ユーザーガイド

AWS CloudTrail

Version 1.0

AWS CloudTrail: ユーザーガイド

Table of Contents

とは AWS CloudTrail?

AWS CloudTrail は、業務監査、リスク監査、ガバナンス、 AWS のサービス コンプライアンスを実現するのに役立つものです。 AWS アカウントユーザ、ロール、 AWS またはサービスが実行したアクションは、イベントとして記録されます。 CloudTrailイベントには、、、 AWS SDK AWS Management Console AWS Command Line Interface、API で実行されたアクションが含まれます。

CloudTrail AWS アカウント 作成時にアクティブになります。でアクティビティが発生すると AWS アカウント、 CloudTrail そのアクティビティはイベントに記録されます。

CloudTrail には、次の 3 つの方法でイベントを記録できます。

- [イベント履歴] - [イベント履歴] では、 AWS リージョン 内の過去 90 日間の管理イベントに関するレコードを表示、検索、ダウンロードできます。このレコードは変更できません。単一の属性でフィルタリングして、イベントを検索できます。アカウントの作成時に、[イベント履歴] へのアクセス権が自動的に付与されます。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。

  CloudTrail イベント履歴の閲覧には料金はかかりません。

- CloudTrail AWS CloudTrail Lake — Lake は、監査とセキュリティの目的でユーザーと API のアクティビティをキャプチャ、保存、アクセス、 AWS 分析するためのマネージドデータレイクです。 CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いたイベントのイミュータブルなコレクションです。イベントデータをイベントデータストアに保存できる期間は、[1 年間の延長可能な保存料金] オプションを選択した場合は最大 3,653 日 (約 10 年)、[7 年間の保存料金] オプションを選択した場合は最大 2,557 日 (約 7 年間) です。を使用して、 AWS アカウント 単一または複数のイベントデータストアを作成できます。 AWS アカウント AWS Organizations S3 CloudTrail バケットの既存の口グを既存または新しいイベントデータストアにインポートできます。Lake CloudTrail ダッシュボードでは上位のイベントトレンドを視覚化することもできます。詳細については、「AWS CloudTrail Lake の使用」を参照してください。

  CloudTrail Lake のイベントデータストアとクエリには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake でクエリを実行すると、スキャンされたデータ量に基

づいて料金が発生します。Lake CloudTrail コストの価格設定と管理について詳しくは、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

- 証跡 — AWS 記録はアクティビティの記録をキャプチャし、これらのイベントを Amazon S3 バケットに配信して保存します。オプションで CloudWatch Logs と Amazon への配信も可能です。EventBridgeこれらのイベントをセキュリティ監視ソリューションに入力できます。また、独自のサードパーティソリューションや Amazon Athena CloudTrail などのソリューションを使用してログを検索および分析することもできます。を使用して、1 AWS アカウント AWS アカウント つまたは複数のトレイルを作成できます。 AWS OrganizationsInsights イベントをログに記録して、異常な API 呼び出しの量とエラー率について管理イベントを分析できます。詳細については、「あなたのためのトレイルの作成 AWS アカウント」を参照してください。

  CloudTrail 証跡を作成することで、進行中の管理イベントのコピーを 1 つでも無料で S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。 CloudTrail 料金の詳細については、「AWS CloudTrail 料金表」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

AWS アカウントアクティビティを可視化することは、セキュリティと運用上のベストプラクティスの重要な側面です。 CloudTrail を使用して、 AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、対応することができます。誰または何がどのアクションを実行したか、どのリソースに対してアクションが実行されたか、いつイベントが発生したか、その他の詳細情報を特定できるため、 AWS アカウント内のアクティビティの分析と対応に役立ちます。

API CloudTrail を使用してアプリケーションに統合したり、組織の記録データストアやイベントデータストアの作成を自動化したり、作成したイベントデータストアや記録のステータスを確認したり、CloudTrail ユーザーによるイベントの表示方法を制御したりできます。

アクセス CloudTrail

CloudTrail では以下のいずれかの方法で作業できます。

トピック

- CloudTrail コンソール
- AWS CLI
- CloudTrail API
- AWS SDK

CloudTrail コンソール

AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。

CloudTrail コンソールには、 CloudTrail 次のような多くのタスクを実行するためのユーザーインターフェイスがあります。

- AWS アカウントの最近のイベントとイベント履歴を表示する。
- 過去 90 日間の管理イベントのフィルター処理済みまたは完全なファイルを、イベント履歴からダウンロードします。
- CloudTrail 記録の作成と編集。
- CloudTrail Lake イベントデータストアの作成と編集。
- イベントデータストアでのクエリの実行。
- CloudTrail 以下を含むトレイルの設定:
  - 証跡用の Amazon S3 バケットの選択。
  - プレフィックスの設定。
  - CloudWatch Logs への配信の設定。
  - AWS KMS キーを使用してトレイルデータを暗号化する。
  - ログファイル配信用の Amazon SNS 通知の証跡での有効化。
  - 証跡タグを追加および管理します。
- 以下を含む CloudTrail Lake イベントデータストアの設定：
  - CloudTrail イベントデータストアをパートナーや自社アプリケーションと統合して、外部ソースからのイベントを口グに記録する。 AWS
  - イベントデータストアをフェデレーションして Amazon Athena からクエリを実行する。
  - AWS KMS キーを使用してイベントデータストアデータを暗号化する。
  - イベントデータストアでのタグの追加および管理。

の詳細については AWS Management Console、を参照してくださいAWS Management Console。

AWS CLI

AWS Command Line Interface は、 CloudTrail コマンドラインから操作できる統合ツールです。詳細については、『AWS Command Line Interface ユーザーガイド』を参照してください。 CloudTrail

CLI コマンドの完全なリストについては、『コマンドリファレンス』の cloudtrail と cloudtrail-data を参照してください。AWS CLI

CloudTrail API

コンソールと CLI に加えて、 CloudTrail RESTful API CloudTrail を使用して直接プログラミングすることもできます。詳細については、API リファレンスと CloudTrail-Data AWS CloudTrail API リファレンスを参照してください。

AWS SDK

CloudTrail API を使用する代わりに、いずれかの AWS SDK を使用することもできます。各 SDK は、各種のプログラミング言語とプラットフォームに対応したライブラリやサンプルコードで構成されています。SDK を使用すると、へのプログラムによるアクセスを簡単に作成できます。CloudTrail例えば、SDK では、暗号を使用してリクエストに署名したり、エラーを管理したり、リクエストを自動的に再試行したりできます。詳細については、「構築するツール」ページを参照してください。 AWS

CloudTrail 仕組み

を作成すると、 CloudTrail 自動的にイベント履歴にアクセスできるようになります AWS アカウント。[イベント履歴] では、 AWS リージョンで過去 90 日間に記録された 管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。

AWS アカウント 過去 90 日間のイベントを継続的に記録するには、トレイルまたは CloudTrail Lake イベントデータストアを作成します。

トピック

- CloudTrail イベント履歴
- CloudTrail レイクデータストアとイベントデータストア
- CloudTrail トレイル
- CloudTrail インサイトイベント
- CloudTrail チャネル

CloudTrail イベント履歴

過去 90 日間の管理イベントは、 CloudTrail イベント履歴ページに移動するとコンソールで簡単に確認できます。aws cloudtrail lookup-events コマンド、または LookupEvents API 操作を実行してイベント履歴を表示することもできます。イベント履歴内のイベントは、単一の属性でイベントをフィルタリングすることによって検索できます。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。

[イベント履歴] はアカウント内に存在する証跡やイベントデータストアには接続されておらず、証跡やイベントデータストアに加えた設定変更の影響も受けません。

CloudTrail **lookup-events**イベント履歴ページの閲覧やコマンドの実行には料金はかかりません。

CloudTrail レイクデータストアとイベントデータストア

イベントデータストアを作成して、CloudTrail イベント (管理イベント、データイベント)、CloudTrailInsights イベント、AWS Audit Manager 証拠、AWS Config 構成項目、または外部のイベントをログに記録できます AWS。

イベントデータストアは AWS リージョン、 AWS リージョン AWS アカウント内の現在のイベントまたはすべてのイベントをログに記録できます。外部からの統合イベントの記録に使用するイベントデータストアは、1 AWS つのリージョンのみを対象とする必要があります。マルチリージョンのイベントデータストアにすることはできません。

に組織を作成した場合は AWS Organizations、 AWS その組織内のすべてのアカウントのすべてのイベントを記録する組織イベントデータストアを作成できます。組織のイベントデータストアを、すべての AWS リージョンまたは現在のリージョンに適用できます。組織のイベントデータストアは管理アカウントまたは委任された管理者アカウントで作成する必要があり、組織への適用として指定した場合は、組織内のすべてのメンバーアカウントに自動的に適用されます。メンバーアカウントは、組織のイベントデータストアを表示することも、これを変更または削除することもできません。組織のイベントデータストアは、外部からのイベントの収集には使用できません AWS。詳細については、「組織のイベントデータストア」を参照してください。

デフォルトでは、イベントデータストア内のすべてのイベントはによって暗号化されます CloudTrail。イベントデータストアを設定する際、独自のデータストアを使用することを選択できます AWS KMS key。独自の KMS キーを使用すると、 AWS KMS 暗号化と復号化にコストがかかります。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。詳細については、「 CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)」を参照してください。

次の表は、イベントデータストアで実行できるタスクに関する情報を示しています。

タスク	説明
Lake ダッシュボードを表示します。	CloudTrail Lake ダッシュボードを使用して、管理イベント、S3 データイベント、または Insights イベントを収集するイベントデータストア内のイベントを視覚化できます。
ログ管理イベント	読み取り専用、書き込み専用、またはすべての管理イベントをログに記録するようにイベントデータストアを設定します。デフォルトでは、イベントデータには管理イベントのログが保存されます。
ログデータイベント	データイベントをログに記録するようにイベントデータストアを設定します。高度なイベントセレクターを使用して、、`readOnly`、`resources.ARN` およびフィールドを絞り込んで`eventName` 、関心のあるイベントのみを記録できます。
Insights イベントをログに記録する	Insights イベントをログ記録するようにイベントデータストアを設定し、管理 API コールに関連する異常なアクティビティを特定し応答できるようにします。詳細については、「Insights イベントのログ記録」を参照してください。 Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。
トレイルイベントをコピーする	トレイルイベントを新規または既存のイベントデータストアにコピーして、 point-in-time トレイルに記録されたイベントのスナップショットを作成できます。
イベントデータストアでフェデレーションを有効にします。	イベントデータストアをフェデレートして、データカタログ内のイベントデータストアに関連付けられたメタデータを確認し、Amazon Athena を使用してイベントデータに対して SQL クエリを実行できます。 AWS Glue AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエン

タスク	説明
	ジンは、クエリするデータを検索、読み取り、処理する方法を知ることができます。
イベントデータストアへのイベント取り込みを停止または開始します。	CloudTrail 管理イベント、データイベント、 AWS Config または構成項目を収集するイベントデータストアでのイベント取り込みを停止または開始できます。
外部のイベントソースとのインテグレーションを作成します。 AWS	CloudTrail Lakeインテグレーションを使用すると、オンプレミスやクラウド、仮想マシン、コンテナでホストされている社内アプリケーションやSaaSアプリケーション、仮想マシン、コンテナなど、ハイブリッド環境のあらゆる外部ソースからのユーザーアクティビティデータを記録して保存できます。 AWS利用可能なインテグレーションパートナーについては、「Lake インテグレーション」を参照してくださいAWS CloudTrail 。
Lake のサンプルクエリをコンソールに表示します。 CloudTrail	CloudTrail コンソールには、独自のクエリの作成を始めるのに役立つサンプルクエリが多数用意されています。
クエリを作成または編集します。	CloudTrail のクエリは SQL で作成されています。 CloudTrail Lake Editor タブでクエリを作成するには、SQL でクエリを一から記述するか、保存済みクエリまたはサンプルクエリを開いて編集します。
クエリ結果を S3 バケットに保存します。	クエリの実行後に、クエリ結果をS3 バケットに保存できます。
保存したクエリ結果をダウンロードする	保存した CloudTrail Lake クエリ結果を含む CSV ファイルをダウンロードできます。
保存したクエリ結果を検証します。	CloudTrail クエリ結果の整合性検証を使用して、クエリ結果が S3 CloudTrail バケットに配信された後に、クエリ結果が変更されたか、削除されたか、または変更されていないかを判断できます。

CloudTrail Lake の詳細については、を参照してくださいAWS CloudTrail Lake の使用。

CloudTrail Lake のイベントデータストアとクエリには料金がかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake でクエリを実行すると、スキャンされたデータ量に基づいて料金が発生します。Lake CloudTrail コストの価格設定と管理について詳しくは、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

CloudTrail トレイル

証跡とは、指定した Amazon S3 バケットにイベントを配信できる設定のことです。また、Amazon CloudWatch ログと Amazon を使用して、イベントをトレイルに配信して分析することもできます EventBridge。

トレイルでは、 CloudTrail 管理イベント、データイベント、および Insights イベントをログに記録できます。

には、マルチリージョントレイルとシングルリージョントレイルの 2 種類のトレイルを作成できます AWS アカウント。

マルチリージョントレイル

マルチリージョントレイルを作成すると、 CloudTrail AWS リージョン AWS 作業しているパーティションのすべてのイベントが記録され、指定した S3 CloudTrail バケットにイベントログファイルが配信されます。マルチリージョントレイルを作成した後にを追加すると、その新しいリージョンが自動的に含まれ、そのリージョンのイベントが記録されます。 AWS リージョン マルチリージョンの証跡を作成すると、アカウント内のすべてのリージョンでのアクティビティを把握できるため、推奨されるベストプラクティスとなります。 CloudTrail コンソールを使用して作成したトレイルはすべてマルチリージョンです。単一リージョンのトレイルをマルチリージョンのトレイルに変換するには、を使用します。 AWS CLI詳細については、「コンソールで証跡を作成する」および「1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用」を参照してください。

単一リージョントレイル

単一リージョントレイルを作成すると、 CloudTrail そのリージョンのイベントのみを記録します。次に、指定した Amazon S3 CloudTrail バケットにイベントログファイルを配信します。AWS CLIを使用する際は、単一のリージョンの証跡のみを作成することができます。さらに 1 つの証跡を作成すると、それらの証跡から同じ S3 CloudTrail バケットまたは別のバケットにイベントログファイルを配信できます。 AWS CLI または API を使用してトレイルを作成する場合の

デフォルトオプションです。 CloudTrail 詳細については、「を使用した証跡の作成、更新、管理 AWS CLI」を参照してください。

> **Note**
>
> どちらのタイプの証跡でも、任意のリージョンから Amazon S3 バケットを指定できます。

で組織を作成した場合は AWS Organizations、 AWS その組織内のすべてのアカウントのすべてのイベントを記録する組織証跡を作成できます。 AWS 組織証跡はすべての地域に適用することも、現在の地域に適用することもできます。組織の証跡は管理アカウントまたは委任された管理者アカウントで作成する必要があり、組織への適用として指定されている場合は、組織内のすべてのメンバーアカウントに自動的に適用されます。メンバーアカウントは組織記録を確認できますが、変更や削除はできません。デフォルトでは、メンバーアカウントは Amazon S3 バケット内にある組織の証跡のログファイルにアクセスできません。

デフォルトでは、 CloudTrail コンソールで記録を作成すると、イベントログファイルは KMS キーで暗号化されます。SSE-KMS 暗号化を有効にしない場合、イベントログは Amazon S3 サーバー側暗号化 (SSE) を使用して暗号化されます。 バケットにログファイルを任意の期間、保存することができます。また、Amazon S3 ライフサイクルのルールを定義して、自動的にログファイルをアーカイブまたは削除することもできます。ログファイルの配信と確認に関する通知が必要な場合は、Amazon SNS 通知を設定できます。

CloudTrail ログファイルを 1 時間に複数回、約 5 分おきに発行します。これらのログファイルには、 CloudTrailサポートしているアカウントのサービスからの API 呼び出しが含まれています。詳細については、「CloudTrail がサポートするサービスと統合」を参照してください。

> **Note**
>
> CloudTrail 通常、API 呼び出しから平均約 5 分以内にログが配信されます。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。
> トレイルの設定を誤ると (S3 バケットにアクセスできないなど)、ログファイルを S3 バケットに 30 日間再配信しようとしますが、 CloudTrail attempted-to-deliver これらのイベントには標準料金が適用されます。 CloudTrail 証跡の不適切な設定による課金を避けるには、その証跡を削除する必要があります。
> CloudTrail ユーザーが直接行ったアクション、またはユーザーに代わってサービスが行ったアクションをキャプチャします。 AWS たとえば、 AWS CloudFormation `CreateStack`呼

び出しによって、Amazon EC2、Amazon RDS、Amazon EBS、またはテンプレートで要求されるその他のサービスへの追加の AWS CloudFormation API 呼び出しが発生する可能性があります。この動作は正常であり、想定されています。 AWS アクションがサービスによって実行されたかどうかは、invokedbyイベントのフィールドで確認できます。 CloudTrail

次の表は、トレイルで実行できるタスクに関する情報を示しています。

タスク	説明
管理イベントのロギング	読み取り専用、書き込み専用、またはすべての管理イベントをログに記録するようにトレイルを設定します。
データイベントをログに記録する	高度なイベントセレクターを使用すると、対象のデータイベントのみを記録する詳細なセレクターを作成できます。高度なイベントセレクターを使用すると、eventName フィールドをフィルタリングして特定の API 呼び出しのロギングを含めたり除外したりできるため、コスト管理に役立ちます。
Insights イベントをログに記録する	管理 API コールに関連する異常なアクティビティを特定して応答できるように、インサイトイベントを記録するように証跡を設定します。 Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。
インサイトイベントを表示する	CloudTrail トレイルでインサイトを有効にすると、 CloudTrail コンソールまたはを使用して、最大 90 日間のインサイトイベントを表示できます AWS CLI。

タスク	説明
インサイトイベントをダウンロードする	CloudTrail トレイルでインサイトを有効にすると、過去 90 日間のトレイルのインサイトイベントを含む CSV または JSON ファイルをダウンロードできます。
トレイルイベントを CloudTrail Lake にコピーします。	既存のトレイルイベントを CloudTrail Lake イベントデータストアにコピーして、 point-in-time トレイルに記録されたイベントのスナップショットを作成できます。
Amazon SNS トピックを作成してサブスクライブする	バケットへのログファイルの配信に関する通知を受信するにはトピックを受信登録します。Amazon SNS は、Amazon Simple Queue Service でのプログラムによる通知を含む複数の方法で通知できます。 **Note** すべてのリージョンのログファイル配信に関する SNS 通知を受信するときは、証跡の SNS トピックを 1 つのみ指定します。すべてのイベントをプログラムで処理する場合は、「CloudTrail 処理ライブラリを使用する」を参照してください。
ログファイルを表示する。	S3 バケットからログファイルを検索してダウンロードします。

タスク	説明
CloudWatch Logs を使用してイベントをモニタリングします。	CloudWatch イベントをログに送信するようにトレイルを設定できます。その後、 CloudWatch Logs を使用して特定の API 呼び出しやイベントがないかアカウントを監視できます。 **Note** CloudWatch すべてのリージョンに適用される証跡をロググループに送信するように設定すると、 CloudTrail すべてのリージョンのイベントが 1 つのロググループに送信されます。
ログ暗号化を有効にします。	ログファイルの暗号化は、ログファイルに追加のセキュリティレイヤーを提供します。
ログファイルの整合性を有効にする	ログファイルの整合性検証は、 CloudTrail ログファイルが配信されてから変更されていないことを確認するのに役立ちます。
ログファイルを他のユーザーと共有できます。 AWS アカウント	アカウント間でログファイルを共有することができます。
複数のアカウントからのログを集約する	複数のアカウントからのログファイルを単一のバケットに集約できます。
パートナーソリューションとの連携	CloudTrail と統合できるパートナーソリューションでアウトプットを分析しましょう。 CloudTrailパートナーソリューションでは、変更の追跡、トラブルシューティング、セキュリティ分析などの幅広い機能セットが提供されます。

CloudTrail 証跡を作成することで、進行中の管理イベントのコピーを 1 つでも無料で S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。 CloudTrail 料金の詳細について

は、「AWS CloudTrail 料金表」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail インサイトイベント

AWS CloudTrail インサイトは、 CloudTrail 管理イベントを継続的に分析することで、 AWS ユーザーが API 呼び出しや API エラー率に関連する異常なアクティビティを特定して対応するのに役立ちます。 CloudTrail Insights は、API 呼び出し量と API エラー率の通常のパターン (ベースラインとも呼ばれる) を分析し、呼び出し量またはエラー率が通常のパターンから外れると Insights イベントを生成します。API コール量に関する Insights イベントは、`write` 管理 API に対して生成されます。一方、API エラー率に関する Insights イベントは、`read` と `write` の両方の管理 API に対して生成されます。

デフォルトでは、 CloudTrail トレイルとイベントデータストアは Insights イベントを記録しません。Insights イベントを口グに記録するようにトレイルまたはイベントデータストアを設定する必要があります。詳細については、「でインサイトイベントを口ギングする AWS Management Console」および「を使用してインサイトイベントを口ギングする AWS Command Line Interface」を参照してください。

Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。

トレイルとイベントデータストアの Insights イベントの表示

CloudTrail トレイルとイベントデータストアの両方の Insights イベントをサポートしていますが、Insights イベントの表示方法やアクセス方法にはいくつか違いがあります。

証跡の Insights イベントの表示

トレイルで Insights イベントを有効にしていて、 CloudTrail 異常なアクティビティが検出された場合、Insights イベントはトレイルの送信先 S3 バケット内の別のフォルダーまたはプレフィックスに記録されます。 CloudTrail コンソールで Insights イベントを表示すると、インサイトのタイプとインシデント期間を確認することもできます。詳細については、「トレイルの CloudTrail Insights イベントをコンソールに表示する CloudTrail 」を参照してください。

トレイルで初めて CloudTrail Insights を有効にしてから、異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントが配信されるまでに最大 36 時間かかることがあります。

イベントデータストアの Insights イベントの表示

CloudTrail Lake で Insights イベントを記録するには、Insights イベントを記録する送信先イベントデータストアと、Insights を有効にして管理イベントをログに記録するソースイベントデータストアが必要です。詳細については、「コンソールを使用して CloudTrail Insights イベントのイベントデータストアを作成する」を参照してください。

ソースイベントデータストアで初めて CloudTrail Insights を有効にしてから、異常なアクティビティが検出された場合、最初の Insights CloudTrail イベントが宛先イベントデータストアに配信されるまでに最大 7 日かかることがあります。

