡を作成できます。
- Amazon S3 に保存されているログの自動削除がないため、長期保存が可能です。
- ユーザーは S3 バケットにライフサイクルポリシーを実装して、長期ストレージコストを管理できます。
- CloudTrail は、より柔軟な保持オプションのために CloudWatch Logs にログを送信するように設定できます。

Amazon CloudWatch

- CloudWatch Logs のログ保持は、より柔軟で設定可能です。
- デフォルトの保持期間はロググループによって異なります。通常は「有効期限なし」に設定されます。
- ユーザーは、1 日から 10 年の範囲のカスタム保持期間を設定するか、無期限の保持を選択できます。
- 異なるロググループには、異なる保持期間を設定できます。
- 保持期間が過ぎると、ログは自動的に削除され、ストレージコストが管理されます。
- CloudWatch Logs は、必要に応じて Amazon S3 にエクスポートして長期保存できます。

Alarms and notifications

AWS CloudTrail

- 主に API アクティビティのログ記録に焦点を当てており、アラームや通知機能は組み込まれていません。ただし、CloudWatch Logs および CloudWatch アラームと統合してCloudTrail イベントのアラームを設定できます。通常、この設定は、不正アクセスの試みや重要なリソースの変更など、セキュリティ関連のイベントについて警告するために使用されます。

Amazon CloudWatch

- リアルタイムモニタリング用に特別に設計されており、堅牢なアラームおよび通知機能が含まれています。CloudWatch では、メトリクス、ログデータ、またはカスタム定義のしきい値に基づいてアラームを設定できます。これらのしきい値を超えると、CloudWatch は Amazon SNS (Amazon Simple Notification Service) 経由で通知を送信したり、インスタンスのスケーリ

ングなどの自動アクションをトリガーしたり、 を使用してカスタム修復ステップを実行したりできます AWS Lambda。これにより、CloudWatch はプロアクティブなシステム管理に不可欠なツールとなり、パフォーマンスの問題や運用上の異常が発生したときに警告します。

Integration

CloudTrail と CloudWatch は、他の AWS サービスや外部ツールとの広範な統合オプションを提供し、その機能とユーティリティを強化します。

CloudTrail 統合

- Amazon S3: ログを長期保存してアーカイブおよび分析する
- CloudWatch Logs: リアルタイムのログ分析とアラートを有効にする
- Amazon EventBridge: API イベントに基づいて自動アクションをトリガーする
- AWS Config: 設定の追跡とコンプライアンスのための入力を提供する
- AWS Security Hub CSPM: 一元化されたセキュリティ体制管理に貢献します
- AWS Lake Formation: CloudTrail ログのデータレイクガバナンスを有効にする
- Amazon Athena: Amazon S3 に保存されている CloudTrail ログに対して SQL クエリを実行する Amazon S3

CloudWatch 統合

- Amazon SNS: アラームとイベントの通知を送信する
- AWS Lambda: メトリクスまたはログに基づいてサーバーレス関数をトリガーする
- Amazon EC2 Auto Scaling: パフォーマンスメトリクスに基づいて容量を調整する
- AWS Systems Manager: CloudWatch データに基づいて運用タスクを自動化する
- AWS X-Ray: トレースデータと組み合わせて詳細なアプリケーションインサイトを得る
- コンテナサービス (Amazon ECS、Amazon EKS): コンテナ化されたアプリケーションをモニタリングする
- サードパーティー製ツール: メトリクスとログを外部モニタリングプラットフォームにエクスポートする

Cost considerations

AWS CloudTrail

- CloudTrail の料金は、主にログに記録および保存されるイベントの数に基づきます。デフォルトでは、CloudTrail イベント履歴は、アカウントの過去 90 日間の管理イベントを無料で記録して保存します。ただし、データイベント (S3 オブジェクトレベルのアクションなど) を有効にしたり、複数の証跡を作成したりすると、イベントの量と Amazon S3 に必要なストレージに基づいて料金が発生します。CloudTrail Insights などの高度な機能を使用すると、異常な API アクティビティをより詳細に分析できるため、追加コストが発生する可能性があります。

Amazon CloudWatch

- CloudWatch には、モニタリングするカスタムメトリクスの数、取り込まれて保存されたログイベントの数、アラームとダッシュボードの使用など、いくつかの要因に基づいてより複雑な料金構造があります。 AWS サービスの基本モニタリングは無料ですが、詳細なモニタリングとカスタムメトリクスには料金が発生します。ログストレージは、取り込まれて保持されるデータの量に基づいて料金が設定されますが、アラームの設定と保守、または高度なログ分析のための CloudWatch Logs Insights の使用には追加コストがかかります。

Data granularity

AWS CloudTrail

- CloudTrail は、 AWS 環境内で行われた個々の API コールをすべてログに記録することで、高粒度を提供します。各ログエントリには、リクエストの実行者、実行されたアクション、影響を受けるリソース、アクションの時刻などの詳細情報が含まれます。この詳細レベルは、特定のユーザーアクションと変更を正確な API コールまで追跡できるため、監査、セキュリティモニタリング、コンプライアンスに不可欠です。