ソースイベントデータストアで CloudTrail Insights を有効にしていて、 CloudTrail 異常なアクティビティを検出すると、Insights CloudTrail イベントが送信先のイベントデータストアに配信されます。その後、送信先イベントデータストアにクエリを実行して Insights イベントに関する情報を取得し、オプションでクエリ結果を S3 バケットに保存できます。詳細については、「クエリを作成または編集する」および「 CloudTrail コンソールにサンプルクエリが表示されます。」を参照してください。

Insights Events ダッシュボードを表示して、送信先イベントデータストア内の Insights イベントを視覚化できます。Lake ダッシュボードの詳細については、「 CloudTrail Lake ダッシュボードを表示する」を参照してください。

CloudTrail チャネル

CloudTrail 次の 2 種類のチャネルをサポートします。

外部のイベントソースとの CloudTrail Lake 統合用チャネル AWS

CloudTrail Lakeはチャネルを使用して CloudTrail、 AWS CloudTrail 外部から協力してくれる外部パートナーや独自のソースからLakeにイベントを持ち込みます。チャネルを作成するときは、チャネルソースから送信されるイベントを保存するイベントデータストアを 1 つまたは複数選択します。送信先イベントデータストアがアクティビティイベントをログ記録するように設定している間は、必要に応じてチャネルの送信先イベントデータストアを変更できます。外部パートナーからのイベント用のチャネルを作成するときは、パートナーまたはソースアプリケーションにチャネル ARN を提供します。チャネルにアタッチされたリソースポリシーにより、ソースはチャネルを介してイベントを送信できます。詳細については、「AWS CloudTrail API リファレンス」の「外部のイベントソースとの統合を作成 AWS」および「`CreateChannel`」を参照してください。

サービスにリンクされたチャネル

AWS サービスは、 CloudTrail ユーザーに代わってイベントを受信するサービスにリンクされたチャネルを作成できます。 AWS サービスにリンクされたチャンネルを作成するサービスは、

チャンネルの高度なイベントセレクターを設定し、チャンネルをすべてのリージョンに適用するのか、現在のリージョンに適用するのかを指定します。

CloudTrail コンソールを使用したり、AWS CLI CloudTrail によって作成されたサービスにリンクされたチャネルに関する情報を表示したりできます。 AWS のサービス

CloudTrail の概念

このセクションでは、 に関連する基本概念をまとめます CloudTrail。

概念：

- CloudTrail イベント
- イベント履歴
- 追跡
- 組織の証跡
- CloudTrail Lake およびイベントデータストア
- CloudTrail インサイト
- タグ
- AWS Security Token Service および CloudTrail
- グローバルサービスイベント

CloudTrail イベント

のイベント CloudTrail は、 AWS アカウント内のアクティビティの記録です。このアクティビティは、IAM アイデンティティによって実行されるアクション、または によってモニタリング可能なサービスにすることができます CloudTrail。 CloudTrail イベントは、、 AWS SDKs AWS Management Console、コマンドラインツール、およびその他の AWS サービスを通じて行われた API と非 API アカウントアクティビティの両方の履歴を提供します。

CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序では表示されません。

CloudTrail は 3 種類のイベントを記録します。

- 管理イベント

- データイベント
- Insights イベント

すべてのイベントタイプは CloudTrail JSON ログ形式を使用します。

デフォルトでは、証跡とイベントデータストアは管理イベントをログ記録しますが、データイベントまたは Insights イベントは記録しません。

と AWS のサービス の統合方法については、 CloudTrail「」を参照してくださいAWS のサービストピック CloudTrail。

管理イベント

管理イベントは、 AWS アカウントのリソースで実行される管理オペレーションに関する情報を提供します。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。

管理イベントには、次のようなものがあります。

- セキュリティの設定 (API AWS Identity and Access Management `AttachRolePolicy`オペレーションなど)。
- デバイスの登録 (例: Amazon EC2 `CreateDefaultVpc` API オペレーション)。
- データをルーティングするルールの設定 (例: Amazon EC2 `CreateSubnet` API オペレーション)。
- ログ記録の設定 (API AWS CloudTrail `CreateTrail`オペレーションなど)。

管理イベントは、アカウントで発生する非 API イベントを含む場合もあります。例えば、ユーザーがアカウントにサインインすると、 は`ConsoleLogin`イベントを CloudTrail ログに記録します。詳細については、「によってキャプチャされた非APIイベント CloudTrail」を参照してください。

デフォルトでは、 CloudTrail 証跡と CloudTrail Lake イベントデータストアは管理イベントをログに記録します。管理イベントのログ記録の詳細については、「」を参照してください管理イベントのログ記録。

データイベント

データイベントでは、リソース上またはリソース内で実行されたリソースオペレーションについての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。

データイベントには、次のようなものがあります。

- S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (GetObject、DeleteObject、および PutObject API オペレーションなど) 。 S3
- AWS Lambda 関数実行アクティビティ (InvokeAPI)。
- CloudTrail PutAuditEvents 外部からのイベントをログに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。
- トピックに関する Amazon SNS Publish および PublishBatch API オペレーション。

証跡およびイベントデータストアで使用できるデータイベントタイプは、以下の表のとおりです。[データイベントタイプ (コンソール)] 列には、コンソールで有効な選択項目が表示されます。resources.type 値列には、 AWS CLI または CloudTrail APIs を使用して証跡またはイベントデータストアにそのタイプのデータイベントを含めるように指定するresources.type値が表示されます。

証跡では、基本イベントセレクタまたはアドバンストイベントセレクタを使用して、Amazon S3 オブジェクト、Lambda 関数、DynamoDB テーブル (テーブルの最初の 3 行に表示) のデータイベントをログ記録できます。残りの行に表示されるデータイベントタイプをログに記録するには、高度イベントセレクタのみを使用できます。

イベントデータストアの場合、データイベントを含めるには、詳細イベントセレクタのみを使用できます。

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon DynamoDB	テーブルに対する Amazon DynamoDB 項目レベルの API アクティビティ (、DeleteItem 、および UpdateItem API PutItemオペレーションなど) 。	DynamoDB	AWS::DynamoDB::Table

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	Note ストリームが有効になっているテーブルの場合、データイベントの `resources` フィールドには `AWS::DynamoDB::Stream` と `AWS::DynamoDB::Table` の両方が含まれます。`resources.type` に `AWS::DynamoDB::Table` を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方がログ記録されます。ストリームイベント を除外		

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	するには、eventName フィールドにフィルターを追加します。		
AWS Lambda	AWS Lambda 関数実行アクティビティ (InvokeAPI)。	Lambda	AWS::Lambda::Function
Amazon S3	S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (GetObject 、DeleteObject 、および PutObject API オペレーションなど)。 S3	S3	AWS::S3::Object
AWS AppConfig	StartConfiguration Session および への呼び出しなどの設定オペレーションの AWS AppConfig API アクティビティGetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS B2B データ交換	`GetTransformerJob` および `StartTransformerJob` の呼び出しなど、Transformer 操作用の B2B データ交換 API アクティビティ。	B2B データ交換	`AWS::B2BI::Transformer`
Amazon Bedrock	エージェントエイリアスでの Amazon Bedrock API アクティビティ。	Bedrock エージェントエイリアス	`AWS::Bedrock::AgentAlias`
	ナレッジベースでの Amazon Bedrock API アクティビティ。	Bedrock ナレッジベース	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront での API アクティビティKeyValueStore。	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	名前空間 での AWS Cloud Map API アクティビティ。	AWS Cloud Map 名前空間	`AWS::ServiceDiscovery::Namespace`
	サービス での AWS Cloud Map API アクティビティ。	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS CloudTrail	CloudTrail PutAuditEvents 外部からのイベントをログに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。	CloudTrail チャンネル	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	カスタマイズに対する Amazon CodeWhisperer API アクティビティ。	CodeWhisperer カスタマイズ	`AWS::CodeWhisperer::Customization`
	プロファイルの Amazon CodeWhisperer API アクティビティ。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito アイデンティティプール に対する Amazon Cognito API アクティビティ。	Cognito アイデンティティプール	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	ストリームに対する Amazon DynamoDB API アクティビティ	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Elastic Block Store	Amazon EBS スナップショットの PutSnapshotBlock 、GetSnapshotBlock 、および ListChangedBlocks などの Amazon Elastic Block Store (EBS) ダイレクト API。	Amazon EBS ダイレクト API	AWS::EC2::Snapshot
Amazon EMR	ログ先行書き込みワークスペースでの Amazon EMR API アクティビティ。	EMR ログ先行書き込みワークスペース	AWS::EMRWAL::Workspace
Amazon FinSpace	環境に対する Amazon FinSpace API アクティビティ。	FinSpace	AWS::FinSpace::Environment

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS Glue	AWS Glue Lake Formation によって作成されたテーブルに対する API アクティビティ。 **Note** AWS Glue テーブルのデータイベントは現在、次のリージョンでのみサポートされています。 • 米国東部 (バージニア北部) • 米国東部 (オハイオ) • 米国西部 (オレゴン) • 欧州 (アイルランド) • アジアパシフィック (東京) リージョン	Lake Formation	`AWS::Glue::Table`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon GuardDuty	ディテクター の Amazon GuardDuty API アクティビティ。https://docs.aws.amazon.com/guardduty/latest/ug/logging-using-cloudtrail.html#guardduty-data-events-in-cloudtrail	GuardDuty ディテクター	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging データストアでの API アクティビティ。	医療用画像データストア	`AWS::MedicalImaging::Datastore`
AWS IoT	証明書 に対する AWS IoT API アクティビティ。	IoT 証明書	`AWS::IoT::Certificate`
	モノに対する AWS IoT API アクティビティ。	IoT モノ	`AWS::IoT::Thing`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS IoT Greengrass Version 2	コンポーネントバージョンの Greengrass コアデバイスからの Greengrass API アクティビティ。 Note Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass コンポーネントバージョン	`AWS::GreengrassV2::ComponentVersion`
	デプロイ上の Greengrass コアデバイスからの Greengrass API アクティビティ。 Note Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass デプロイ	`AWS::GreengrassV2::Deployment`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS IoT SiteWise	アセット での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_CreateAsset.html	IoT SiteWise アセット	`AWS::IoTSiteWise::Asset`
	時系列 での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_DescribeTimeSeries.html	IoT SiteWise 時系列	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	エンティティ での IoT TwinMaker API アクティビティ。 https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateEntity.html	IoT TwinMaker エンティティ	`AWS::IoTTwinMaker::Entity`
	ワークスペース での IoT TwinMaker API アクティビティ。 https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateWorkspace.html	IoT TwinMaker ワークスペース	`AWS::IoTTwinMaker::Workspace`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Kendra インテリジェントランキング	リスコア実行プラン に対する Amazon Kendra Intelligent Ranking API アクティビティ。	Kendra ランキング	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra 向け)	テーブルでの Amazon Keyspaces API アクティビティ。	Cassandra テーブル	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	ストリーム での Kinesis Data Streams API アクティビティ。	Kinesis ストリーム	`AWS::Kinesis::Stream`
	ストリームコンシューマー での Kinesis Data Streams API アクティビティ。	Kinesis ストリームコンシューマー	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	`GetMedia` や への呼び出しなど、ビデオストリーム での Kinesis Video Streams API アクティビティ`PutMedia`。	Kinesis ビデオストリーム	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	ネットワーク上の Amazon Managed Blockchain API アクティビティ。	Managed Blockchain ネットワーク	`AWS::ManagedBlockchain::Network`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	`eth_getBalance` や `eth_getBlockByNumber` などの Ethereum ノードに対する Amazon Managed Blockchain JSON-RPC コール。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune Graph	Neptune Graph でのクエリ、アルゴリズム、ベクトル検索などのデータ API アクティビティ。	Neptune Graph	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Connector for Active Directory API アクティビティ。	AWS Private CA Connector for Active Directory	`AWS::PCAConnectorAD::Connector`
Amazon Q アプリ	Amazon Q Apps での Data API アクティビティ。	Amazon Q アプリ	`AWS::QApps:QApp`
Amazon Q Business	アプリケーション上の Amazon Q Business API アクティビティ。	Amazon Q Business アプリケーション	`AWS::QBusiness::Application`
	データソース上の Amazon Q Business API アクティビティ。	Amazon Q Business データソース	`AWS::QBusiness::DataSource`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	インデックスでの Amazon Q Business API アクティビティ。	Amazon Q Business インデックス	`AWS::QBusiness::Index`
	ウェブエクスペリエンスでの Amazon Q Business API アクティビティ。	Amazon Q Business ウェブエクスペリエンス	`AWS::QBusiness::WebExperience`
Amazon RDS	DB クラスターでの Amazon RDS API アクティビティ。	RDS Data API - DB クラスター	`AWS::RDS::DBCluster`
Amazon S3	アクセスポイントでの Amazon S3 API アクティビティ。	S3 アクセスポイント	`AWS::S3::AccessPoint`
	Amazon S3 Object Lambda アクセスポイント API アクティビティ 、 `CompleteMultipartUpload` や への呼び出しなど`GetObject` 。	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts オブジェクトレベル API アクティビティ。	S3 Outposts	`AWS::S3Outposts::Object`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon SageMaker	エンドポイントでの Amazon SageMaker InvokeEndpointWithResponseStream アクティビティ。	SageMaker エンドポイント	AWS::SageMaker::Endpoint
	特徴量ストアでの Amazon SageMaker API アクティビティ。	SageMaker 特徴量ストア	AWS::SageMaker::FeatureGroup
	実験トライアルコンポーネント での Amazon SageMaker API アクティビティ。 https://docs.aws.amazon.com/sagemaker/latest/dg/experiments-monitoring.html	SageMaker メトリクス実験トライアルコンポーネント	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	プラットフォームエンドポイントでの Amazon SNS Publish API オペレーション。	SNS プラットフォームエンドポイント	AWS::SNS::PlatformEndpoint
	トピックに関する Amazon SNS Publish および PublishBatch API オペレーション。	SNS トピック	AWS::SNS::Topic

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon SQS	メッセージでの Amazon SQS API アクティビティ。	SQS	`AWS::SQS::Queue`
AWS Step Functions	ステートマシンでの Step Functions API アクティビティ。	Step Functions ステートマシン	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain インスタンスでの API アクティビティ。	サプライチェーン	`AWS::SCN::Instance`
Amazon SWF	ドメイン での Amazon SWF API アクティビティ。 https://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dev-domains.html	SWF ドメイン	`AWS::SWF::Domain`
AWS Systems Manager	コントロールチャネルでの Systems Manager API アクティビティ。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	マネージドノードでの Systems Manager API アクティビティ。	Systems Manager マネージドノード	`AWS::SSM::ManagedNode`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Timestream	データベース上の Amazon Timestream Query API アクティビティ。	Timestream データベース	AWS::Timestream::Database
	テーブル上の Amazon Timestream Query API アクティビティ。	Timestream テーブル	AWS::Timestream::Table
Amazon Verified Permissions	ポリシーストア上の Amazon Verified Permissions API アクティビティ。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces シンクライアント	WorkSpaces デバイス上のシンクライアント API アクティビティ。	シンクライアントデバイス	AWS::ThinClient::Device
	WorkSpaces 環境でのシンクライアント API アクティビティ。	シンクライアント環境	AWS::ThinClient::Environment
AWS X-Ray	トレース での X-Ray API アクティビティ。	X-Ray トレース	AWS::XRay::Trace

証跡またはイベントデータストアの作成時、デフォルトでは、データイベントは記録されません。CloudTrail データイベントを記録するには、アクティビティを収集するサポートされているリソースまたはリソースタイプを明示的に追加する必要があります。データイベントの口グ記録の詳細については、「データイベントを口グ記録する」を参照してください。

データイベントの口グ記録には追加料金が適用されます。 CloudTrail 料金については、「 AWS CloudTrail の料金」を参照してください。

Insights イベント

CloudTrail Insights イベントは、 CloudTrail 管理アクティビティを分析することで、アカウント内の異常な API コールレートまたはエラーレートのアクティビティをキャプチャします AWS 。Insights イベントは、関連する API、エラーコード、インシデント時間、統計情報などの関連情報を提供し、異常なアクティビティについて理解して対処するのに役立ちます。 CloudTrail 証跡またはイベントデータストアでキャプチャされた他のタイプのイベントとは異なり、Insights イベントは、 がアカウントの API 使用量またはエラー率のログ記録の変更 CloudTrail を検出したときにのみログに記録されます。これは、アカウントの一般的な使用パターンとは大きく異なります。

Insights イベントを生成する可能性のあるアクティビティの例を次に示します。

- 通常、アカウントは Amazon S3 `DeleteBucket` API コールを 1 分あたり 20 個までログに記録しますが、アカウントは 1 分あたり平均 100 個の `DeleteBucket` API コールを開始しています。異常なアクティビティの開始時に Insights イベントが記録され、異常なアクティビティの終了を示すために別の Insights イベントが記録されます。
- 通常、アカウントは Amazon EC2 `AuthorizeSecurityGroupIngress` API のコールを 1 分あたり 20 個を記録しますが、アカウントは `AuthorizeSecurityGroupIngress` へのコールをまったく記録し始めていません。異常なアクティビティの開始時に Insights イベントが記録され、10 分後、以上にアクティビティが終了すると、異常なアクティビティの終了を示すために別の Insights イベントが記録されます。
- 通常は、アカウントで AWS Identity and Access Management API `DeleteInstanceProfile` に関する `AccessDeniedException` エラーのログ記録が 7 日間に 1 つもありません。アカウントが `DeleteInstanceProfile` API コールで 1 分あたり平均 12 `AccessDeniedException` エラーのログを記録し始めます。異常なエラーレートのアクティビティが発生した時に Insights イベントが記録されますが、この異常アクティビティの終了を示すために別の Insights イベントも記録されます。

これらの例は、説明のみを目的としています。結果はユースケースによって異なる場合があります。

CloudTrail Insights イベントをログに記録するには、新規または既存の証跡またはイベントデータストアで Insights イベントを明示的に有効にする必要があります。Insights イベントのログ記録に関する詳細については、「Insights イベントのログ記録」を参照してください。

Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。

証跡とイベントデータストアの Insights イベントの表示

CloudTrail は、証跡とイベントデータストアの両方で Insights イベントをサポートしますが、Insights イベントの表示方法とアクセス方法にはいくつかの違いがあります。

証跡の Insights イベントの表示

証跡で Insights イベントを有効にしていて、異常なアクティビティ CloudTrail を検出すると、Insights イベントは証跡の送信先 S3 バケット内の別のフォルダまたはプレフィックスに記録されます。 CloudTrail コンソールで Insights イベントを表示すると、インサイトのタイプとインシデント期間を確認することもできます。詳細については、「トレイルの CloudTrail Insights イベントをコンソールに表示する CloudTrail 」を参照してください。

イベントデータストアの Insights イベントの表示

CloudTrail Lake で Insights イベントをログに記録するには、Insights イベントをログに記録する送信先イベントデータストアと、Insights を有効にして管理イベントをログに記録するソースイベントデータストアが必要です。詳細については、「コンソールを使用して CloudTrail Insights イベントのイベントデータストアを作成する」を参照してください。

ソースイベントデータストアで CloudTrail Insights を有効にしていて、異常なアクティビティ CloudTrail を検出した場合、 は Insights イベントを送信先イベントデータストアに CloudTrail 配信します。その後、送信先イベントデータストアにクエリを実行して Insights イベントに関する情報を取得し、オプションでクエリ結果を S3 バケットに保存できます。詳細については、「クエリを作成または編集する」および「 CloudTrail コンソールにサンプルクエリが表示されます。 」を参照してください。

Insights Events ダッシュボードを表示して、送信先イベントデータストアの Insights イベントを視覚化できます。詳細については、「 CloudTrail Lake ダッシュボードを表示する」を参照してください。

イベント履歴

CloudTrail イベント履歴は、 内の過去 90 日間の CloudTrail 管理イベントの表示可能、検索可能、ダウンロード可能、およびイミュータブルなレコードを提供します AWS リージョン。この履歴を使用して、、 SDK AWS Management Console、コマンドラインツール、およびその他の AWS サービスで AWS アカウントで実行されたアクションを可視化できます。 AWS SDKs コンソールでイベント履歴の表示をカスタマイズするには、表示する列 CloudTrail を選択します。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。

追跡

証跡は、イベントを S3 バケット CloudTrail に配信し、オプションで CloudWatch Logs と Amazon EventBridgeに配信できるようにする設定です。証跡を使用して、配信する CloudTrail イベントを選択し、 CloudTrail イベントログファイルを AWS KMS キーで暗号化し、ログファイル配信用の Amazon SNS 通知を設定できます。証跡の作成と管理の詳細については、「あなたのためのトレイルの作成 AWS アカウント」を参照してください。

マルチリージョンおよびシングルリージョンの証跡

には、 AWS アカウントマルチリージョン証跡と単一リージョン証跡の 2 種類の証跡を作成できます。

マルチリージョンの証跡

マルチリージョン証跡を作成すると、 は作業しているAWS パーティションのすべての AWS リージョン でイベント CloudTrail を記録し、指定した S3 バケットに CloudTrail イベントログファイルを配信します。マルチリージョンの証跡を作成した後に AWS リージョン が追加されると、その新しいリージョンが自動的に含まれ、そのリージョンのイベントがログに記録されます。マルチリージョンの証跡を作成すると、アカウント内のすべてのリージョンでのアクティビティを把握できるため、推奨されるベストプラクティスとなります。 CloudTrail コンソールを使用して作成する証跡はすべてマルチリージョンです。を使用して、単一リージョンの証跡をマルチリージョンの証跡に変換できます AWS CLI。詳細については、「コンソールで証跡を作成する」および「1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用」を参照してください。

単一リージョンの証跡

単一リージョンの証跡を作成すると、 はそのリージョンのイベントのみ CloudTrail を記録します。次に、指定した Amazon S3 バケットに CloudTrail イベントログファイルを配信します。AWS CLIを使用する際は、単一のリージョンの証跡のみを作成することができます。追加の単一の証跡を作成する場合は、それらの証跡に CloudTrail イベントログファイルを同じ S3 バケットに配信させるか、別のバケットに配信させることができます。これは、 または CloudTrail API AWS CLI を使用して証跡を作成する場合のデフォルトのオプションです。詳細については、「を使用した証跡の作成、更新、管理 AWS CLI」を参照してください。

> **Note**
>
> どちらのタイプの証跡でも、任意のリージョンから Amazon S3 バケットを指定できます。

マルチリージョン証跡には次の利点があります。

- 証跡の設定は、すべての に一貫して適用されます AWS リージョン。
- 1 つの Amazon S3 バケット AWS リージョン 内のすべての からイベントを受信し、オプションで Logs CloudWatch ロググループで CloudTrail イベントを受信します。 Amazon S3
- すべての の証跡設定を 1 つの場所 AWS リージョン から管理します。

証跡をすべての AWS リージョンに適用すると、 は特定のリージョンで作成した証跡 CloudTrail を使用して、作業しているAWS パーティション内の他のすべてのリージョンで同じ設定の証跡を作成します。

その結果、次のことが起こります。

- CloudTrail は、すべての AWS リージョンからのアカウントアクティビティのログファイルを、指定した単一の Amazon S3 バケットに配信し、オプションで Logs CloudWatch ロググループに配信します。
- 証跡に Amazon SNS トピックを設定した場合、すべての AWS リージョンのログファイル配信に関する SNS 通知がその 1 つの SNS トピックに送信されます。

証跡がマルチリージョンかシングルリージョンかにかかわらず、Amazon に送信されるイベントは、1 つのイベントバスではなく、各リージョンのイベントバス で受信 EventBridge されます。

1 リージョンに対する複数の証跡

デベロッパー、セキュリティ担当者、IT 監査者など、関連するユーザーグループが複数ある場合は、1 つのリージョンに対して複数の証跡を作成できます。これにより、各グループがログファイルの独自のコピーを受け取れるようになります。

CloudTrail は、リージョンごとに 5 つの証跡をサポートします。マルチリージョンの証跡は、リージョンごとに 1 つの証跡としてカウントされます。

以下は、5 つの証跡を持つリージョンの例です。

- 米国西部 (北カリフォルニア) リージョンに、そのリージョンだけに適用される証跡を 2 つ作成する。
- 米国西部 (北カリフォルニア) リージョンにさらに 2 つのマルチリージョン証跡を作成します。
- アジアパシフィック (シドニー) リージョンに別のマルチリージョン証跡を作成します。この証跡は、米国西部 (北カリフォルニア) リージョンでも証跡として存在します。

証跡のリストは、 CloudTrail コンソールの AWS リージョン 証跡ページで確認できます。詳細については、「証跡の更新」を参照してください。 CloudTrail 料金については、「 AWS CloudTrail の料金」を参照してください。

組織の証跡

組織の証跡は、管理アカウントと AWS Organizations 組織内のすべてのメンバーアカウントの CloudTrail イベントを同じ Amazon S3 バケット、 CloudWatch ログ、および Amazon に配信できるようにする設定です EventBridge。組織の証跡を作成すると、組織のための統一されたイベントログ記録戦略を定義するのに役立ちます。

コンソールを使用して作成されたすべての組織の証跡は、組織内の各メンバーアカウントで有効になっている AWS リージョン からのイベントをログに記録するマルチリージョン組織の証跡です。組織内のすべての AWS パーティションのイベントをログに記録するには、各パーティションにマルチリージョン組織の証跡を作成します。を使用して、単一リージョンまたはマルチリージョンの組織の証跡を作成できます AWS CLI。単一リージョンの証跡を作成する場合は、証跡の AWS リージョン （ ホームリージョンとも呼ばれる) でのみアクティビティを記録します。

のほとんどの AWS リージョン はデフォルトで有効になっていますが AWS アカウント、特定のリージョン (オプトインリージョンとも呼ばれます) を手動で有効にする必要があります。デフォルトで有効になっているリージョンについては、「 AWS Account Management リファレンスガイド」の「リージョンを有効または無効にする前の考慮事項」を参照してください。がサポートするリージョンのリストについては、 CloudTrail「」を参照してくださいCloudTrail サポートされているリージョン。

組織の証跡を作成すると、指定した名前の証跡のコピーが、組織に属するメンバーアカウントで作成されます。

- 組織の証跡が単一リージョン用で、証跡のホームリージョンがオプトリージョン でない場合、証跡のコピーは各メンバーアカウントの組織の証跡のホームリージョンに作成されます。

- 組織の証跡が単一リージョン用で、証跡のホームリージョンがオプトリージョン の場合、証跡のコピーは、そのリージョンを有効にしたメンバーアカウントの組織の証跡のホームリージョンに作成されます。
- 組織の証跡がマルチリージョンで、証跡のホームリージョンがオプトインリージョン でない場合、証跡のコピーは各メンバーアカウントで有効になっている各 AWS リージョン に作成されます。メンバーアカウントがオプトインリージョンを有効にすると、マルチリージョン証跡のコピーが、そのリージョンのアクティベーションが完了した後に、メンバーアカウントの新しくオプトインされたリージョンに作成されます。
- 組織の証跡がマルチリージョンで、ホームリージョンがオプトインリージョン の場合、マルチ AWS リージョン リージョン証跡が作成された をオプトインしない限り、メンバーアカウントは組織の証跡にアクティビティを送信しません。例えば、マルチリージョンの証跡を作成し、証跡のホームリージョンとして欧州 (スペイン) リージョンを選択した場合、そのアカウントの欧州 (スペイン) リージョンを有効にしたメンバーアカウントのみが、そのアカウントのアクティビティを組織の証跡に送信します。

> **Note**
>
> CloudTrail は、リソースの検証が失敗した場合でも、メンバーアカウントに組織の証跡を作成します。検証の失敗の例は次のとおりです。
>
> - Amazon S3 バケットポリシーが正しくない
> - Amazon SNS トピックポリシーが正しくない
> - Logs CloudWatch ロググループに配信できない
> - KMS キーを使用して暗号化するアクセス許可が不十分
>
> アクセス CloudTrail 許可を持つメンバーアカウントは、 CloudTrail コンソールで証跡の詳細ページを表示するか、 コマンドを実行する AWS CLI [get-trail-status]ことで、組織の証跡の検証に失敗したことを確認できます。

メンバーアカウントで CloudTrail アクセス許可を持つユーザーは、アカウント AWS から AWS CloudTrail コンソールにログインするとき、または などの AWS CLI コマンドを実行するときに、組織の証跡 (証跡 ARN を含む) を表示できます `describe-trails` (ただし、メンバーアカウントは、を使用するときは、名前ではなく、組織の証跡の ARN を使用する必要があります AWS CLI) 。ただし、メンバーアカウントのユーザーには、組織の証跡の削除、ログのオン/オフの切り替え、ログ

に記録されるイベントの種類の変更、または組織の証跡の変更を行うための十分なアクセス許可がありません。 AWS Organizationsの詳細については、「Organizations の用語と概念」を参照してください。組織の証跡を作成して作業する方法の詳細については、「組織の証跡の作成」を参照してください。

CloudTrail Lake およびイベントデータストア

CloudTrail Lake では、イベントに対してきめ細かな SQL ベースのクエリを実行し、独自のアプリケーションや と統合されているパートナーなど AWS、 外部のソースからのイベントを ログ記録できます CloudTrail。 CloudTrail Lake を使用するには、アカウントに証跡を設定する必要はありません。

イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いたイベントのイミュータブルなコレクションです。イベントデータをイベントデータストアに保存できる期間は、[1 年間の延長可能な保存料金] オプションを選択した場合は最大 3,653 日 (約 10 年)、[7 年間の保存料金] オプションを選択した場合は最大 2,557 日 (約 7 年間) です。将来使用するために Lake クエリを保存することができ、クエリの結果は最大 7 日間表示できます。クエリ結果を S3 バケットに保存することもできます。 CloudTrail Lake は、組織からのイベントをイベントデータストア AWS Organizations に保存したり、複数のリージョンやアカウントからのイベントを保存することもできます。 CloudTrail Lake は、セキュリティ調査とトラブルシューティングの実行に役立つ監査ソリューションの一部です。詳細については、「AWS CloudTrail Lake の使用」および「CloudTrail 湖の概念と用語」を参照してください。

CloudTrail インサイト

CloudTrail Insights は、 AWS ユーザーが CloudTrail 管理イベントを継続的に分析することで、API コールに記録された異常なボリュームの API コールやエラーを特定して応答するのに役立ちます。Insights イベントは、異常なレベルの `write` 管理 API アクティビティ、または管理 API アクティビティで返された異常なレベルのエラーの記録です。デフォルトでは、証跡とイベントデータストアは CloudTrail Insights イベントを記録しません。コンソールでは、証跡あるいはイベントデータストアを作成または更新する際に Insights イベントがログ記録されるように選択できます。 CloudTrail API を使用すると、既存の証跡またはイベントデータストアの設定を `PutInsightSelectors` API で編集することで、Insights イベントをログに記録できます。CloudTrail Insights イベントのログ記録には追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「Insights イベントのログ記録」と「AWS CloudTrail 料金表」を参照してください。

タグ

タグは、証 CloudTrail 跡、イベントデータストア、チャネル、 CloudTrail ログファイルの保存に使用される S3 バケット、 AWS Organizations 組織と組織単位などのリソースに割り当てる AWS ことができる、ユーザー定義のキーとオプションの値です。証跡と証跡のログファイルの保存に使用する S3 バケットに同じタグを追加することで、 でこれらのリソースの管理、検索、フィルタリングを簡単に行うことができますAWS Resource Groups。タグ付け戦略を実装して、リソースを一貫して効果的に、そして簡単に検索して管理できます。詳細については、AWS 「リソースのタグ付けのベストプラクティス」を参照してください。

AWS Security Token Service および CloudTrail

AWS Security Token Service （ AWS STS) は、グローバルエンドポイントを持つサービスであり、リージョン固有のエンドポイントもサポートしています。エンドポイントとは、ウェブサービスリクエストのエントリポイントとなる URL のことです。例えば、 `https://cloudtrail.us-west-2.amazonaws.com`は AWS CloudTrail サービスの米国西部 (オレゴン) リージョンエントリポイントです。リージョンのエンドポイントは、アプリケーションのレイテンシーを低減するのに役立ちます。

AWS STS リージョン固有のエンドポイントを使用する場合、そのリージョンの証跡は、そのリージョンで発生した AWS STS イベントのみを配信します。たとえば、エンドポイント `sts.us-west-2.amazonaws.com` を使用している場合、us-west-2 の証跡は、us-west-2 から発生した AWS STS イベントのみを配信します。 AWS STS リージョンエンドポイントの詳細については、IAM ユーザーガイドの「 AWS リージョン AWS STS での のアクティブ化と非アクティブ化」を参照してください。

AWS リージョンエンドポイントの完全なリストについては、AWS 「」の「リージョンとエンドポイント」を参照してくださいAWS 全般のリファレンス。グローバル AWS STS エンドポイントからのイベントの詳細については、「グローバルサービスイベント」を参照してください。

グローバルサービスイベント

> **Important**
>
> 2021 年 11 月 22 日に、 は証跡がグローバルサービスイベントをキャプチャする方法 AWS CloudTrail を変更しました。これで、Amazon CloudFront、、および によって作成されたイベント AWS STS は AWS Identity and Access Management、それらが作成されたリージョン、米国東部 (バージニア北部) リージョン、us-east-1 に記録されます。これにより、 がこ

れらのサービスを他の AWS グローバルサービスのサービスと一貫して CloudTrail 扱うようになります。米国東部 (バージニア北部) 以外でグローバルサービスイベントを受信するには、米国東部 (バージニア北部) 以外のグローバルサービスイベントを使用するシングルリージョン証跡を、必ずマルチリージョン証跡に変換してください。グローバルサービスイベントのキャプチャの詳細については、このセクション後半の グローバルサービスイベントのログ記録の有効化と無効化 を参照してください。
対照的に、 CloudTrail コンソールのイベント履歴と aws cloudtrail lookup-events コマンドは、これらのイベントが発生した AWS リージョン にイベントを表示します。

ほとんどのサービスの場合、イベントはアクションが発生したリージョンで記録されます。 AWS Identity and Access Management (IAM) AWS STSや Amazon などのグローバルサービスの場合 CloudFront、イベントはグローバルサービスを含むすべての証跡に配信されます。

ほとんどのグローバルサービスの場合、イベントは米国東部 (バージニア北部) リージョンで発生しているものとしてログに記録されますが、一部のグローバルサービスイベントは米国東部 (オハイオ) リージョンや米国西部 (オレゴン) リージョンなどのその他のリージョンで発生しているものとしてログに記録されます。

グローバルサービスイベントを重複して受信しないようにするには、次の点に注意してください。

- グローバルサービスイベントは、コンソールを使用して作成された証跡にデフォルトで配信されます CloudTrail 。イベントは、その証跡のバケットに配信されます。
- 単一のリージョンの証跡が複数ある場合は、証跡を設定し、グローバルサービスイベントがそれらの証跡の 1 つのみに配信されるようにすることを検討してください。詳しくは、グローバルサービスイベントのログ記録の有効化と無効化 を参照してください。
- 証跡の設定をすべてのリージョンのログ記録から単一のリージョンのログ記録に変更すると、その証跡に対してグローバルサービスイベントのログ記録は自動的に無効になります。同様に、証跡の設定を単一のリージョンのログ記録からすべてのリージョンのログ記録に変更すると、その証跡に対してグローバルサービスイベントのログ記録は自動的に有効になります。

  証跡に対するグローバルサービスイベントのログ記録の変更の詳細については、「グローバルサービスイベントのログ記録の有効化と無効化」を参照してください。

例:

1. CloudTrail コンソールで証跡を作成します。デフォルトでは、この証跡はグローバルサービスイベントをログに記録します。

2. 単一リージョンの証跡を複数作成したとします。
3. 単一リージョンの証跡について、グローバルサービスを含める必要はありません。グローバルサービスイベントは、1 つ目の証跡に対して配信されます。詳細については、「を使用した証跡の作成、更新、管理 AWS CLI」を参照してください。

> **Note**
>
> AWS CLI、 AWS SDKs、または CloudTrail API を使用して証跡を作成または更新する場合、証跡のグローバルサービスイベントを含めるか除外するかを指定できます。 CloudTrail コンソールからグローバルサービスイベントのログ記録を設定することはできません。

CloudTrail サポートされているリージョン

> **Note**
>
> CloudTrail Lake でサポートされているリージョンについては、「」を参照してくださいCloudTrail Lake がサポートするリージョン。
> データプレーンエンドポイントの詳細については、「」の「データプレーンエンドポイント」を参照してくださいAWS 全般のリファレンス。

リージョン名	リージョン	コントロールプレーンエンドポイント	[プロトコル]	サポート日付
米国東部 (バージニア北部)	us-east-1	cloudtrail.us-east-1.amazonaws.com	HTTPS	2013 年 11 月 13 日
米国東部 (オハイオ)	us-east-2	cloudtrail.us-east-2.amazonaws.com	HTTPS	2016 年 10 月 17 日
米国西部 (北カリフォルニア)	us-west-1	cloudtrail.us-west-1.amazonaws.com	HTTPS	2014 年 5 月 13 日

リージョン名	リージョン	コントロールプレーンエンドポイント	[プロトコル]	サポート日付
米国西部（オレゴン）	us-west-2	cloudtrail.us-west-2.amazonaws.com	HTTPS	2013 年 11 月 13 日
アフリカ (ケープタウン)	af-south-1	cloudtrail.af-south-1.amazonaws.com	HTTPS	2020 年 4 月 22 日
アジアパシフィック (香港)	ap-east-1	cloudtrail.ap-east-1.amazonaws.com	HTTPS	04/24/2019
アジアパシフィック (ハイデラバード)	ap-south-2	cloudtrail.ap-south-2.amazonaws.com	HTTPS	11/22/2022
アジアパシフィック (ジャカルタ)	ap-southeast-3	cloudtrail.ap-southeast-3.amazonaws.com	HTTPS	12/13/2021
アジアパシフィック (メルボルン)	ap-southeast-4	cloudtrail.ap-southeast-4.amazonaws.com	HTTPS	01/23/2023
アジアパシフィック（ムンバイ）	ap-south-1	cloudtrail.ap-south-1.amazonaws.com	HTTPS	2016 年 6 月 27 日
アジアパシフィック (大阪)	ap-northeast-3	cloudtrail.ap-northeast-3.amazonaws.com	HTTPS	2018 年 2 月 12 日

リージョン名	リージョン	コントロールプレーンエンドポイント	[プロトコル]	サポート日付
アジアパシフィック (ソウル)	ap-northeast-2	cloudtrail.ap-northeast-2.amazonaws.com	HTTPS	2016 年 1 月 6 日
アジアパシフィック (シンガポール)	ap-southeast-1	cloudtrail.ap-southeast-1.amazonaws.com	HTTPS	2014 年 6 月 30 日
アジアパシフィック (シドニー)	ap-southeast-2	cloudtrail.ap-southeast-2.amazonaws.com	HTTPS	2014 年 5 月 13 日
アジアパシフィック (東京)	ap-northeast-1	cloudtrail.ap-northeast-1.amazonaws.com	HTTPS	2014 年 6 月 30 日
カナダ (中部)	ca-central-1	cloudtrail.ca-central-1.amazonaws.com	HTTPS	2016 年 12 月 8 日
カナダ西部 (カルガリー)	ca-west-1	cloudtrail.ca-west-1.amazonaws.com	HTTPS	12/20/2023
中国 (北京)	cn-north-1	cloudtrail.cn-north-1.amazonaws.com.cn	HTTPS	2014/03/01
中国 (寧夏)	cn-northwest-1	cloudtrail.cn-northwest-1.amazonaws.com.cn	HTTPS	2017/12/11
欧州 (フランクフルト)	eu-central-1	cloudtrail.eu-central-1.amazonaws.com	HTTPS	2014 年 10 月 23 日
欧州 (アイルランド)	eu-west-1	cloudtrail.eu-west-1.amazonaws.com	HTTPS	2014 年 5 月 13 日

リージョン名	リージョン	コントロールプレーンエンドポイント	[プロトコル]	サポート日付
欧州 (ロンドン)	eu-west-2	cloudtrail.eu-west-2.amazonaws.com	HTTPS	2016 年 12 月 13 日
欧州 (ミラノ)	eu-south-1	cloudtrail.eu-south-1.amazonaws.com	HTTPS	04/27/2020
欧州 (パリ)	eu-west-3	cloudtrail.eu-west-3.amazonaws.com	HTTPS	2017/12/18
欧州 (スペイン)	eu-south-2	cloudtrail.eu-south-2.amazonaws.com	HTTPS	11/16/2022
欧州 (ストックホルム)	eu-north-1	cloudtrail.eu-north-1.amazonaws.com	HTTPS	2018 年 12 月 11 日
欧州 (チューリッヒ)	eu-central-2	cloudtrail.eu-central-2.amazonaws.com	HTTPS	11/09/2022
イスラエル (テルアビブ)	il-central-1	cloudtrail.il-central-1.amazonaws.com	HTTPS	07/31/2023
中東 (バーレーン)	me-south-1	cloudtrail.me-south-1.amazonaws.com	HTTPS	2019-07-29
中東 (アラブ首長国連邦)	me-central-1	cloudtrail.me-central-1.amazonaws.com	HTTPS	08/30/2022
南米 (サンパウロ)	sa-east-1	cloudtrail.sa-east-1.amazonaws.com	HTTPS	2014 年 6 月 30 日
AWS GovCloud (米国東部)	us-gov-east-1	cloudtrail.us-gov-east-1.amazonaws.com	HTTPS	2018/11/12

リージョン名	リージョン	コントロールプレーンエンドポイント	[プロトコル]	サポート日付
AWS GovCloud（米国西部）	us-gov-west-1	cloudtrail.us-gov-west-1.amazonaws.com	HTTPS	08/16/2011

CloudTrail での の使用の詳細については AWS GovCloud (US) Regions、 AWS GovCloud (US) ユーザーガイドの「サービスエンドポイント」を参照してください。

中国 (北京) リージョン CloudTrail での の使用の詳細については、「」の「中国の AWS のエンドポイントと ARNs」を参照してくださいAmazon Web Services 全般のリファレンス。

CloudTrail がサポートするサービスと統合

CloudTrail は、多くの のイベントのログ記録をサポートしています AWS のサービス。サポートされている各サービスの詳細については、そのサービスのガイドを参照してください。サービス固有のトピックのリストについては、「」を参照してくださいAWS のサービストピック CloudTrail。さらに、 CloudTrail ログで収集されたデータを分析して処理するために AWS のサービス 使用できるものもあります。

> **Note**
>
> 各サービスでサポートされているリージョンのリストについては、Amazon Web Services 全般のリファレンスの「サービスエンドポイントとクォータ」を参照してください

トピック

- AWS CloudTrail ログと サービスの統合
- CloudTrail Amazon との統合 EventBridge
- CloudTrail との統合 AWS Organizations
- AWS のサービストピック CloudTrail
- CloudTrail サポートされていないサービス

AWS CloudTrail ログと サービスの統合

> **Note**
>
> CloudTrail Lake を使用してイベントをクエリおよび分析することもできます。 CloudTrail Lake クエリは、イベント履歴 の単純なキーと値のルックアップ、または の実行よりも、より詳細でカスタマイズ可能なイベントの表示を提供しますLookupEvents。 CloudTrail Lake ユーザーは、 CloudTrail イベントの複数のフィールドで複雑な標準クエリ言語 (SQL) クエリを実行できます。詳細については、「AWS CloudTrail Lake の使用」および「トレイルイベントを CloudTrail Lake にコピーする」を参照してください。
> CloudTrail Lake イベントデータストアとクエリには CloudTrail 料金が発生します。 CloudTrail Lake の料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

CloudTrail ログで収集されたイベントデータをさらに分析し、それに基づいて行動するように、他の AWS サービスを設定できます。詳細については、以下のトピックを参照してください。

AWS サービス	トピック	説明
Amazon Athena	AWS CloudTrail ログのクエリ	CloudTrail ログで Athena を使用することは、 AWS サービスアクティビティの分析を強化する強力な方法です。たとえば、クエリを使用して傾向を識別したり、ソース IP アドレスやユーザーなど属性でアクティビティをさらに分離したりすることが可能です。 CloudTrail コンソールから直接ログをクエリするためのテーブルを自動的に作成し、それらのテーブルを使用して Athena でクエリを実行できます。詳細については、「Amazon Athena ユー

AWS サービス	トピック	説明
		ザーガイド」の CloudTrail「コンソールでの CloudTrail ログのテーブルの作成」を参照してください。 Amazon Athena **Note** Amazon Athena でクエリを実行する際には、追加コストが発生します。詳細については、Amazon Athena 料金 を参照してください。

AWS サービス	トピック	説明
Amazon CloudWatch Logs	Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング	CloudWatch Logs CloudTrail で を設定して証跡ログをモニタリングし、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ことができます。例えば、アラームをトリガーし、それらの CloudWatch アラームがトリガーされたときに通知を送信する CloudWatch ログメトリクスフィルターを定義できます。 **Note** Amazon CloudWatch および Amazon CloudWatch Logs の標準料金が適用されます。詳細については、「Amazon CloudWatch 料金表」を参照してください。

CloudTrail Amazon との統合 EventBridge

Amazon EventBridge は、 AWS リソースの変更を記述するシステムイベントのストリームをほぼリアルタイムで配信する AWS サービスです。では EventBridge、 によって記録されたイベントに応答するルールを作成できます CloudTrail。詳細については、「Amazon でルールを作成する EventBridge」を参照してください。