Amazon CloudWatch

- CloudWatch は、モニタリングとパフォーマンス管理のための集約データに焦点を当てています。定期的に (通常は 1 分または 5 分ごとに) メトリクスを収集し、 AWS リソースから運用データをログに記録します。CloudWatch はシステムのパフォーマンスとアプリケーションの動作に関する詳細なインサイトを提供しますが、そのデータは CloudTrail と比較してより集約されます。例えば、個々のリクエストやアクションではなく、時間の経過に伴う平均 CPU 使用率をモニタリングできます。ただし、CloudWatch Logs は CloudTrail と同様のより詳細なデータを提供できますが、多くの場合、API コールを追跡するのではなく、運用ログの分析に使用されます。

Real-time tracking

AWS CloudTrail

- CloudTrail は本質的にリアルタイム追跡用に設計されていませんが、near-real-timeアラートを提供するように設定できます。デフォルトでは、CloudTrail は API アクティビティを記録しますが、ログ配信にはわずかな遅延があります。より迅速な追跡のために、CloudTrail を Amazon CloudWatch Events と統合したり AWS Lambda 、特定の API コールやアクティビティに基づいてログに記録されるとすぐにアクションをトリガーしたりできます。この設定により、重要なセキュリティイベントや設定変更をnear-real-timeモニタリングできます。

Amazon CloudWatch

- 一方、CloudWatch はシステムおよびアプリケーションのパフォーマンスをリアルタイムで追跡するために構築されています。 AWS リソースからのメトリクスを継続的にモニタリングし、事前定義されたしきい値を超えたときにアラームや通知を即座にトリガーできます。また、CloudWatch はログデータをリアルタイムで収集および分析するため、アプリケーションログのモニタリング、異常の検出、運用上の問題発生時の対応が可能になります。これにより、CloudWatch は AWS 環境のヘルスとパフォーマンスをリアルタイムで維持するための不可欠なツールになります。

使用アイテム

AWS CloudTrail と Amazon CloudWatch の選択基準について読んだので、ニーズに合ったサービスを選択し、以下の情報を使用してそれぞれの使用を開始できます。

AWS CloudTrail

- の開始方法 AWS CloudTrail

  AWS CloudTrail は、 の運用およびリスク監査、ガバナンス、コンプライアンスを有効にするのに役立つ AWS サービスです AWS アカウント。これを開始する方法は次のとおりです。

  ガイドを見る

- AWS アカウント アクティビティを確認する

  CloudTrail のイベント履歴機能 AWS アカウント を使用して、 で最近の AWS API アクティビティを確認する方法について説明します。

チュートリアルを使用する

- 証跡の作成

  データや Insights イベントを含むすべてのリージョンで AWS API アクティビティをログに記録する証跡を作成する方法について説明します。

  チュートリアルを使用する

- のセキュリティのベストプラクティス AWS CloudTrail

  このガイドでは、組織 AWS CloudTrail で を使用する際の検出的および予防的なセキュリティのベストプラクティスについて説明します。

  ガイドを見る

Amazon CloudWatch

- Amazon CloudWatch の開始方法

  Amazon CloudWatch を使用して、 AWS リソースと AWS で実行するアプリケーションをリアルタイムでモニタリングします。CloudWatch を使用してメトリクスを収集し、追跡できます。メトリクスとは、リソースやアプリケーションに関して測定できる変数です。

  ガイドを見る

- Amazon CloudWatch メトリクスの開始方法

  このガイドでは、基本モニタリングと詳細モニタリング、メトリクスのグラフ化方法、CloudWatch 異常検出の使用方法について説明します。

  ガイドを見る

- Amazon EKS と Kubernetes で Container Insights をセットアップする

  EKS クラスターで Amazon CloudWatch Observability ESK アドオンと ADTO を設定して、メトリクスを CloudWatch に送信します。また、CloudWatch Logs にログを送信するように Fluent Bit または Fluentd を設定する方法についても説明します。

  ガイドを見る

- Amazon CloudWatch Application Insights の開始方法

コンソールを使用して CloudWatch Application Insights がモニタリング用にアプリケーションを管理できるようにする方法について説明します。

ガイドを見る

- Container Insights の使用

  CloudWatch Container Insights がコンテナ化されたアプリケーションとマイクロサービスからメトリクスとログを収集、集約、要約する方法について説明します。

  ガイドを見る

- Amazon ECS での Container Insights のセットアップ

  クラスターとサービスレベルのメトリクスの設定、EC2 インスタンスレベルのメトリクスを収集するための ADOT のデプロイ、CloudWatch Logs にログを送信するように FireLens を設定する方法について説明します。

  ガイドを見る

AWS CloudTrail または Amazon CloudWatch のドキュメント履歴

次の表に、この決定ガイドの重要な変更点を示します。このガイドの更新に関する通知については、RSS フィードをサブスクライブできます。

変更	説明	日付
初回リリース	決定ガイドの初回リリース。	2024 年 9 月 20 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。