EventBridge コンソールでルールを作成 EventBridge することで、証跡でサブスクライブしているイベントを に配信できます。

EventBridge コンソールから：

- AWS API Call via CloudTrail の詳細タイプを選択して、 eventTypeの で CloudTrail データと管理イベントを配信しますAwsApiCall。詳細タイプの値が のイベントを記録するにはAWS API Call via CloudTrail、現在管理イベントまたはデータイベントを口グ記録している証跡が必要です。
- AWS Management Console サインインイベントを配信する AWS Console Sign In via CloudTrail detail-type を選択します。詳細タイプが のイベントを記録するにはAWS Console Sign In via CloudTrail、現在管理イベントを記録している証跡が必要です。
- Insights イベントを配信するAWS Insight via CloudTrail詳細タイプを選択します。詳細タイプの値が のイベントを記録するにはAWS Insight via CloudTrail、現在 Insights イベントを記録している証跡が必要です。Insights イベントの口グ記録に関する詳細は、「Insights イベントの口グ記録」を参照してください。

証跡の作成方法に関する詳細については、「証跡の作成」を参照してください。

CloudTrail との統合 AWS Organizations

AWS Organizations 組織の管理アカウントは、組織の CloudTrail リソースを管理するための委任管理者を追加できます。 AWS Organizationsの組織内のすべての AWS アカウントのすべてのイベントデータを収集する、組織の管理アカウントまたは委任された管理者アカウントに、組織の証跡または組織のイベントデータストアを作成できます。組織の証跡を作成すると、組織のための統一されたイベントログ記録戦略を定義するのに役立ちます。

組織の証跡は、組織内の各 AWS アカウントに自動的に適用されます。メンバーアカウントのユーザーはこれらの証跡を見ることはできますが、変更することはできず、デフォルトでは組織証跡用に作成されたログファイルを見ることもできません。詳細については、「組織の証跡の作成」を参照してください。

AWS のサービストピック CloudTrail

ログファイル内のその AWS サービスのイベント例など、個々のサービスのイベントが CloudTrail 口グにどのように記録されるかについて詳しく知ることができます。特定の AWS のサービスが とどのように統合されるかの詳細については CloudTrail、そのサービスの個々のガイドの「統合に関するトピック」を参照してください。

まだプレビュー中であるか、一般提供 (GA) 用にまだリリースされていないサービス、またはパブリック APIsがないサービスは、サポートされているとは見なされません。現在、Amazon VPC エンドポイントのポリシー固有のイベントはログに記録 CloudTrail されません。

> **Note**
>
> 各サービスでサポートされているリージョンのリストについては、Amazon Web Services 全般のリファレンスの「サービスエンドポイントとクォータ」を参照してください
> データイベントのログ記録を実行するサービスの詳細については、「データイベント」を参照してください。

AWS サービス	CloudTrail トピック	サポート開始
Amazon API Gateway	を使用して Amazon API Gateway への API 管理呼び出しをログに記録する AWS CloudTrail	2015 年 7 月 9 日
Amazon AppFlow	を使用した Amazon AppFlow API コールのログ記録 AWS CloudTrail	2020 年 4 月 22 日
Amazon AppStream 2.0	を使用した Amazon AppStream 2.0 API コールのログ記録 AWS CloudTrail	2019 年 4 月 25 日
Amazon Athena	を使用した Amazon Athena API コールのログ記録 AWS CloudTrail	2017 年 5 月 19 日
Amazon Aurora	での Amazon Aurora API コールのモニタリング AWS CloudTrail	08/31/2018
Amazon Bedrock	を使用した Amazon Bedrock API コールのログ記録 AWS CloudTrail	10/23/2023
Amazon Braket	を使用した Amazon Braket API ログ記録 CloudTrail	08/12/2020

AWS サービス	CloudTrail トピック	サポート開始
Amazon Chime	を使用した Amazon Chime 管理コールのログ記録 AWS CloudTrail	2017 年 9 月 27 日
Amazon Cloud Directory	を使用した Cloud Directory API コールのログ記録 AWS CloudTrail	2017 年 1 月 26 日
Amazon CloudFront	を使用して AWS CloudTrail CloudFront API に送信されたリクエストをキャプチャする	2014 年 5 月 28 日
Amazon CloudSearch	を使用した Amazon CloudSearch Configuration Service コールのログ記録 AWS CloudTrail	2014 年 10 月 16 日
Amazon CloudWatch	での Amazon CloudWatch API コールのログ記録 AWS CloudTrail	2014 年 4 月 30 日
Amazon CloudWatch Logs	での Amazon CloudWatch Logs API コールのログ記録 AWS CloudTrail	2016 年 3 月 10 日
Amazon CodeCatalyst	AWS アカウント を使用して接続された での CodeCatalyst API コールのログ記録 AWS CloudTrail	12/01/2022
Amazon CodeGuru Reviewer	を使用した Amazon CodeGuru Reviewer API コールのログ記録 AWS CloudTrail	12/02/2019
Amazon CodeWhisperer	AWS CloudTrail および CodeWhisperer APIs	04/13/2023

AWS サービス	CloudTrail トピック	サポート開始
Amazon Cognito	を使用した Amazon Cognito API コールのログ記録 AWS CloudTrail	2016 年 2 月 18 日
Amazon Comprehend	を使用した Amazon Comprehend API コールのログ記録 AWS CloudTrail	2018 年 1 月 17 日
Amazon Comprehend Medical	AWS CloudTrailを使用した Amazon Comprehend Medical API コールのログ記録	2018 年 11 月 27 日
Amazon Connect	AWS CloudTrailでの Amazon Connect API コールのログ記録	2019 年 12 月 11 日
Amazon Data Firehose	を使用した Amazon Data Firehose API コールのモニタリング AWS CloudTrail	2016 年 3 月 17 日
Amazon Data Lifecycle Manager	を使用した Amazon Data Lifecycle Manager API コールのログ記録 AWS CloudTrail	2018 年 7 月 24 日
Amazon Detective	AWS CloudTrailでの Amazon Detective API コールのログ記録	03/31/2020
Amazon DevOpsGuru	を使用した Amazon DevOpsGuru API コールのログ記録 AWS CloudTrail	05/04/2021
Amazon DocumentDB (MongoDB 互換性)	AWS CloudTrailでの Amazon DocumentDB API コールのログ記録	2019 年 1 月 9 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon DynamoDB	を使用した DynamoDB オペレーションのログ記録 AWS CloudTrail	2015 年 5 月 28 日
Amazon EC2	を使用した Amazon EC2 API コールのログ記録 AWS CloudTrail	2013 年 11 月 13 日
Amazon EC2 Auto Scaling	を使用した Auto Scaling API コールのログ記録 CloudTrail	2014 年 7 月 16 日
Amazon EC2 Capacity Blocks	を使用したキャパシティブロック API コールのログ記録 AWS CloudTrail	10/31/2023
Amazon EC2 Image Builder	を使用した EC2 Image Builder API コールのログ記録 CloudTrail	12/02/2019
Amazon Elastic Block Store (Amazon EBS) EBS direct API	を使用した API コールのログ記録 AWS CloudTrail AWS CloudTrailを使用した EBS direct API の API コールのログ記録	Amazon EBS: 2013 年 11 月 13 日 EBSダイレクトAPI：2020 年 6 月 30 日
Amazon Elastic Container Registry (Amazon ECR)	を使用した Amazon ECR API コールのログ記録 AWS CloudTrail	2015 年 12 月 21 日
Amazon Elastic Container Service (Amazon ECS)	を使用した Amazon ECS API コールのログ記録 AWS CloudTrail	2015 年 4 月 9 日
Amazon Elastic File System (Amazon EFS)	を使用した Amazon EFS API コールのログ記録 AWS CloudTrail	2016 年 6 月 28 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Elastic Kubernetes Service (Amazon EKS)	を使用した Amazon EKS API コールのログ記録 AWS CloudTrail	2018 年 6 月 5 日
Amazon Elastic Transcoder	を使用した Amazon Elastic Transcoder API コールのログ記録 AWS CloudTrail	2014 年 10 月 27 日
Amazon ElastiCache	を使用した Amazon ElastiCache API コールのログ記録 AWS CloudTrail	2014 年 9 月 15 日
Amazon EMR	での Amazon EMR API コールのログ記録 AWS CloudTrail	2014 年 4 月 4 日
Amazon EMR on EKS	AWS CloudTrailを使用した EKS API コールの Amazon EMR API コールのログ記録	12/09/2020
Amazon EventBridge	を使用した Amazon EventBridge API コールのログ記録 AWS CloudTrail	07/11/2019
Amazon FinSpace	AWS CloudTrail ログのクエリ	10/18/2022
Amazon Forecast	を使用した Amazon Forecast API コールのログ記録 AWS CloudTrail	2018 年 11 月 28 日
Amazon Fraud Detector	AWS CloudTrailでの Amazon Fraud Detector API コールのログ記録	01/09/2020
Amazon FSx for Lustre	を使用した Amazon FSx for Lustre API コールのログ記録 AWS CloudTrail	2019 年 1 月 11 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon FSx for Windows File Server	によるモニタリング AWS CloudTrail	2018 年 11 月 28 日
Amazon GameLift	を使用した Amazon GameLift API コールのログ記録 AWS CloudTrail	2016 年 1 月 27 日
Amazon GuardDuty	を使用した Amazon GuardDuty API コールのログ記録 AWS CloudTrail	2018 年 2 月 12 日
Amazon Inspector	を使用した Amazon Inspector API コールのログ記録 AWS CloudTrail	11/29/2021
Amazon Inspector Classic	を使用した Amazon Inspector Classic API コールのログ記録 AWS CloudTrail	2016 年 4 月 20 日
Amazon Inspector Scan	の Amazon Inspector スキャン情報 CloudTrail	11/27/2023
Amazon Interactive Video Service	AWS CloudTrailを使用した Amazon IVS API コールのログ記録	07/15/2020
Amazon Kendra	を使用した Amazon Kendra API コールの AWS CloudTrail ログ記録と、 ログを使用した Amazon Kendra Intelligent Ranking API コールの AWS CloudTrail ログ記録	2020 年 5 月 11 日
Amazon Keyspaces (Apache Cassandra 向け)	AWS CloudTrailでの Amazon Keyspaces API コールのログ記録	2020 年 1 月 13 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Managed Service for Apache Flink	を使用した Managed Service for Apache Flink API コールのログ記録 AWS CloudTrail	2019 年 3 月 22 日
Amazon Kinesis Data Streams	を使用した Amazon Kinesis Data Streams API コールのログ記録 AWS CloudTrail	2014 年 4 月 25 日
Amazon Kinesis Video Streams	を使用した Kinesis Video Streams API コールのログ記録 AWS CloudTrail	2018 年 5 月 24 日
Amazon Lex	を使用した Amazon Lex API コールのログ記録 CloudTrail	2017 年 8 月 15 日
Amazon Lightsail	を使用した Lightsail API コールのログ記録 AWS CloudTrail	2016 年 12 月 23 日
Amazon Location Service	AWS CloudTrailでのログ記録とモニタリング	12/15/2020
Amazon Lookout for Equipment	Amazon Lookout for Equipment のモニタリング	12/01/2020
Amazon Lookout for Metrics	での Amazon Lookout for Metrics API アクティビティの表示 AWS CloudTrail	12/08/2020
Amazon Lookout for Vision	AWS CloudTrailでの Amazon Lookout for Vision コールのログ記録	12/01/2020
Amazon Machine Learning	を使用した Amazon ML API コールのログ記録 AWS CloudTrail	2015 年 12 月 10 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Macie	AWS CloudTrailを使用した Amazon Macie API コールのログ記録	2020 年 5 月 13 日
Amazon Managed Blockchain	AWS CloudTrail Amazon Managed Blockchain API コールのログ記録 AWS CloudTrailを使用した Managed Blockchain API呼び出しのための Ethereum のログ記録 (プレビュー)	04/01/2019
Amazon Managed Grafana	AWS CloudTrailを使用した Amazon Managed Grafana API コールのログ記録	12/15/2020
Amazon Managed Service for Prometheus	AWS CloudTrailを使用した Amazon Managed Service for Prometheus API コールのログ記録	12/15/2020
Amazon Managed Streaming for Apache Kafka	を使用した API コールのログ記録 AWS CloudTrail	2018 年 12 月 11 日
Amazon Managed Workflows for Apache Airflow	での監査ログの表示 AWS CloudTrail	11/24/2020
Amazon MemoryDB for Redis	を使用した Amazon MemoryDB for Redis API コールのログ記録 AWS CloudTrail	08/19/2021
Amazon MQ	を使用した Amazon MQ API コールのログ記録 AWS CloudTrail	2018 年 7 月 19 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Neptune	を使用した Amazon Neptune API コールのログ記録 AWS CloudTrail	2018 年 5 月 30 日
Amazon Nimble Studio	を使用した Nimble Studio 呼び出しのログ記録 AWS CloudTrail	06/19/2023
Amazon One Enterprise	を使用した Amazon One Enterprise API コールのログ記録 AWS CloudTrail	11/27/2023
Amazon OpenSearch サービス	による Amazon OpenSearch Service API コールのモニタリング AWS CloudTrail	2015 年 10 月 1 日
Amazon Personalize	を使用した Amazon Personalize API コールのログ記録 AWS CloudTrail	2018 年 11 月 28 日
Amazon Pinpoint	を使用した Amazon Pinpoint API コールのログ記録 AWS CloudTrail	2018 年 2 月 6 日
Amazon Pinpoint SMS および音声 API	を使用した Amazon Pinpoint API コールのログ記録 AWS CloudTrail	2018 年 11 月 16 日
Amazon Polly	を使用した Amazon Polly API コールのログ記録 AWS CloudTrail	2016 年 11 月 30 日
Amazon Q (ビジネス用)	を使用した Amazon Q API コールのログ記録 AWS CloudTrail	11/28/2023

AWS サービス	CloudTrail トピック	サポート開始
Amazon Q (AWS ビルダー用)	を使用した Amazon Q API コールのログ記録 AWS CloudTrail	11/28/2023
Amazon Quantum Ledger Database (Amazon QLDB)	AWS CloudTrailでの Amazon QLDB API コールのログ記録	2019 年 9 月 10 日
Amazon QuickSight	を使用したオペレーションのログ記録 CloudTrail	2017 年 4 月 28 日
Amazon Relational Database Service (Amazon RDS)	を使用した Amazon RDS API コールのログ記録 AWS CloudTrail	2013 年 11 月 13 日
「Amazon RDS Performance Insights」	を使用した Amazon RDS API コールのログ記録 AWS CloudTrail Amazon RDS Performance Insights API は、Amazon RDS API のサブセットです。	2018 年 6 月 21 日
Amazon Redshift	を使用した Amazon Redshift API コールのログ記録 AWS CloudTrail	2014 年 6 月 10 日
Amazon Rekognition	を使用した Amazon Rekognition API コールのログ記録 AWS CloudTrail	2018 年 4 月 6 日
Amazon Route 53	AWS CloudTrail を使用して Route 53 API に送信されたリクエストをキャプチャする	2015 年 2 月 11 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Route 53 Application Recovery Controller	を使用した Amazon Route 53 Application Recovery Controller API コールのログ記録 AWS CloudTrail	07/27/2021
Amazon S3	を使用した Amazon S3 API コールのログ記録 AWS CloudTrail	管理イベント: 2015 年 9 月 1 日 データイベント: 2016 年 11 月 21 日
Amazon S3 Glacier	を使用した S3 Glacier API コールのログ記録 AWS CloudTrail	2014 年 12 月 11 日
Amazon SageMaker	を使用した Amazon SageMaker API コールのログ記録 AWS CloudTrail	2018 年 1 月 11 日
Amazon Security Lake	を使用した Amazon Security Lake API コールのログ記録 CloudTrail	05/30/2023
Amazon Simple Email Service (Amazon SES)	を使用した Amazon SES API コールのログ記録 AWS CloudTrail	2015 年 5 月 7 日
Amazon Simple Notification Service (Amazon SNS)	を使用した Amazon SNS API コールのログ記録 AWS CloudTrail	2014 年 10 月 9 日
Amazon Simple Queue Service (Amazon SQS)	を使用した Amazon SQS API アクションのログ記録 AWS CloudTrail	2014 年 7 月 16 日

AWS サービス	CloudTrail トピック	サポート開始
Amazon Simple Workflow Service (Amazon SWF)	を使用した API コールの記録 AWS CloudTrail	管理イベント: 05/13/2014 データイベント: 02/14/2024
Amazon Textract	を使用した Amazon Textract API コールのログ記録 AWS CloudTrail	2019 年 5 月 29 日
Amazon Timestream	を使用した Timestream API コールのログ記録 AWS CloudTrail	09/30/2020
Amazon Transcribe	を使用した Amazon Transcribe API コールのログ記録 AWS CloudTrail	2018 年 6 月 28 日
Amazon Translate	AWS CloudTrailでの Amazon Translate API コールのログ記録	2018 年 4 月 4 日
Amazon Verified Permissions	を使用した Amazon Verified Permissions API コールのログ記録 AWS CloudTrail	06/13/2023
Amazon Virtual Private Cloud (Amazon VPC)	を使用した API コールのログ記録 AWS CloudTrail Amazon VPC API は、Amazon EC2 API のサブセットです。	2013 年 11 月 13 日
Amazon VPC Lattice	CloudTrail ログ	03/31/2023
Amazon VPC Reachability Analyzer	を使用した Reachability Analyzer API コールのログ記録 AWS CloudTrail	11/27/2023

AWS サービス	CloudTrail トピック	サポート開始
Amazon WorkDocs	を使用した Amazon WorkDocs API コールのログ記録 AWS CloudTrail	2014 年 8 月 27 日
Amazon WorkMail	を使用した Amazon WorkMail API コールのログ記録 AWS CloudTrail	2017 年 12 月 12 日
Amazon WorkSpaces	を使用した Amazon WorkSpaces API コールのログ記録 CloudTrail	2015 年 4 月 9 日
Amazon WorkSpaces シンクライアント	を使用した Amazon WorkSpaces シンクライアント API コールのログ記録 AWS CloudTrail	11/26/2023
Amazon WorkSpaces Web	を使用した Amazon WorkSpaces Web API コールのログ記録 AWS CloudTrail	11/30/2021
Application Auto Scaling	を使用した Application Auto Scaling API コールのログ記録 AWS CloudTrail	2016 年 10 月 31 日
AWS Amplify	AWS CloudTrailを使用した Amplify API コールのログ記録	11/30/2020
AWS App Mesh	AWS CloudTrailを使用した App Mesh API コールのログ記録	AWS App Mesh 10/30/2019 App Mesh Envoy Management Service 2022 年 3 月 18 日
AWS App Runner	を使用した App Runner API コールのログ記録 AWS CloudTrail	05/18/2021

AWS サービス	CloudTrail トピック	サポート開始
AWS AppConfig	を使用した AWS AppConfig API コールのログ記録 AWS CloudTrail	管理イベント: 07/31/2020 データイベント: 01/04/2024
AWS AppFabric	を使用した AWS AppFabric API コールのログ記録 AWS CloudTrail	06/27/2023
AWS Application Cost Profiler	AWS Application Cost Profiler API リファレンス	05/13/2021
AWS Application Discovery Service	AWS CloudTrailでの Application Discovery Service API コールのログ記録	2016 年 5 月 12 日
AWS アプリケーション変換サービス	(Microservice Extractor for AWS .NET などの AWS ツールで使用されるバックエンドサービス)	08/26/2023
AWS AppSync	を使用した API コールのログ記録 AWS AppSyncAWS CloudTrail	2018 年 2 月 13 日
AWS Artifact	を使用した AWS Artifact API コールのログ記録 AWS CloudTrail	01/27/2023
AWS Audit Manager	を使用した AWS Audit Manager API コールのログ記録 AWS CloudTrail	12/07/2020
AWS Auto Scaling	を使用した AWS Auto Scaling API コールのログ記録 CloudTrail	2018 年 8 月 15 日

AWS サービス	CloudTrail トピック	サポート開始
AWS B2B データ交換	を使用した AWS B2B Data Interchange API コールのログ記録 AWS CloudTrail	12/01/2023
AWS Backup	を使用した API コールのログ記録 AWS BackupAWS CloudTrail	2019 年 2 月 4 日
AWS Batch	を使用した AWS Batch API コールのログ記録 AWS CloudTrail	2018 年 1 月 10 日
AWS Billing and Cost Management	を使用した AWS Billing and Cost Management API コールのログ記録 AWS CloudTrail	2018 年 6 月 7 日
AWS Billing Conductor	を使用した AWS Billing Conductor API コールのログ記録 AWS CloudTrail	03/12/2024
AWS BugBust	を使用した BugBust API コールのログ記録 CloudTrail	06/24/2021
AWS Certificate Manager	AWS CloudTrailを使用する	2016 年 3 月 25 日
AWS Clean Rooms	を使用した AWS Clean Rooms API コールのログ記録 AWS CloudTrail	03/21/2023
AWS Cloud Map	を使用した AWS Cloud Map API コールのログ記録 AWS CloudTrail	2018 年 11 月 28 日
AWS Cloud9	を使用した AWS Cloud9 API コールのログ記録 AWS CloudTrail	2019 年 1 月 21 日

AWS サービス	CloudTrail トピック	サポート開始
AWS CloudFormation	での AWS CloudFormation API コールのログ記録 AWS CloudTrail	2014 年 4 月 2 日
AWS CloudHSM	を使用した AWS CloudHSM API コールのログ記録 AWS CloudTrail	2015 年 1 月 8 日
AWS CloudShell	でのログ記録とモニタリング AWS CloudShell	12/15/2020
AWS CloudTrail	AWS CloudTrail API リファレンス (すべての CloudTrail API コールは によってログに記録されます) CloudTrail。	2013 年 11 月 13 日
AWS CodeArtifact	を使用した CodeArtifact API コールのログ記録 AWS CloudTrail	06/10/2020
AWS CodeBuild	を使用した AWS CodeBuild API コールのログ記録 AWS CloudTrail	2016 年 12 月 1 日
AWS CodeCommit	を使用した API コールのログ記録 AWS CodeCommitAWS CloudTrail	2017 年 1 月 11 日
AWS CodeDeploy	によるデプロイのモニタリング AWS CloudTrail	2014 年 12 月 16 日
AWS CodePipeline	を使用した CodePipeline API コールのログ記録 AWS CloudTrail	2015 年 7 月 9 日

AWS サービス	CloudTrail トピック	サポート開始
AWS CodeStar	を使用した AWS CodeStar API コールのログ記録 AWS CloudTrail	2017 年 6 月 14 日
AWS CodeStar 通知	を使用した AWS CodeStar 通知 API コールのログ記録 AWS CloudTrail	2019 年 11 月 5 日
AWS Config	を使用した AWS Config API コールのログ記録 AWS CloudTrail	2015 年 2 月 10 日
AWS コントロールカタログ	を使用した AWS Control Catalog API コールのログ記録 AWS CloudTrail	04/08/2024
AWS Control Tower	を使用した AWS Control Tower アクションのログ記録 AWS CloudTrail	2019-08-12
AWS Data Pipeline	を使用した AWS Data Pipeline API コールのログ記録 AWS CloudTrail	2014 年 12 月 2 日
AWS Database Migration Service (AWS DMS)	を使用した AWS Database Migration Service API コールのログ記録 AWS CloudTrail	2016 年 2 月 4 日
AWS DataSync	を使用した AWS DataSync API コールのログ記録 AWS CloudTrail	2018 年 11 月 26 日
AWS Deadline クラウド	を使用した通話のログ記録 CloudTrail	04/02/2024

AWS サービス	CloudTrail トピック	サポート開始
AWS Device Farm	を使用した AWS Device Farm API コールのログ記録 AWS CloudTrail	2015 年 7 月 13 日
AWS Direct Connect	での AWS Direct Connect API コールのログ記録 AWS CloudTrail	2014 年 3 月 8 日
AWS Directory Service	を使用した AWS Directory Service API コールのログ記録 CloudTrail	2015 年 5 月 14 日
AWS Elastic Beanstalk (Elastic Beanstalk)	での Elastic Beanstalk API コールの使用 AWS CloudTrail	2014 年 3 月 31 日
AWS Elastic Disaster Recovery	を使用した AWS Elastic Disaster Recovery API コールのログ記録 AWS CloudTrail	11/17/2021
AWS Elemental MediaConnect	を使用した AWS Elemental MediaConnect API コールのログ記録 AWS CloudTrail	2018 年 11 月 27 日
AWS Elemental MediaConvert	を使用した AWS Elemental MediaConvert API コールのログ記録 CloudTrail	2017 年 11 月 27 日
AWS Elemental MediaLive	を使用した API コールのログ記録 MediaLive AWS CloudTrail	2019 年 1 月 19 日
AWS Elemental MediaPackage	を使用した AWS Elemental MediaPackage API コールのログ記録 AWS CloudTrail	2018 年 12 月 21 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Elemental MediaStore	を使用した AWS Elemental MediaStore API コールのログ記録 CloudTrail	2017 年 11 月 27 日
AWS Elemental MediaTailor	を使用した AWS Elemental MediaTailor API コールのログ記録 AWS CloudTrail	2019 年 2 月 11 日
AWS エンティティ解決	A を使用した AWS エンティティ解決 API コールのログ記録AWS CloudTrail	07/26/2023
AWS Fault Injection Service	を使用した API コールのログ記録 AWS CloudTrail	03/15/2021
AWS Firewall Manager	を使用した AWS Firewall Manager API コールのログ記録 AWS CloudTrail	2018 年 4 月 5 日
AWS Global Accelerator	を使用した AWS Global Accelerator API コールのログ記録 AWS CloudTrail	2018 年 11 月 26 日
AWS Glue	を使用したオペレーションのログ記録 AWS GlueAWS CloudTrail	2017 年 11 月 7 日
AWS Ground Station	を使用した AWS Ground Station API コールのログ記録 AWS CloudTrail	2019/05/31
AWS Health	を使用した AWS Health API コールのログ記録 AWS CloudTrail	2016 年 11 月 21 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Health Dashboard	を使用した AWS Health API コールのログ記録 AWS CloudTrail	2016 年 12 月 1 日
AWS HealthImaging	を使用した AWS HealthImaging API コールのログ記録 AWS CloudTrail	07/26/2023
AWS HealthLake	を使用した AWS HealthLake API コールのログ記録 AWS CloudTrail	12/07/2020
AWS HealthOmics	を使用した AWS HealthOmics API コールのログ記録 AWS CloudTrail	11/29/2022
AWS IAM Identity Center	を使用した IAM Identity Center API コールのログ記録 AWS CloudTrail	2017 年 12 月 7 日
AWS Identity and Access Management (IAM)	を使用した IAM イベントのログ記録 AWS CloudTrail	2013 年 11 月 13 日
AWS IoT	を使用した AWS IoT API コールのログ記録 AWS CloudTrail	2016 年 4 月 11 日
AWS IoT 1-Click	を使用した AWS IoT 1-Click API コールのログ記録 AWS CloudTrail	2018 年 5 月 14 日
AWS IoT 分析	を使用した AWS IoT Analytics API コールのログ記録 AWS CloudTrail	2018 年 4 月 23 日
AWS IoT イベント	を使用した AWS IoT Events API コールのログ記録 AWS CloudTrail	2019 年 6 月 11 日

AWS サービス	CloudTrail トピック	サポート開始
AWS IoT Greengrass	を使用した AWS IoT Greengrass API コールのログ記録 AWS CloudTrail	2018 年 10 月 29 日
AWS IoT Greengrass V2	で AWS IoT Greengrass V2 API コールをログに記録する AWS CloudTrail	12/14/2020
AWS IoT SiteWise	を使用した AWS IoT SiteWise API コールのログ記録 AWS CloudTrail	04/29/2020
AWS Key Management Service (AWS KMS)	を使用した API コールのログ記録 AWS KMSAWS CloudTrail	2014 年 11 月 12 日
AWS Lake Formation	を使用した AWS Lake Formation API コールのログ記録 AWS CloudTrail	08/09/2019
AWS Lambda	を使用した AWS Lambda API コールのログ記録 AWS CloudTrail	管理イベント: 2015 年 4 月 9 日 データイベント: 2017 年 11 月 30 日
AWS Launch Wizard	を使用した AWS Launch Wizard API コールのログ記録 AWS CloudTrail	11/08/2023
AWS License Manager	を使用した AWS License Manager API コールのログ記録 AWS CloudTrail	2019 年 3 月 1 日
AWS Mainframe Modernization	を使用した AWS Mainframe Modernization API コールのログ記録 AWS CloudTrail	06/08/2022

AWS サービス	CloudTrail トピック	サポート開始
AWS Managed Services	AMS Accelerate でのログ管理	2016 年 12 月 21 日
AWS Marketplace 契約	を使用した契約 API コールのログ記録 AWS CloudTrail	09/01/2023
AWS Marketplace デプロイサービス	を使用した AWS Marketplace Deployment Service 呼び出しのログ記録 CloudTrail	11/29/2023
AWS Marketplace 検出	を使用した AWS Marketplace Discovery API コールのログ記録 AWS CloudTrail	12/15/2022
AWS Marketplace 計測サービス	を使用した AWS Marketplace API コールのログ記録 AWS CloudTrail	2018 年 8 月 22日
AWS Migration Hub	を使用した AWS Migration Hub API コールのログ記録 AWS CloudTrail	2017 年 8 月 14 日
AWS Network Firewall	を使用した AWS Network Firewall API への呼び出しのログ記録 AWS CloudTrail	11/17/2020
AWS OpsWorks for Chef Automate	を使用した AWS OpsWorks for Chef Automate API コールのログ記録 AWS CloudTrail	2018 年 7 月 16 日
AWS OpsWorks for Puppet Enterprise	OpsWorks を使用した Puppet Enterprise API コールのログ記録 AWS CloudTrail	2018 年 7 月 16 日
AWS OpsWorks Stacks	を使用した AWS OpsWorks Stacks API コールのログ記録 AWS CloudTrail	2014 年 6 月 4 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Organizations	を使用した AWS Organizations API コールのログ記録 AWS CloudTrail	2017 年 2 月 27 日
AWS Outposts	を使用した AWS Outposts API コールのログ記録 AWS CloudTrail	02/04/2020
AWS Panorama	AWS Panorama API リファレンス	10/20/2021
AWS Payment Cryptography	を使用した AWS Payment Cryptography API コールのログ記録 AWS CloudTrail	06/08/2023
AWS プライベート 5G	を使用した AWS プライベート 5G API コールのログ記録 AWS CloudTrail	08/11/2022
AWS Private Certificate Authority (AWS Private CA)	の使用 CloudTrail	2018 年 4 月 4 日
AWS Proton	でのログ記録とモニタリング AWS Proton	06/09/2021
AWS re:Post プライベート	を使用した AWS re:Post プライベート API コールのログ記録 AWS CloudTrail	11/26/2023
AWS Resilience Hub	AWS CloudTrail	11/10/2021
AWS Resource Access Manager (AWS RAM)	を使用した AWS RAM API コールのログ記録 AWS CloudTrail	2018 年 11 月 20 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Resource Explorer	を使用した AWS Resource Explorer API コールのログ記録 AWS CloudTrail	11/07/2022
AWS Resource Groups	Resource Groups でのログ記録とモニタリング	2018 年 6 月 29 日
AWS RoboMaker	を使用した AWS RoboMaker API コールのログ記録 AWS CloudTrail	2019 年 1 月 16 日
AWS Secrets Manager	AWS Secrets Manager シークレットの使用をモニタリングする	2018 年 4 月 5 日
AWS Security Hub	を使用した AWS Security Hub API コールのログ記録 AWS CloudTrail	2018 年 11 月 27 日
AWS Security Token Service (AWS STS)	を使用した IAM イベントのログ記録 AWS CloudTrail IAM トピックには、 に関する情報が含まれています AWS STS。	2013 年 11 月 13 日
AWS Serverless Application Repository	を使用した API コールのログ記録 AWS Serverless Application RepositoryAWS CloudTrail	2018 年 2 月 20 日
AWS Service Catalog	を使用した Service Catalog API コールのログ記録 AWS CloudTrail	2016 年 7 月 6 日
AWS Shield	を使用した Shield Advanced API コールのログ記録 AWS CloudTrail	2018 年 2 月 8 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Snowball エッジ	を使用した AWS Snowball Edge API コールのログ記録 AWS CloudTrail	2019 年 1 月 25 日
AWS Step Functions	を使用した AWS Step Functions API コールのログ記録 AWS CloudTrail	2016 年 12 月 1 日
AWS Storage Gateway	を使用した Storage Gateway API コールのログ記録 AWS CloudTrail	2014 年 12 月 16 日
AWS Support	を使用した AWS Support API コールのログ記録 AWS CloudTrail	2016 年 4 月 21 日
AWS Support 推奨事項 (プレビュー)	を使用した AWS Support Recommendations API コールのログ記録 AWS CloudTrail	05/22/2024
AWS Systems Manager	を使用した AWS Systems Manager API コールのログ記録 AWS CloudTrail	2017 年 11 月 29 日
AWS Systems Manager Incident Manager	を使用した AWS Systems Manager Incident Manager API コールのログ記録 AWS CloudTrail	05/10/2021
AWS 通信ネットワークビルダー (AWS TNB)	を使用した AWS Telco Network Builder API コールのログ記録 AWS CloudTrail	02/21/2023
AWS Transfer for SFTP	を使用した AWS Transfer for SFTP API コールのログ記録 AWS CloudTrail	2019 年 1 月 8 日

AWS サービス	CloudTrail トピック	サポート開始
AWS Transit Gateway	Logging API Calls for Your Transit Gateway Using AWS CloudTrailを使用した転送ゲートウェイの API コールのログ記録	2018 年 11 月 26 日
AWS Trusted Advisor	を使用した AWS Trusted Advisor コンソールアクションのログ記録 AWS CloudTrail	10/22/2020
AWS Verified Access	を使用した AWS Verified Access API コールのログ記録 AWS CloudTrail	04/27/2023
AWS WAF	を使用した API コールのログ記録 AWS WAFAWS CloudTrail	2016 年 4 月 28 日
AWS Well-Architected Tool	を使用した AWS Well-Architected Tool API コールのログ記録 AWS CloudTrail	12/15/2020
AWS X-Ray	を使用した AWS X-Ray API コールのログ記録 CloudTrail	2018 年 4 月 25 日
Elastic Load Balancing	AWS CloudTrail Classic Load Balancer のログ記録と AWS CloudTrail Application Load Balancer のログ記録	2014 年 4 月 4 日
FreeRTOS 無線通信経由更新 (OTA)	を使用した AWS IoT OTA API コールのログ記録 AWS CloudTrail	2019 年 5 月 22 日
Service Quotas	を使用した Service Quotas API コールのログ記録 AWS CloudTrail	06/24/2019

CloudTrail サポートされていないサービス

プレビュー段階のサービス、まだ一般公開 (GA) されていないサービス、また、公開 API がないサービスは、サポートの対象とはみなされません。

さらに、以下の AWS サービスとイベントはサポートされていません。

- AWS Import/Export
- Amazon VPC エンドポイントのポリシー固有のイベント

サポートされているサービスのリストについては、 AWS 「」を参照してくださいAWS のサービストピック CloudTrail。

のクォータ AWS CloudTrail

以下の表では、その中のクォータ (以前は制限と呼ばれていました) について説明しています。CloudTrail CloudTrail には調整可能なクォータはありません。の他のクォータについては AWS、「サービスクォータ」を参照してください。AWS

リソース	デフォルトのクォータ	コメント
リージョンごとの追跡情報	5	このクォータを増やすことはできません。
API の取得、説明、一覧表示	1 秒あたり 10 件のトランザクション (TPS)	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。、CancelQuery 、LookupEvents ListInsightsMetricData PutAuditEvents 、および StartQuery API はこのカテゴリには含まれません。

リソース	デフォルトのクォータ	コメント
CancelQuery、 StartQuery API	1 秒あたり 3 件のトランザクション (TPS)	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。 このクォータを増やすことはできません。
LookupEvents API	1 秒あたり 2 件のトランザクション (TPS)	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。 このクォータを増やすことはできません。
ListInsightsMetricData API	1 秒あたりのトランザクション (TPS) は 1	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。 このクォータを増やすことはできません。
PutAuditEvents API	1 秒あたり 100 件のトランザクション (TPS)	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。 このクォータを増やすことはできません。
他のすべての API	1 秒あたりのトランザクション (TPS) は 1	スロットリングなしで 1 秒あたりに実行できるオペレーションリクエストの最大数。 このクォータを増やすことはできません。

リソース	デフォルトのクォータ	コメント
イベントデータストア	10	1 つの AWS リージョン に設定できるイベントデータストアの最大数。これには、そのリージョンの単一リージョンイベントデータストアだけでなく、すべての AWS リージョンにわたるマルチリージョンイベントデータストアも含まれます。これには、すべてのライフサイクルステージのイベントデータストアも含まれます。 このクォータを増やすことはできません。
チャネル	25	このクォータは、外部のイベントソースとの CloudTrail Lake 統合に使用されるチャネルに適用され AWS、サービスにリンクされたチャネルには適用されません。 このクォータを増やすことはできません。
同時クエリ	10	Lake で同時に実行できる、キューに入っている、または実行中のクエリの最大数。CloudTrail このクォータを増やすことはできません。

リソース	デフォルトのクォータ	コメント
1 回のリクエストあたりのイベント数 PutAuditEvents	100	PutAuditEvents リクエストごとに最大 100 のアクティビティイベント (または最大 1 MB) を追加することが可能です。 このクォータを増やすことはできません。
イベントセレクタ	5/ 証跡	このクォータを増やすことはできません。
アドバンストイベントセレクタ	すべてのアドバンストイベントセレクタの 500 の条件	証跡またはイベントデータストアが高度なイベントセレクタを使用している場合、条件値の最大数はすべての高度なイベントセレクタにわたり 500 に設定されています。証跡またはイベントデータストアが、すべてのリソース (すべての S3 バケットまたはすべての Lambda 関数など) のデータイベントをログに記録しない限り、データリソースは 250 に制限されます。データリソースは、イベントセレクタに分散できますが、合計が 250 を超えることはできません。 このクォータを増やすことはできません。

リソース	デフォルトのクォータ	コメント
イベントセレクタのデータリソース	証跡情報にあるすべてのイベントセレクタ 250	イベントセレクタまたはアドバンストイベントセレクタを使用してデータイベントを制限する場合、証跡内のすべてのイベントセレクタにおいて、データリソースの合計数は 250 を超えることはできません。各イベントセレクタで設定可能なリソース数の制限は最大 250 です。この最大制限数は、データリソースの合計数がすべてのイベントセレクタにおいて 250 を超えていない場合に限り許可されています。 例: • イベントセレクタが 5 の証跡情報では、各設定で 50 のデータリソースが許可されています。(5*50=250) • イベントセレクタが 5 の証跡情報では、その内 3 つがデータリソース 50 で設定され、その 1 つはデータリソース 99 で設定、そしてもう 1 つはデータリソース 1 で設定することも許可されています。((3*50)+1+99=250) • イベントセレクタ 5 で設定されている証跡情報ですべてをデータリソース 100 に

リソース	デフォルトのクォータ	コメント
		設定することは許可されていません。(5*100=500) イベントセレクタは証跡にのみ適用されます。イベントデータストアには、高度なイベントセレクタを使用する必要があります。 このクォータを増やすことはできません。 すべての S3 バケットやすべての Lambda 関数など、すべてのリソースでデータイベントを口グに記録するように選択した場合、このクォータは適用されません。

リソース	デフォルトのクォータ	コメント
イベントサイズ	すべてのイベントバージョン:256 KB CloudWatch を超えるイベントはログに送信できない イベントバージョン 1.05 以降: 合計イベントサイズの制限 256 KB	Amazon CloudWatch ログとAmazon EventBridge ではそれぞれ 256 KB の最大イベントサイズを許可しています。 CloudTrail 256 KB CloudWatch を超えるイベントはログまたはに送信されません EventBridge。 イベントバージョン 1.05 で開始し、イベントの最大サイズは 256 KB です。これは、悪意のある攻撃者による悪用を防ぎ、イベントを CloudWatch Logs AWS EventBridge やなどの他のサービスで利用できるようにするためです。
CloudTrail Amazon S3 に送信されるファイルサイズ	圧縮後、50 MB の ZIP ファイル	管理イベントとデータイベントの両方で、最大 50 MB の (圧縮) ZIP ファイルで S3 CloudTrail にイベントを送信します。 トレイルで有効にすると、ZIP ファイルを S3 に送信した後に Amazon SNS CloudTrail からログ配信通知が送信されます。

AWS CloudTrail チュートリアルを始める

初めての方は AWS CloudTrail、これらのチュートリアルがその機能の使用方法を学ぶのに役立ちます。

トピック

- 使用権限を付与してください CloudTrail
- イベント履歴を表示する
- 管理イベントを記録する証跡を作成します。
- S3 データイベント用のイベントデータストアを作成します。
- トレイルイベントを CloudTrail Lake イベントデータストアにコピーします。
- Lake ダッシュボードを表示します。 CloudTrail
- CloudTrail Lake のサンプルクエリを表示して実行する
- CloudTrail Lake のクエリ結果を S3 バケットに保存する

使用権限を付与してください CloudTrail

トレイル、イベントデータストア、 CloudTrail チャネルなどのリソースを作成、更新、管理するには、 CloudTrail使用権限を付与する必要があります。このセクションでは、で利用できる管理ポリシーについて説明します。 CloudTrail

> **Note**
>
> CloudTrail 管理タスクを実行するためにユーザーに付与する権限は、Amazon S3 バケットにログファイルを配信したり、Amazon SNS CloudTrail トピックに通知を送信したりするために必要な権限とは異なります。これらのアクセス許可の詳細については、「の Amazon S3 バケットポリシー CloudTrail」を参照してください。
> Amazon Logs との統合を設定する場合は、Amazon CloudWatch Logs CloudTrail CloudWatch ロググループにイベントを配信するために引き受けられるロールも必要です。CloudTrail を使用するロールを作成する必要があります。詳細については、「コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与」および「CloudWatch ログへのイベントの送信」を参照してください。

AWS 以下の管理ポリシーを使用できます CloudTrail。

- AWSCloudTrail_FullAccess— このポリシーは、トレイル、イベントデータストア、 CloudTrail CloudTrail チャネルなどのリソースに対するアクションへのフルアクセスを提供します。このポリシーは、 CloudTrailトレイル、イベントデータストア、チャンネルの作成、更新、削除に必要な権限を付与します。

  このポリシーは、Amazon S3 バケット、ログのロググループ、 CloudWatch およびトレイル用の Amazon SNS トピックを管理するためのアクセス権限も提供します。ただし、`AWSCloudTrail_FullAccess`管理ポリシーには Amazon S3 バケット、 CloudWatch Logs のロググループ、または Amazon SNS トピックを削除するアクセス権限は提供されません。AWS 他のサービスの管理ポリシーについては、『AWS 管理ポリシーリファレンスガイド』を参照してください。

  > **Note**
  >
  > AWSCloudTrail_FullAccessこのポリシーは、組織全体で広く共有されることを意図したものではありません。 AWS アカウントこのロールを持つユーザーは、 AWS アカウントで最も機密かつ重要な監査機能を無効にしたり、再設定したりすることができます。このため、このポリシーはアカウント管理者にのみ適用する必要があります。このポリシーの使用を厳重に管理および監視する必要があります。

- AWSCloudTrail_ReadOnlyAccess— このポリシーは、最近のイベントやイベント履歴など、CloudTrail コンソールを閲覧する権限を付与します。また、このポリシーにより、既存の証跡、イベントデータストア、およびチャネルを表示することもできます。このポリシーが適用されているロールとユーザーはイベント履歴をダウンロードできますが、証跡、イベントデータストア、またはチャンネルを作成または更新することはできません。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーとグループ AWS IAM Identity Center:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。

- IAM ユーザー:

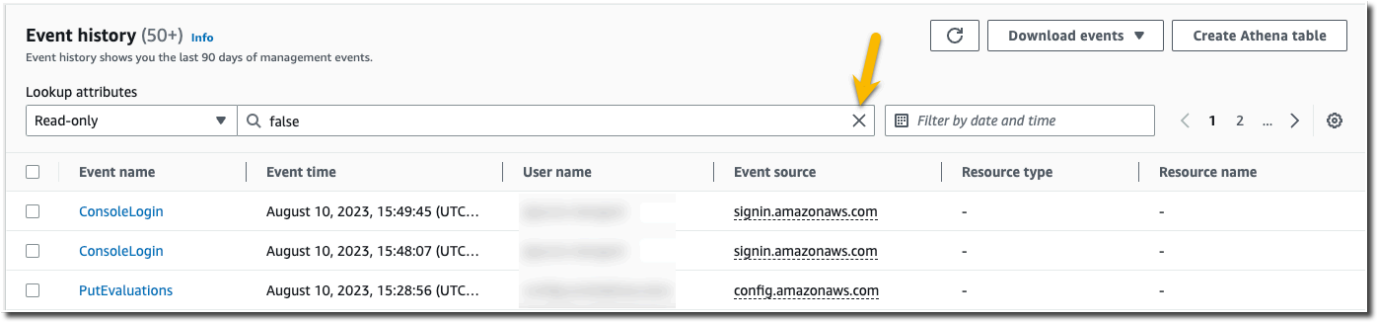
- ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。詳細については、「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

イベント履歴を表示する

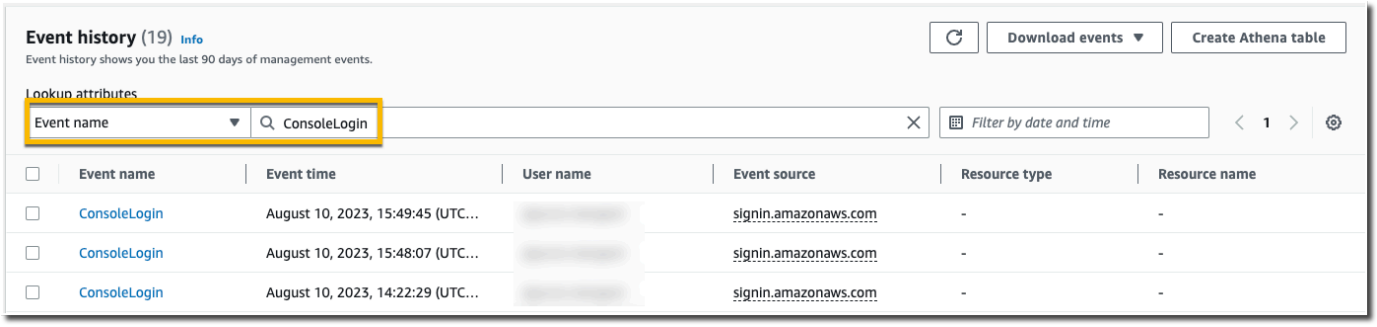
このセクションでは、 CloudTrail CloudTrail コンソールのイベント履歴ページを使用して、現在の過去 90 日間の管理イベントを表示する方法について説明します AWS リージョン。 AWS アカウント

イベント履歴を表示するには

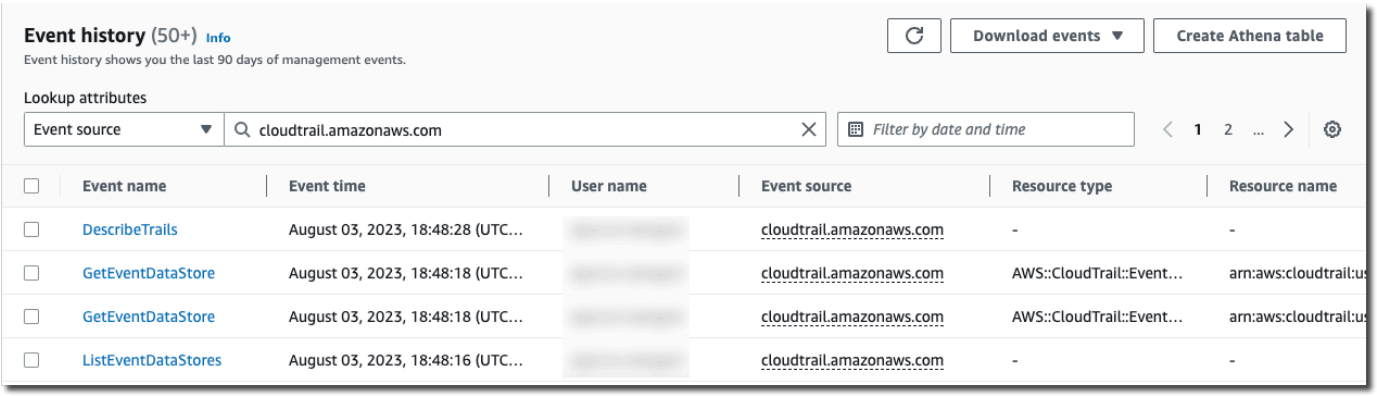
1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインで [Event history (イベント履歴)] を選択します。最新のイベントが最初に表示された、フィルタリングされたイベントのリストが表示されます。イベントのデフォルトのフィルターは読み取り専用で、[false] に設定されています。このフィルターをクリアするには、フィルターの右側にある [X] をクリックします。[イベント履歴] 内のイベントは、単一の属性でイベントをフィルタリングして検索できます。



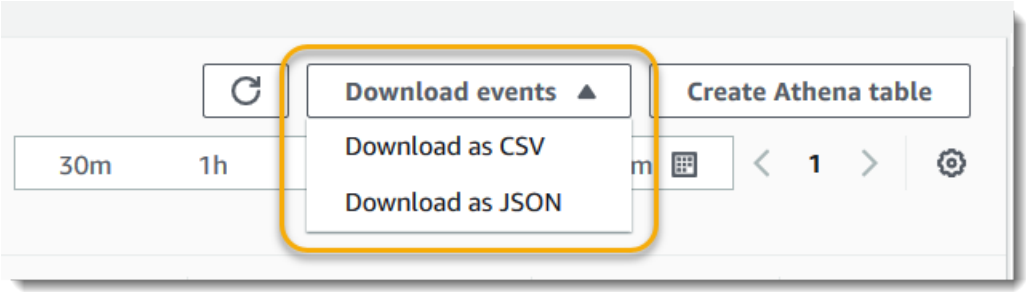
3. フィルターする属性を選択し、その属性の値をすべて入力します。 CloudTrail 値の一部ではフィルタリングできません。たとえば、コンソールのログインイベントをすべて表示するには、イベント名フィルターを選択し、属性値を指定しますConsoleLogin。



または、 CloudTrail 最近の管理イベントを表示するには、[イベントソース] を選択して指定しますcloudtrail.amazonaws.com。



4. 特定の管理イベントを表示するには、イベント名を選択します。イベントの詳細ページでは、イベントの詳細を表示したり、参照されているリソースを表示したり、イベントレコードを表示したりできます。
5. イベントを比較するには、[イベント履歴] テーブルの左余白のチェックボックスをオンにして、最大 5 つのイベントを選択します。選択したイベントの詳細は、「イベント詳細の比較」 side-by-side テーブルで確認できます。
6. イベント履歴を保存するには、CSV または JSON 形式のファイルとしてダウンロードします。イベント履歴のダウンロードには数分かかることがあります。



詳細については、「CloudTrail イベント履歴の操作」を参照してください。

管理イベントを記録する証跡を作成します。

初めてのトレイルでは、AWS すべてのリージョンの管理イベントをすべて記録し、データイベントは記録しないトレイルを作成することをおすすめします。管理イベントの例には、IAM `CreateUser` や `AttachRolePolicy` イベントなどのセキュリティイベント、`RunInstances` や `CreateBucket` などのリソースイベントが含まれています。 CloudTrail コンソールでの証跡作成の一部として、証跡のログファイルを保存する Amazon S3 バケットを作成します。

> **Note**
>
> このチュートリアルでは、最初の証跡を作成することを前提としています。 AWS アカウントにある証跡の数と、それらの証跡の設定方法によっては、以下の手順で費用が発生する場合と発生しない場合があります。 CloudTrail ログファイルを Amazon S3 バケットに保存しますが、これにはコストがかかります。料金の詳細については、「AWS CloudTrail の料金」および「Amazon S3 の料金」を参照してください。

追跡を作成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. 地域セレクターで、 AWS 証跡を作成したい地域を選択します。これは、証跡のホームリージョン です。

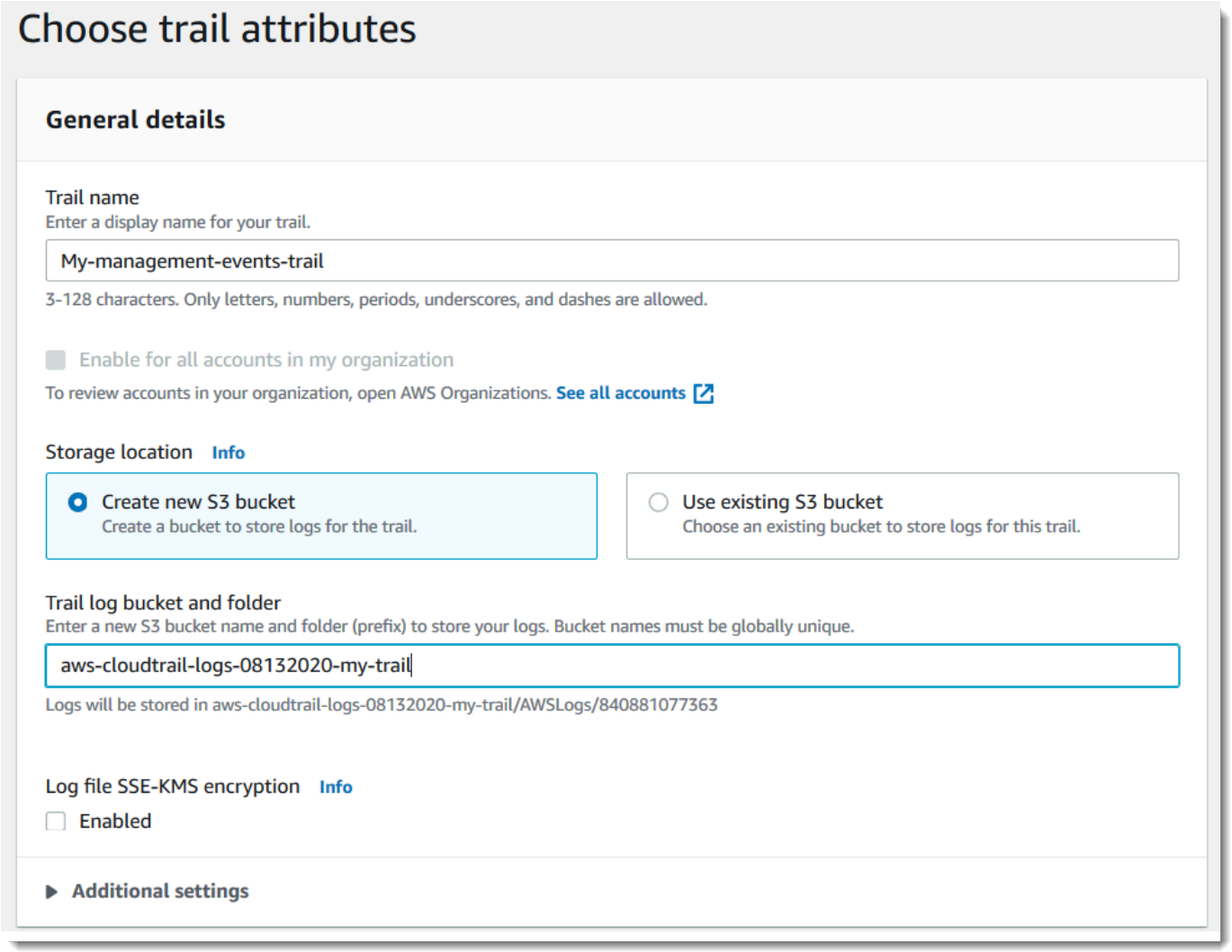
   > **Note**
   >
   > AWS トレイルがすべてのリージョンのイベントを記録している場合でも、 AWS トレイルの作成後にトレイルを表示および更新できるのはホームリージョンのみです。

3. CloudTrail サービスのホームページ、「証跡」ページ、または「ダッシュボード」ページの「証跡を作成」セクションで、「証跡を作成」を選択します。
4. [Trail name (証跡名)] で、証跡に*`My-Management-Events-Trail`* などの名前を付けます。追跡の目的をすぐに識別できる名前を使用するのがベストプラクティスです。この例では、管理イベントを口グに記録する追跡を作成しています。
5. [組織内のすべてのアカウントで有効化] は、デフォルト設定のままにします。このオプションは、Organizations でアカウントを設定しない限り、変更できません。

6. [ストレージの場所] で、[新しい S3 バケットを作成する] を選択すると、新しいバケットが作成されます。バケットを作成したら、 CloudTrail 必要なバケットポリシーを作成して適用します。新しい S3 バケットを作成する場合、デフォルトではバケットのサーバー側の暗号化が有効になっているため、IAM `s3:PutEncryptionConfiguration` ポリシーにアクションの権限を含める必要があります。バケットには識別しやすい名前を付けてください。

   ログを見つけやすくするために、既存のバケットに新しいフォルダー (プレフィックスとも呼ばれる) CloudTrail を作成してログを保存します。

   > **Note**
   >
   > Amazon S3 バケットの名前はグローバルで一意であることが必要です。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの名前付け」を参照してください。

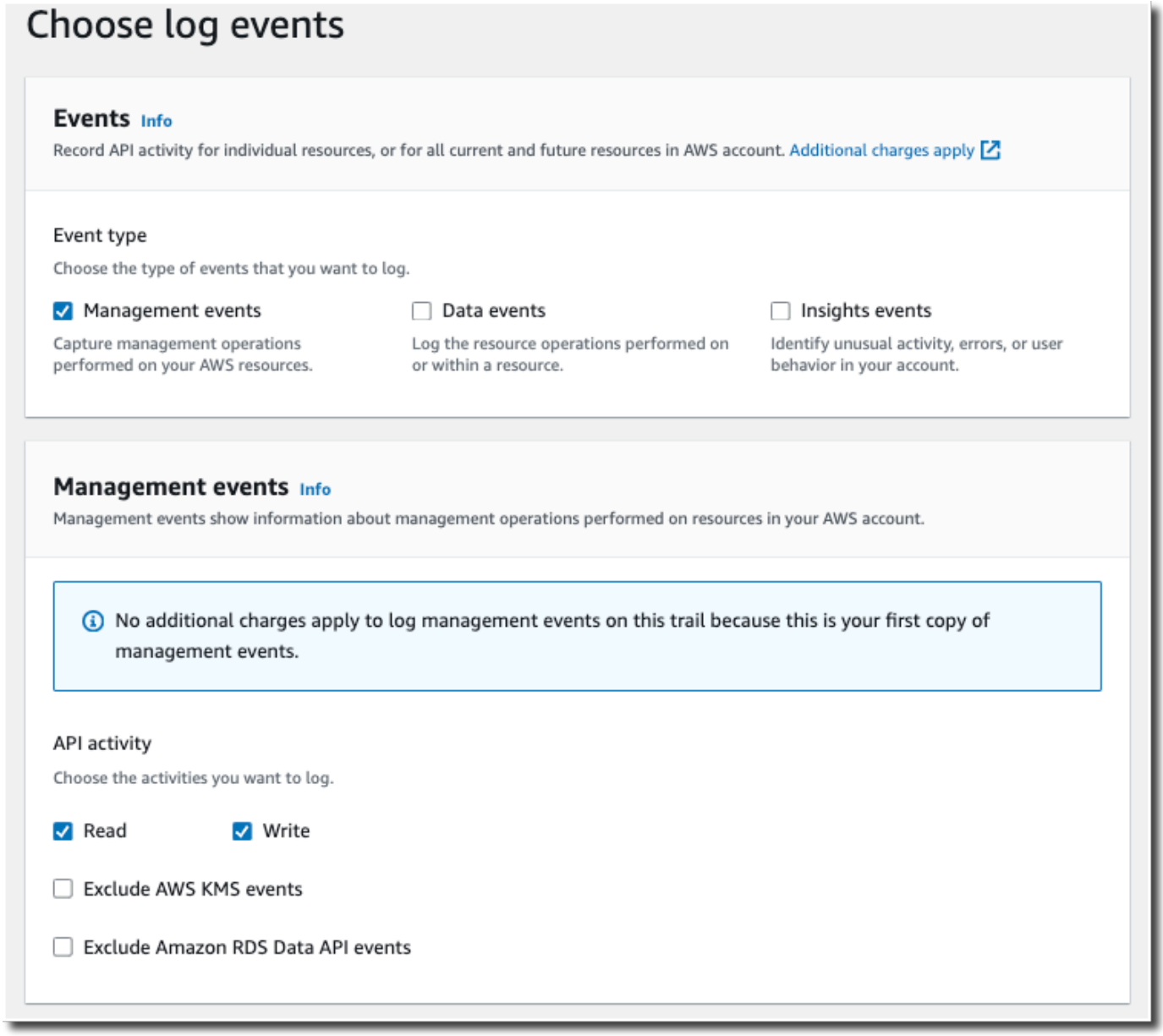


7. [ログファイル SSE-KMS 暗号化] を無効にするには、このチェックボックスをオフにします。デフォルトでは、SSE-S3 の暗号化を使用して、ログファイルが暗号化されます。この設定の詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の使用」を参照してください。
8. [Additional settings] はデフォルト設定のままにします。
9. Logs はデフォルト設定のままにしておきます。CloudWatch 今のところ、Amazon CloudWatch ログにログを送信しないでください。
10. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) を証跡に追加します。タグは、 CloudTrail トレイルやその他のリソース (CloudTrail ログファイルを含む Amazon S3 バケットなど) を識別するのに役立ちます。例えば、**`Compliance`** という名前の **`Auditing`** という値のタグをアタッチできます。

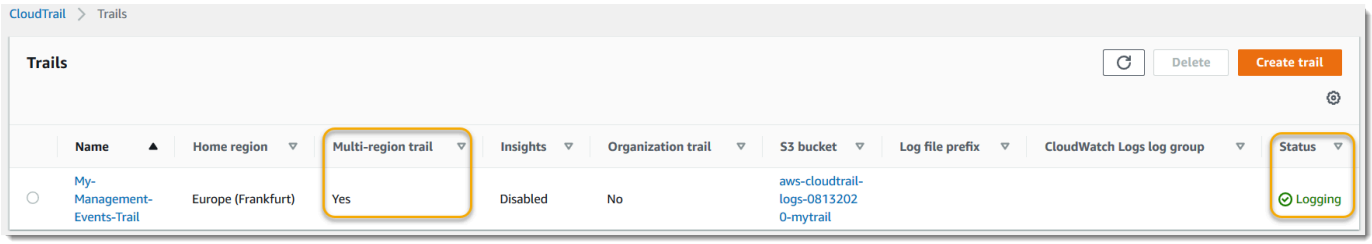
> **Note**
>
> コンソールでトレイルを作成するときにタグを追加したり、Amazon S3 CloudTrail バケットを作成してコンソールにログファイルを保存したりできますが、 CloudTrail コンソールから Amazon S3 バケットにタグを追加することはできません。 CloudTrail バケットへのタグの追加など、Amazon S3 バケットのプロパティの表示と変更の詳細については、「Amazon S3 ユーザーガイド」を参照してください。

タグの作成が完了したら、[Next] をクリックします。

11. [Choose log events] ページで、ログに記録するイベントタイプを選択します。この証跡では、[管理イベント] はそのままにしておきます。[管理イベント] 領域で、[読み取り] および [書き込み] イベントの両方をログに記録することをまだ選択していない場合は、選択します。すべての管理イベントをログに記録するには、[AWS KMS イベントを除外] と [Amazon RDS Data API イベントを除外] のチェックボックスを空白のままにします。



12. [データイベント] および [Insights イベント] の設定はデフォルトのままにしておきます。このトレイルでは、データや CloudTrail Insights イベントは記録されません。[次へ] をクリックします。
13. [確認と作成] ページで、詳細用に選択した設定を確認します。戻って変更するには、セクションの [Edit] を選クリックします。証跡を作成する準備ができたら、[Create trail] を選択します。
14. [証跡] ページには、新しい証跡がテーブルに表示されます。トレイルはマルチリージョン証跡に設定され、ログ記録はデフォルトで有効になっています。



ログファイルの表示

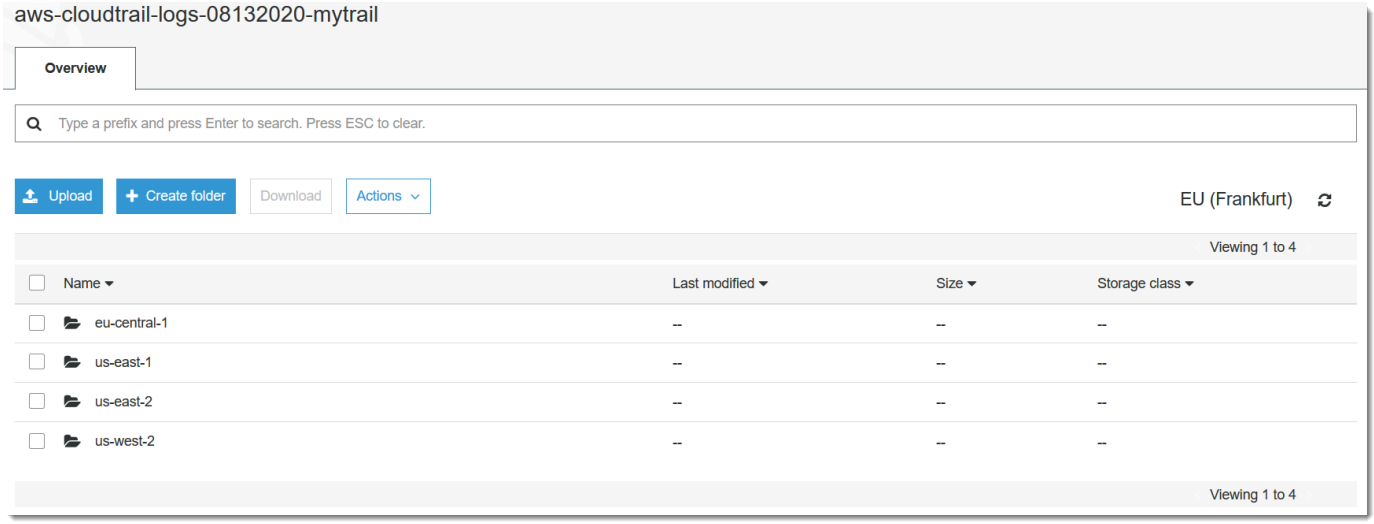
最初の証跡を作成してから平均約 5 分以内に、最初のログファイルセットを証跡の Amazon S3 CloudTrail バケットに配信します。これらのファイルを確認して、含まれる情報についての情報取得などを行えます。

> **Note**
>
> CloudTrail 通常、API 呼び出しから平均約 5 分以内にログが配信されます。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。
> 証跡の設定を誤ると (S3 バケットにアクセスできないなど)、ログファイルを S3 バケットに 30 日間再配信しようとしますが、 CloudTrail attempted-to-deliver これらのイベントには標準料金が適用されます。 CloudTrail 証跡の不適切な設定による課金を避けるには、その証跡を削除する必要があります。

ログファイルの表示

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ のコンソールを開きます。 CloudTrail
2. ナビゲーションペインで、[Trails] (追跡) を選択します。[証跡] ページで、先ほど作成した証跡の名前を探します (例では、*My-Management-Events-Trail*)。
3. トレイルの行で、S3 バケットの値を選択します (この例では *aws-cloudtrail-logs-08132020-mytrail*)。
4. Amazon S3 コンソールが開き、ログファイルの最上位レベルにそのバケットが表示されます。AWS すべてのリージョンのイベントを記録するトレイルを作成したので、各リージョンのフォルダーを示すレベルで画面が開きます。*###### Amazon S3 ##################### AWS/##/##### ID/###* CloudTrail AWS ログファイルを確認したいリージョンのフォルダを

選択します。例えば、米国東部 (オハイオ) リージョンのログファイルを確認する場合は、[us-east-2] を選択します。



5. バケットフォルダ構造を、そのリージョンのアクティビティのログを確認する年、月、日に移動します その日には、多数のファイルがあります。 AWS ファイルの名前はアカウント ID で始まり、.gz拡張子で終わります。*########## ID # 123456789012 ########################:123456789012 _ _ us-east-2 _ 20190610T1255abcdeExample .json.gz#CloudTrail*

   これらのファイルを表示するには、ダウンロードして、解凍し、プレーンテキストエディタか JSON ビューアーで表示します。ブラウザによっては、.gz および JSON ファイルを直接表示することもできます。JSON ビューアを使用することをおすすめします。ログファイル内の情報を簡単に解析できるからです。 CloudTrail

次のステップの計画

証跡ができたので、 AWS アカウント内のイベントやアクティビティの継続的な記録にアクセスできるようになりました。この継続的な記録は AWS アカウントのための会計と監査のニーズを満たすのに役立ちます。しかし、 CloudTrail CloudTrail データを使ってできることはまだまだたくさんあります。

- 証跡データのセキュリティを強化してください。 CloudTrail証跡を作成すると、自動的に一定レベルのセキュリティが適用されます。ただし、データ安全性を確保するために実行できる追加のステップがあります。
  - デフォルトでは、トレイルの作成時に作成した Amazon S3 バケットには、 CloudTrail そのバケットにログファイルを書き込むことを許可するポリシーが適用されています。バケットには一

般にはアクセスできませんが、アカウント内のバケットの読み取りと書き込みの権限があれば、AWS AWS アカウント内の他のユーザーがアクセスできる可能性があります。バケットのポリシーを確認し、必要に応じて変更を加え、アクセスを制限します。詳細については、「Amazon S3 セキュリティのドキュメント」と「バケットを保護するためのチュートリアルの例」を参照してください。

- バケットに配信されるログファイルは、Amazon S3 CloudTrail が管理する暗号化キー (SSE-S3) による Amazon サーバー側の暗号化によって暗号化されます。直接管理可能なセキュリティレイヤーを提供するために、AWS KMS代わりに—マネージドキーによるサーバー側の暗号化 (SSE-KMS) をログファイルに使用することもできます。 CloudTrail で SSE-KMS を使用するには CloudTrail、KMS キー (とも呼ばれる) を作成して管理します。AWS KMS key詳細については、「 CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)」を参照してください。
- 追加のセキュリティ計画については、のセキュリティのベストプラクティスを確認してください。 CloudTrail

- データイベントをログに記録する証跡を作成します。1 つ以上の Amazon S3 バケットでオブジェクトが追加、取得、削除されたとき、DynamoDB テーブルで項目が追加、変更、削除されたとき、または 1 AWS Lambda つ以上の関数が呼び出されたときのロギングに関心がある場合、これらはデータイベントです。このチュートリアルの前半で作成した管理イベント証跡では、これらのタイプのイベントを記録しません。サポートされているリソースタイプの一部またはすべてについて、データイベントをログに記録するための記録を別に作成できます。詳細については、「データイベント」を参照してください。

  > **Note**
  >
  > データイベントのログ記録には追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

- CloudTrail Insights イベントをトレイルに記録します。 AWS CloudTrail インサイトは、CloudTrail 管理イベントを継続的に分析することで、API 呼び出しや API AWS エラー率に関連する異常なアクティビティをユーザーが特定して対応するのに役立ちます。 CloudTrail Insights は数学モデルを使用して、アカウントの API およびサービスイベントアクティビティの通常のレベルを判断します。これは、通常のパターンの外にある動作を特定し、Insights イベントを生成し、これらのイベントを証跡に選択した送信先 S3 バケットの `/CloudTrail-Insight` フォルダに配信します。 CloudTrail Insights の詳細については、を参照してくださいInsights イベントのログ記録。

> **Note**
>
> Insights イベントの記録には追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

- 特定のイベントが発生したときに通知されるように CloudWatch Logs アラームを設定します。CloudWatch ログを使用すると、 CloudTrailによってキャプチャされた特定のイベントを監視し、アラートを受信できます。例えば、セキュリティグループの変更、失敗した AWS Management Console サインインイベント、IAM ポリシーの変更など、主要なセキュリティおよびネットワーク関連の管理イベントをモニタリングできます。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。
- 分析ツールを使用して、 CloudTrail ログの傾向を特定できます。イベント履歴のフィルタは最近のアクティビティで特定のイベントまたはイベントタイプを見つけるのに役立ちますが、アクティビティをより長い期間にわたって検索する機能を提供しません。より深い、より詳細な分析には、Amazon Athena を使用できます。詳細については、Amazon Athena ユーザーガイドの「AWS CloudTrail ログのクエリ」を参照してください。

S3 データイベント用のイベントデータストアを作成します。

イベントデータストアを作成して、 CloudTrail イベント (管理イベント、データイベント)、CloudTrail Insights イベント、AWS Audit Manager 証拠、AWS Config 設定項目、AWS または非イベントを口グに記録できます。

データイベント用のイベントデータストアを作成するときは、 AWS のサービス データイベントを記録したいリソースタイプとリソースタイプを選択します。 AWS のサービス その口グデータイベントの詳細については、を参照してくださいデータイベント。

このウォークスルーでは、Amazon S3 データイベント用のイベントデータストアを作成する方法を示します。このチュートリアルでは、すべての Amazon S3 データイベントを口グに記録するのではなく、カスタム口グセレクターテンプレートを選択し、特定の S3 バケットからオブジェクトが削除された場合にのみイベントの口グを記録します。

CloudTrail Lake イベントデータストアには料金がかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail コストの価格設定と管理については、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

S3 データイベント用にイベントデータストアを作成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail にあるコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [イベントデータストアの設定] ページの [一般的な詳細] で、イベントデータストアに *s3-data-events-eds* などの名前を付けます。イベントデートストアの意図をすぐに識別できる名前を使用するのがベストプラクティスです。 CloudTrail 命名要件については、を参照してください命名の要件。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、 pay-as-you-go 価格設定で保存期間の延長が可能になります。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントが指定された保存期間内かどうかをチェックして、イベントを保持するかどうかを決定します。`eventTime`例えば、保存期間を 90 日に指定した場合、90 CloudTrail `eventTime` 日以上経過したイベントは削除されます。

7. (オプション) [暗号化] で、独自の KMS キーを使用してイベントデータストアを暗号化するかどうかを選択します。デフォルトでは、イベントデータストア内のすべてのイベントは、 AWS ユーザーが所有および管理する KMS CloudTrail キーを使用して暗号化されます。

   独自の KMS キーを使用して暗号化を有効にするには、[独自の AWS KMS key を使用する] を選択します。[新規] AWS KMS key を選択して自動的に作成するか、[既存] を選択して既存の KMS キーを使用します。「KMS エイリアスの入力」 で、エイリアスを次の形式で指定します。`alias/` *`MyAliasName`* 独自の KMS キーを使用するには、KMS キーポリシーを編集して、CloudTrail ログの暗号化と復号化を許可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。AWS KMS の主要ポリシーの設定 CloudTrail CloudTrail AWS KMS マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、 AWS KMS 暗号化と復号化にコストがかかります。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > AWS Key Management Service 組織のイベントデータストアの暗号化を有効にするには、管理アカウント用の既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンは、クエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 CloudTrail 必要な権限を持つロールが自動的に作成されます。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

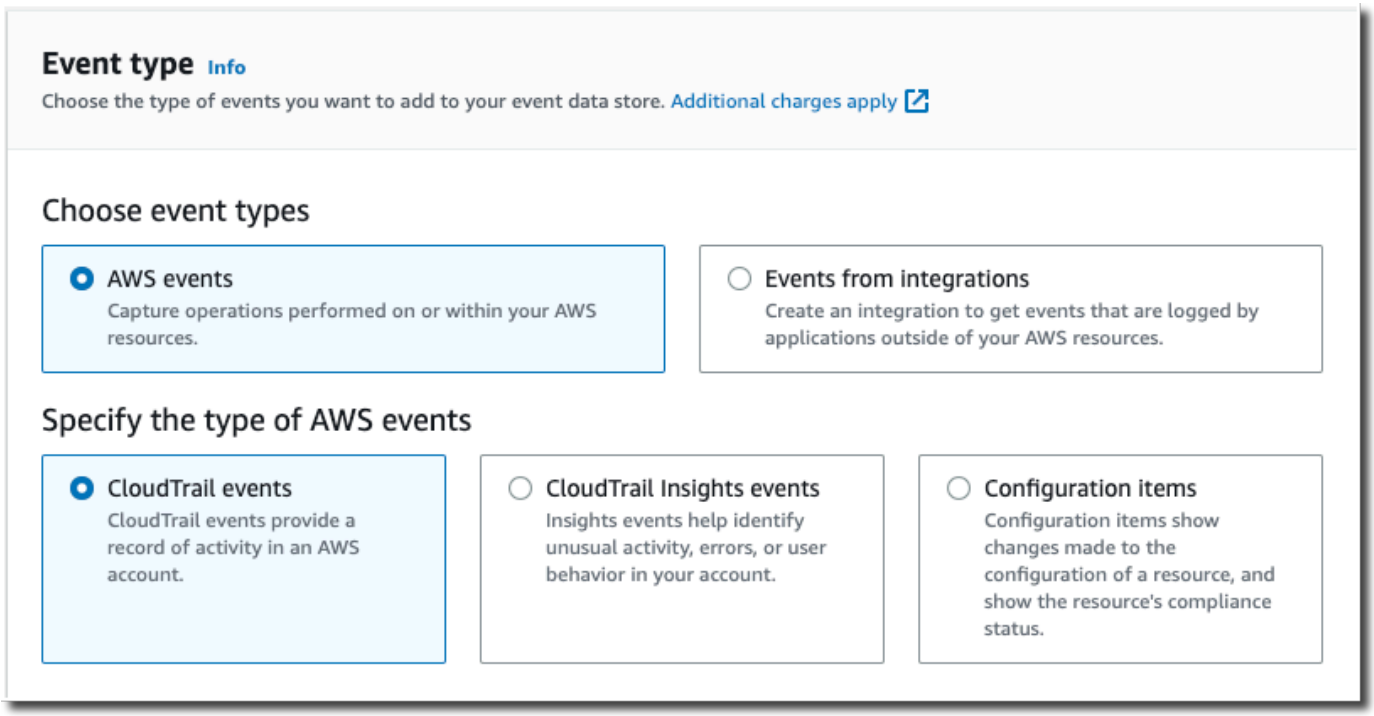
c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) をデータセットに追加します。 CloudTrail タグはイベントデータストアを識別するのに役立ちます。例えば、**stage** という名前の **prod** という値のタグをアタッチできます。タグを使用して、イベントデータストアへのアクセスを制限できます。タグを使用して、イベントデータストアのクエリコストと取り込みコストを追跡することもできます。

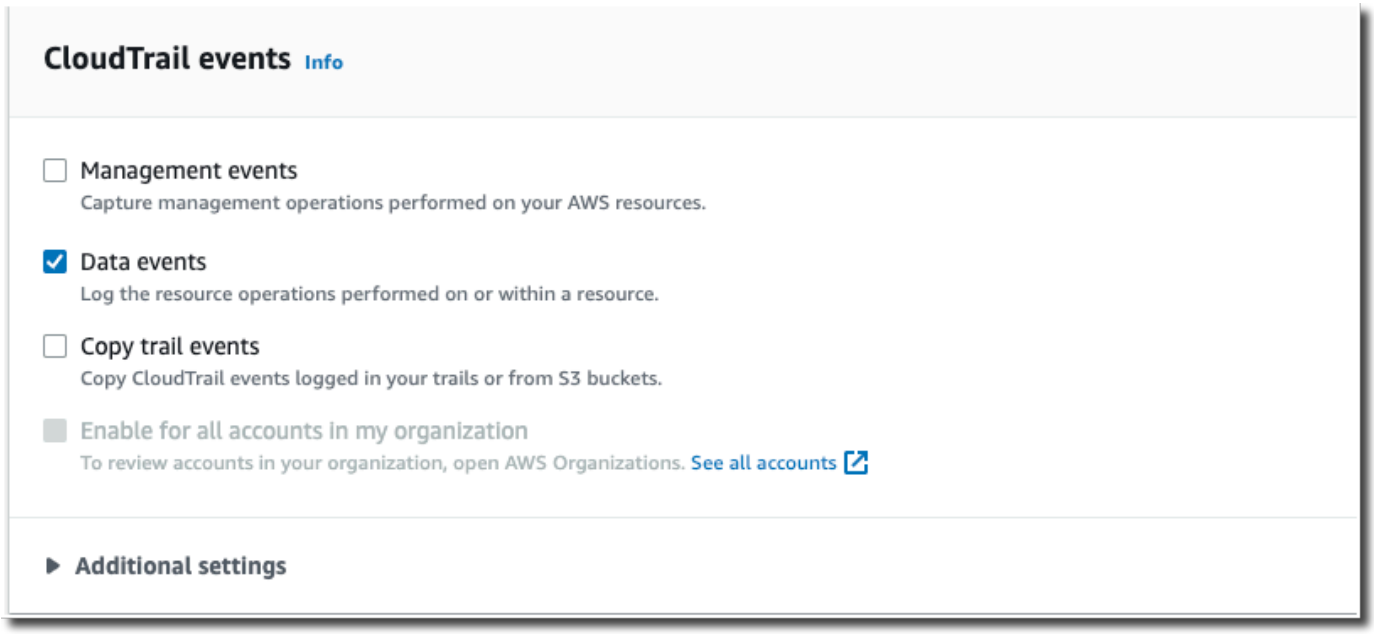
   タグを使用してコストを追跡する方法については、「CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法については AWS、『リソースへのタグ付け』ユーザーガイドの「 AWS AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. [イベントの選択]ページで、[イベントタイプ] はデフォルトの選択のままにします。



12. CloudTrail イベントの場合は、[データイベント] を選択し、[管理イベント] を選択解除します。データイベントの詳細については、「データイベントを口グ記録する」を参照してください。

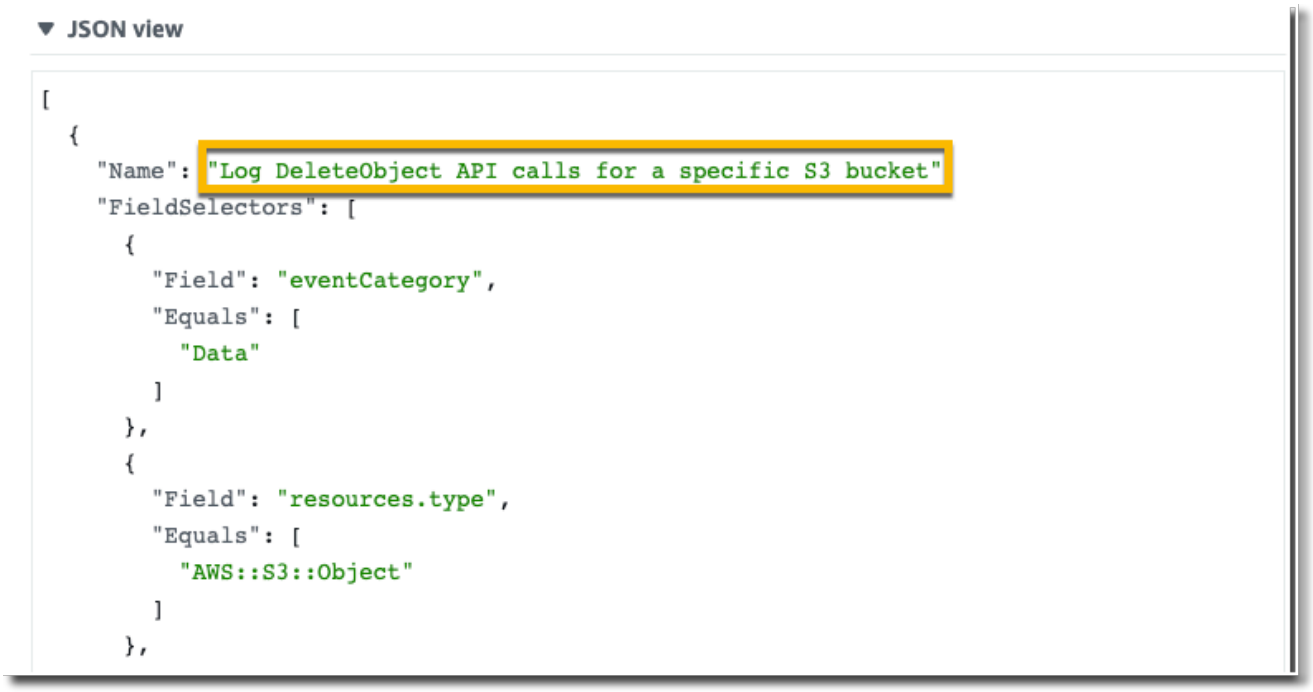


13. [証跡イベントのコピー] は、デフォルト設定のままにします。このオプションを使用して、既存の証跡イベントをイベントデータストアにコピーします。詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。
14. 組織のイベントデートストアの場合は、[組織内の全アカウントで有効にする] を選択します。このオプションは、 AWS Organizations でアカウントを設定していない場合は変更できません。
15. [追加設定] は、デフォルトの選択のままにします。デフォルトでは、 AWS リージョン イベントデータストアはすべてのイベントを収集し、作成時にイベントの取り込みを開始します。
16. [データイベント]で、次のように項目を選びます。

    a. [データイベントタイプ] に、[S3] を選択します。データイベントタイプは AWS のサービス 、データイベントが記録されるリソースを識別します。

    b. [ログセレクターテンプレート]、で [カスタム] を選択します。[カスタム] を選択すると、`eventName`、`resources.ARN`、`readOnly` フィールドのフィルタリングを行うカスタムイベントセレクターを定義できます。これらのフィールドについて詳しくは、AWS CloudTrail API AdvancedFieldSelectorリファレンスのを参照してください。

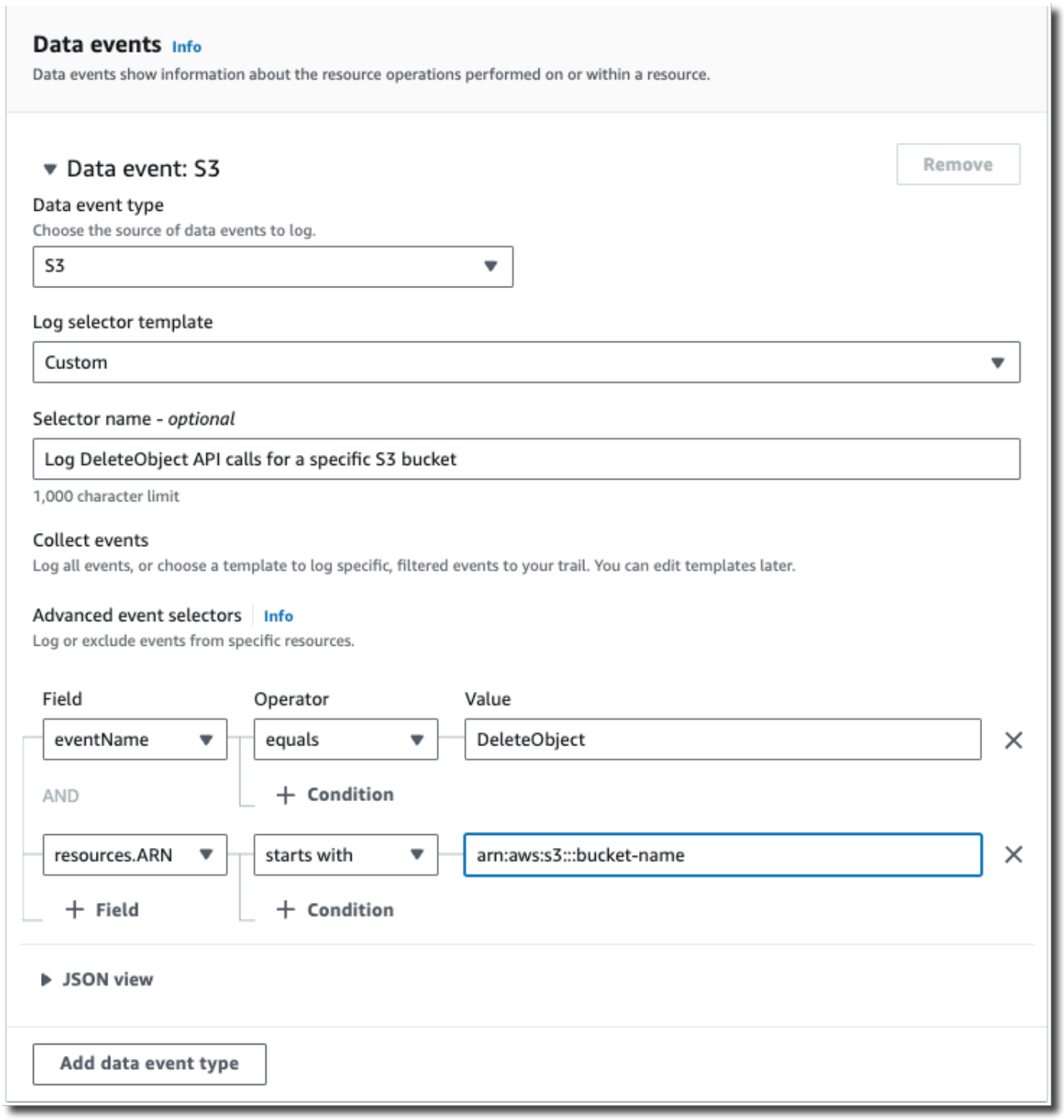
    c. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクター名は、「特定の S3 バケットの DeleteObject API 呼び出しを記録する」など、高度なイベントセレクターを説明する名前です。セレクタ名は、拡張イベントセレクタに「`Name`」と表示され、[JSON ビュー] を展開すると表示されます。



d. アドバンスドイベントセレクターでは、およびフィールドをフィルタリングするカスタムイベントセレクターを作成します。eventName resources.ARNイベントデータストアの高度なイベントセレクタは、証跡に適用する高度なイベントセレクタと同じように機能します。高度なイベントセレクタを作成する方法の詳細については、「高度なイベントセレクタを使用してデータイベントを記録する」を参照してください。

   i. [フィールド] に、[eventName] を選択します。[オペレーター]に、[equals] を選択します。[値] に「**`DeleteObject`**」と入力します。[+ Field] を選択すると、別のフィールドでフィルタリングできます。

   ii. [フィールド]に、[resources.ARN] を選択します。[オペレータ] では [オペレータ] を選択しますStartsWith。[値] に、バケットの ARN を入力します (例: *`arn:aws:s3:::bucket-name`*)。ARN の取得方法については、「Amazon シンプルストレージサービスユーザーガイド」で「Amazon S3 リソース」を参照してください。



17. [Next] (次へ) を選択して、選択内容を確認します。
18. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。

19. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    イベントデータストアは、この時点以降の高度なイベントセレクタに一致するイベントを取得します。イベントデータストアを作成する前に発生したイベントは、既存の証跡イベントをコピーすることを選択しない限り、イベントデータストアには保存されません。

イベントデータストアに対してクエリを実行できるようになりました。サンプルクエリを表示および実行する方法については、 CloudTrail Lake のサンプルクエリを表示して実行する を参照してください。

トレイルイベントを CloudTrail Lake イベントデータストアにコピーします。

このチュートリアルでは、トレイルイベントを新しい CloudTrail Lake イベントデータストアにコピーして履歴分析を行う方法を説明します。証跡イベントのコピーに関する詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail コストの価格設定と管理については、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

トレイルイベントを CloudTrail Lake イベントデータストアにコピーすると、イベントデータストアが取り込む非圧縮データの量に基づいて料金が発生します。

トレイルイベントを CloudTrail Lake にコピーすると、gzip（圧縮）CloudTrail 形式で保存されているログを解凍し、ログに含まれるイベントをイベントデータストアにコピーします。非圧縮データのサイズは、実際の S3 ストレージサイズよりも大きくなる可能性があります。圧縮されていないデータのサイズを概算するには、S3 バケット内のログのサイズに 10 を掛けます。

コピーするイベントの時間範囲を短くすることで、コストを削減できます。コピーしたイベントのクエリにイベントデータストアのみを使用する予定の場合は、イベントの取り込みを無効にして、今後のイベントで料金が発生しないようにすることができます。コストについて詳しくは、「料金表」と「」を参照してくださいAWS CloudTrail 。 CloudTrail Lake コストの管理

新規イベントデータストアへ証跡イベントをコピーする

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [イベントデータストアの設定] ページの [一般的な詳細] で、イベントデータストアに名前 (など) を入力します*my-management-events-eds*。イベントデートストアの意図をすぐに識別できる名前を使用するのがベストプラクティスです。 CloudTrail 命名要件については、を参照してください命名の要件。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、 pay-as-you-go 価格設定で保存期間の延長が可能になります。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントが指定された保存期間内かどうかをチェックして、イベントを保持するかどうかを決定します。`eventTime`例えば、保存期間を 90 日に指定した場合、90 CloudTrail `eventTime` 日以上経過したイベントは削除されます。

> **Note**
>
> このイベントデータストアにトレイルイベントをコピーする場合、 CloudTrail `eventTime`指定した保存期間より古いイベントはコピーされません。適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントをイベントデータストアに保持したい日数 (保持期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

7. (オプション) [暗号化] で、独自の KMS キーを使用してイベントデータストアを暗号化するかどうかを選択します。デフォルトでは、イベントデータストア内のすべてのイベントは、 AWS ユーザーが所有および管理する KMS CloudTrail キーを使用して暗号化されます。

   独自の KMS キーを使用して暗号化を有効にするには、[独自の AWS KMS key を使用する] を選択します。[新規] AWS KMS key を選択して自動的に作成するか、[既存] を選択して既存の KMS キーを使用します。「KMS エイリアスの入力」 で、エイリアスを次の形式で指定します。`alias/` *`MyAliasName`*独自の KMS キーを使用するには、KMS キーポリシーを編集して、CloudTrail ログの暗号化と復号化を許可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。AWS KMS の主要ポリシーの設定 CloudTrail CloudTrail AWS KMS マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、 AWS KMS 暗号化と復号化にコストがかかります。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > AWS Key Management Service 組織のイベントデータストアの暗号化を有効にするには、管理アカウント用の既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンは、クエリするデータを検索、読み

取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 CloudTrail 必要な権限を持つロールが自動的に作成されます。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) をデータセットに追加します。 CloudTrail タグはイベントデータストアを識別するのに役立ちます。例えば、**stage** という名前の **prod** という値のタグをアタッチできます。タグを使用して、イベントデータストアへのアクセスを制限できます。タグを使用して、イベントデータストアのクエリコストと取り込みコストを追跡することもできます。

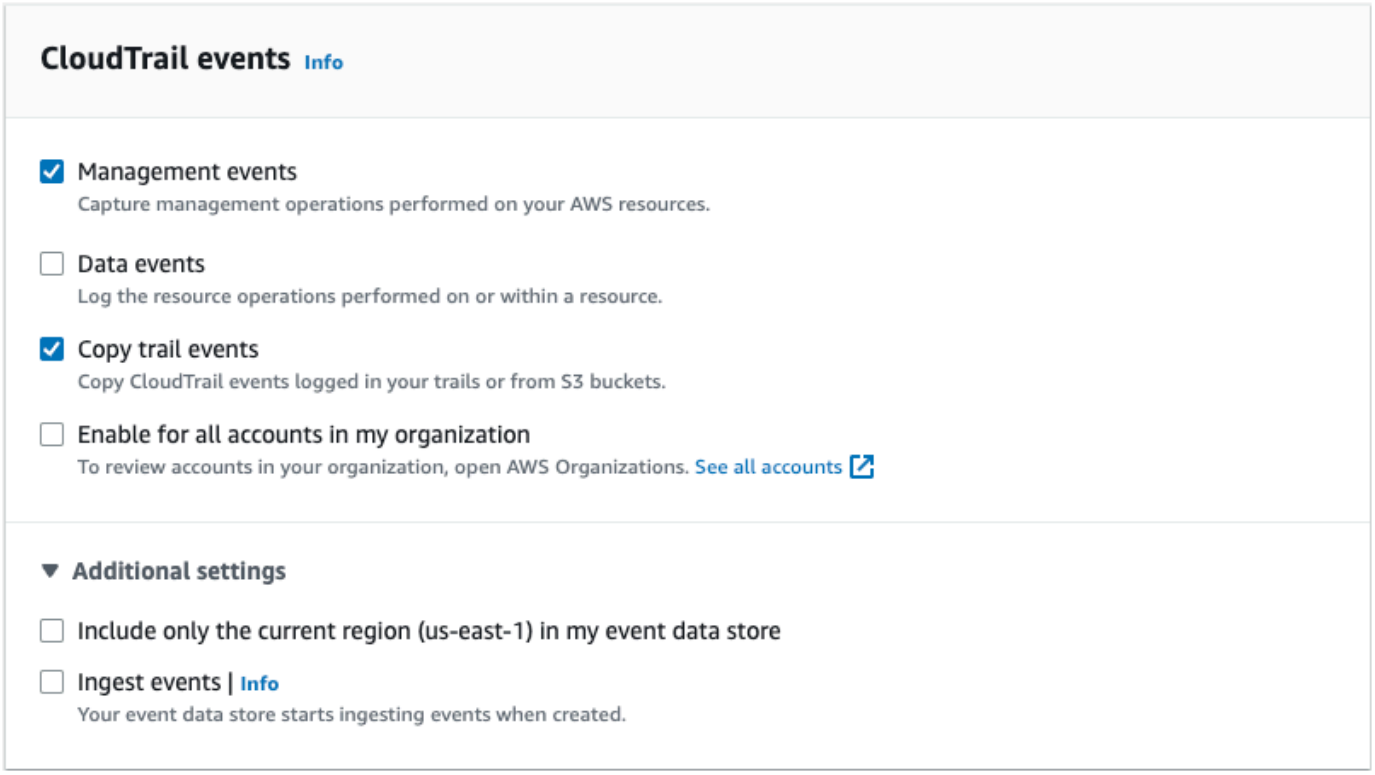
   タグを使用してコストを追跡する方法については、「 CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法については AWS、『リソースへのタグ付け』ユーザーガイドの「 AWS AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. [イベントの選択]ページで、[イベントタイプ] はデフォルトの選択のままにします。

12. CloudTrail イベントについては、[管理イベント] を選択したままにし、[トレイルイベントのコピー] を選択します。この例では、イベントデータストアは過去のイベントの分析にのみ使用し、将来のイベントは取り込まないため、イベントタイプを考慮する必要はありません。

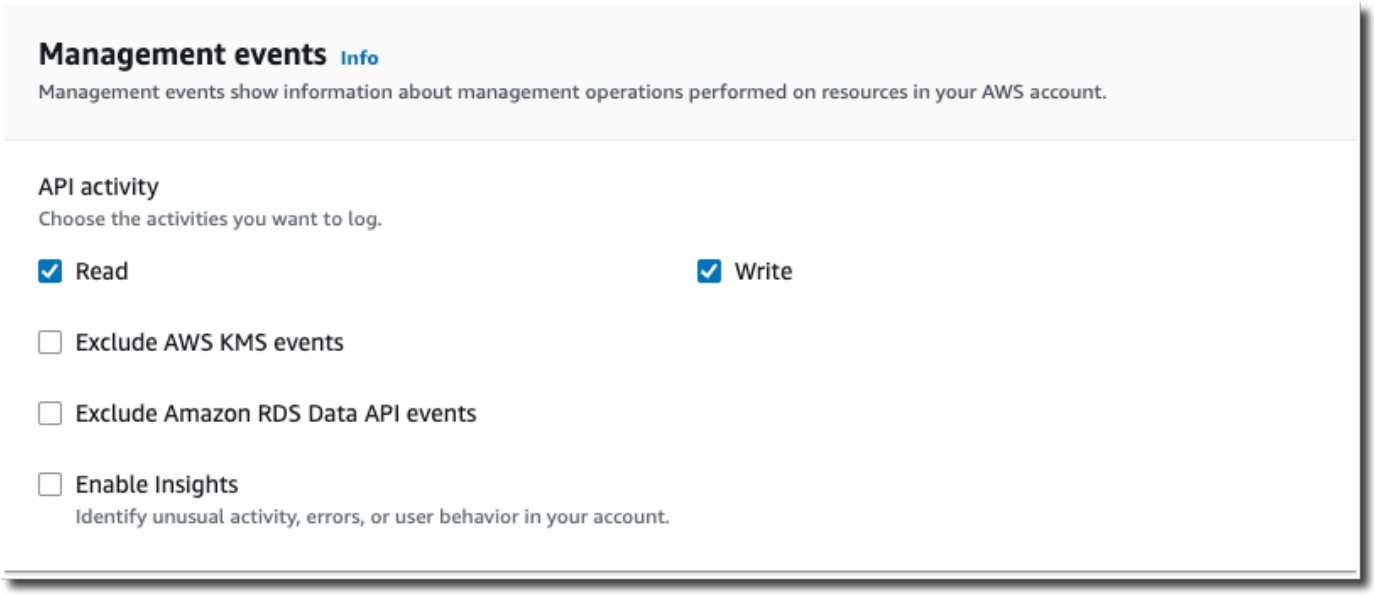
    既存の証跡を置き換えるためにイベントデータストアを作成する場合は、証跡と同じイベントセレクターを選択して、イベントデータストアが同じイベント範囲であることを確認してください。



13. 組織のイベントデータストアの場合は、[組織内の全アカウントで有効にする] を選択します。このオプションは、 AWS Organizations でアカウントを設定していない場合は変更できません。

> **Note**
>
> 組織のイベントデータストアを作成する場合、組織イベントデータストアに証跡イベントをコピーできるのは管理アカウントだけなので、組織の管理アカウントでサインインする必要があります。

14. [追加設定] で、[イベントの取り込み] を選択解除します。この例では、コピーされたイベントのクエリのみを扱い、イベントデータストアでは未来のイベントを取り込まないためです。デフォルトでは、 AWS リージョン イベントデータストアはすべてのイベントを収集し、作成時にイベントの取り込みを開始します。
15. [管理イベント] は、デフォルト設定のままにします。



16. [証跡イベントのコピー] 領域で、以下の手順を完了してください。

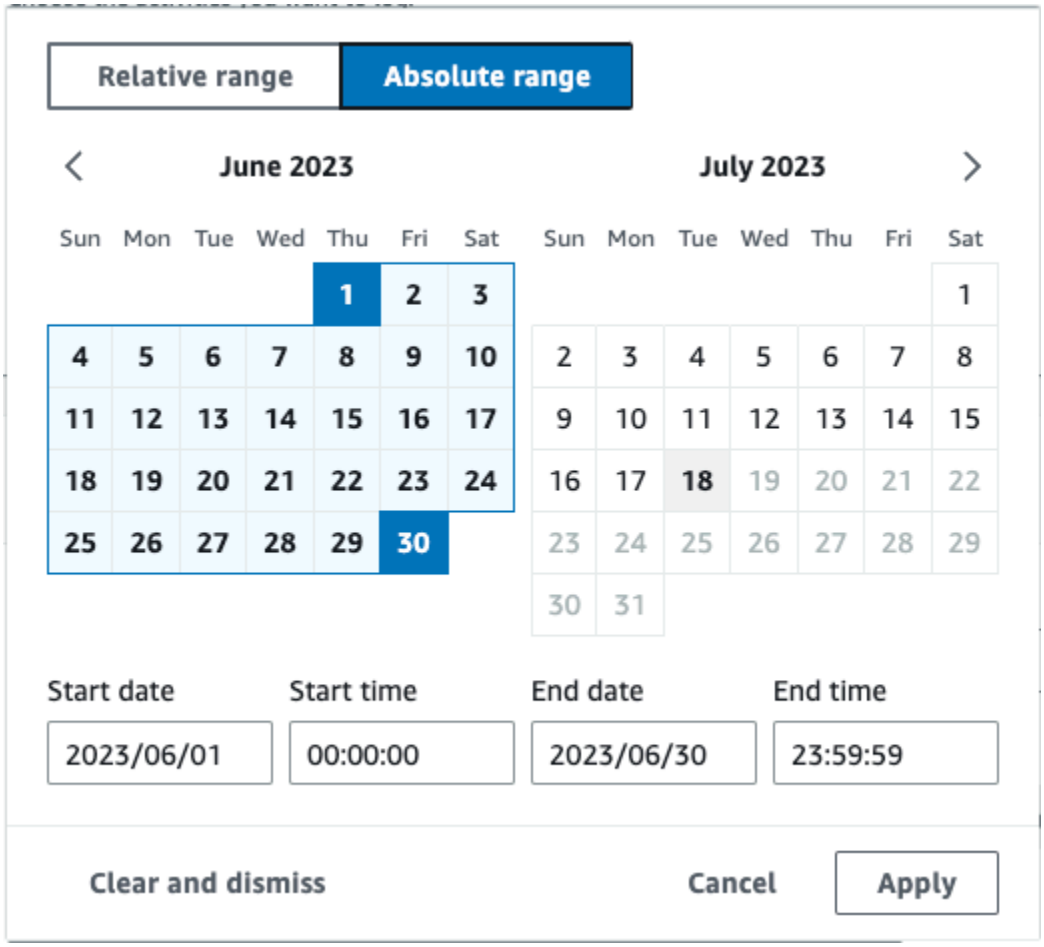
    a. コピーするトレイルを選択します。この例では、*management-events* という名前の証跡を扱います。

       デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、`CloudTrail`他のサービスのプレフィックスをチェックしません。 AWS CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、[Enter S3 URI] を選択し、[Browse S3] を選択してプレフィックスを参照します。トレイルのソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでデータの復号化が許可されていることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。KMS キーポリシーの更新の詳細については、「ソース S3 バケット内のデータを復号化するための KMS キーポリシー」を参照してください。

    b. イベントをコピーする時間範囲を選択してください。 CloudTrail トレイルイベントをコピーする前に、プレフィックスとログファイル名をチェックして、選択した開始日と終了日の間の日付が名前に含まれていることを確認します。[Relative range] (相対範囲) または[Absolute range] (絶対範囲) を選択することができます。ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の時間範囲を選択します。

- [相対範囲] を選択すると、過去 6 か月、1 年、2 年、7 年間に記録されたイベントをコピーするか、またはカスタム範囲をコピーするかを選択できます。 CloudTrail 選択した期間内に記録されたイベントをコピーします。
- [絶対範囲] を選択すると、特定の開始日と終了日を選択できます。 CloudTrail 選択した開始日と終了日の間に発生したイベントをコピーします。

この例では、[絶対範囲] を選択し、6 月全体を選択します。

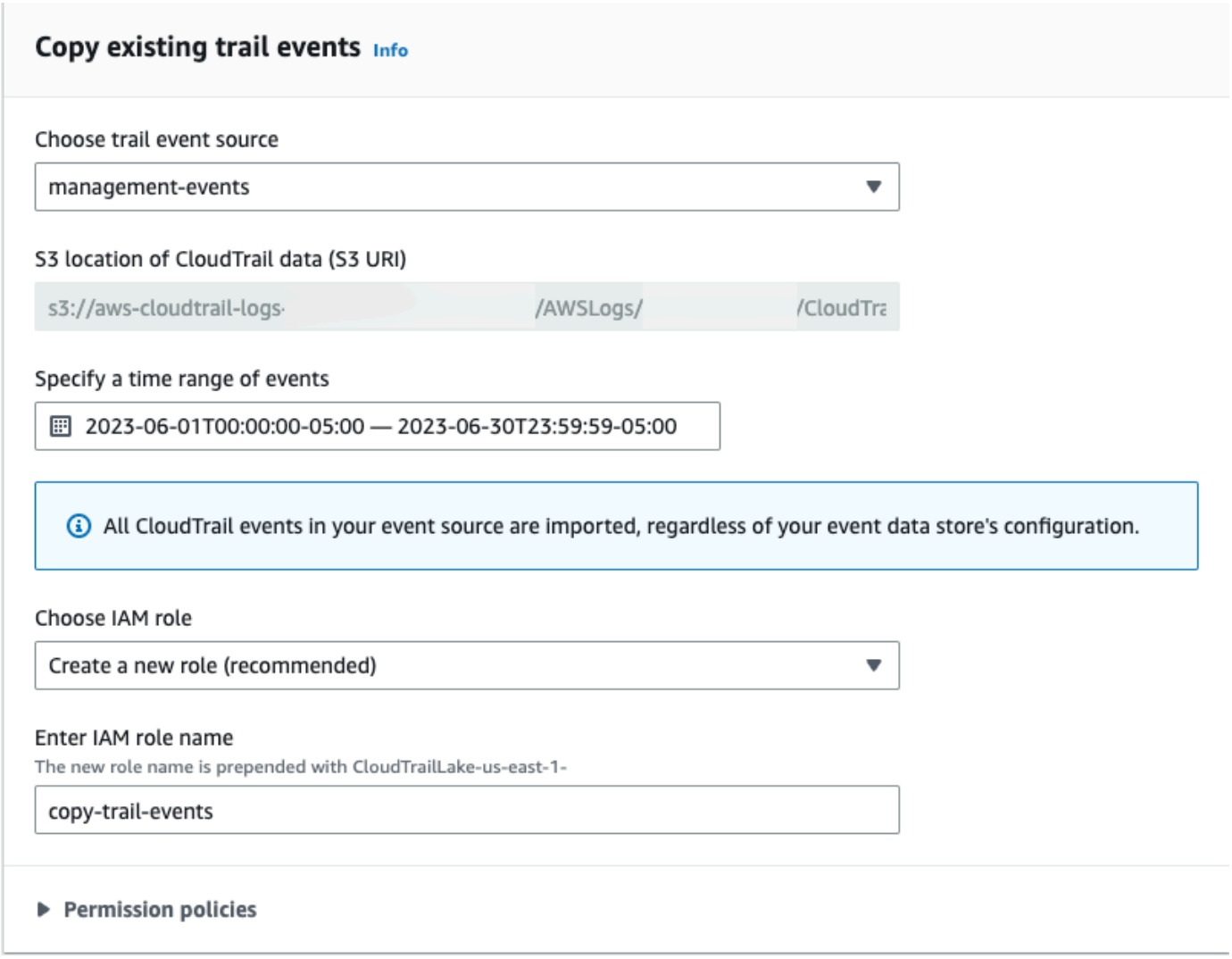


c. [Permissions] (アクセス許可) については、以下の IAM ロールのオプションから選択します。既存の IAM ロールを選択する場合は、IAM ロールポリシーが必要なアクセス許可を提供していることを確認してください。IAM ロールの許可の更新の詳細については、「証跡イベントをコピーするための IAM 許可」を参照してください。

- [Create a new role (recommended)] (新しいロールの作成 (推奨)) を選択して、新しい IAM ロールを作成します。[IAM ロール名を入力] には、ロールの名前を入力します。CloudTrailこの新しいロールに必要な権限が自動的に作成されます。

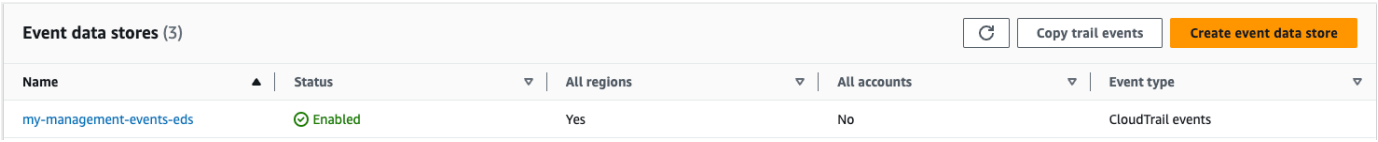
- リストにないカスタム IAM ロールを使用するには、[カスタム IAM ロール ARN を使用] を選択します。[Enter IAM role ARN] (IAM ロールの ARN を入力) で、IAM ARN を入力します。
- ドロップダウンリストから既存の IAM ロールを選択します。

この例では、[新しいロールを作成し (推奨)] を選択し、**copy-trail-events** と名前をつけます。



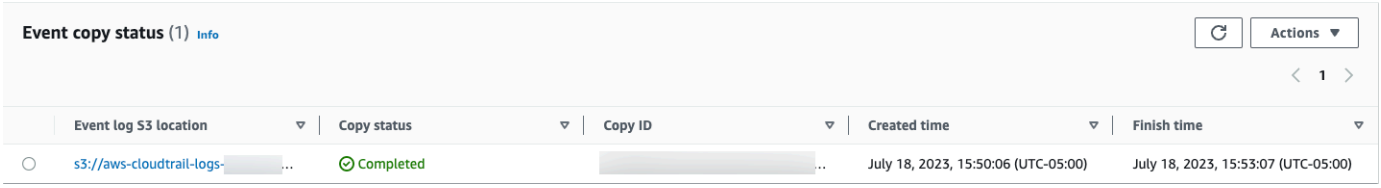
17. [Next] (次へ) を選択して、選択内容を確認します。
18. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。

19. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

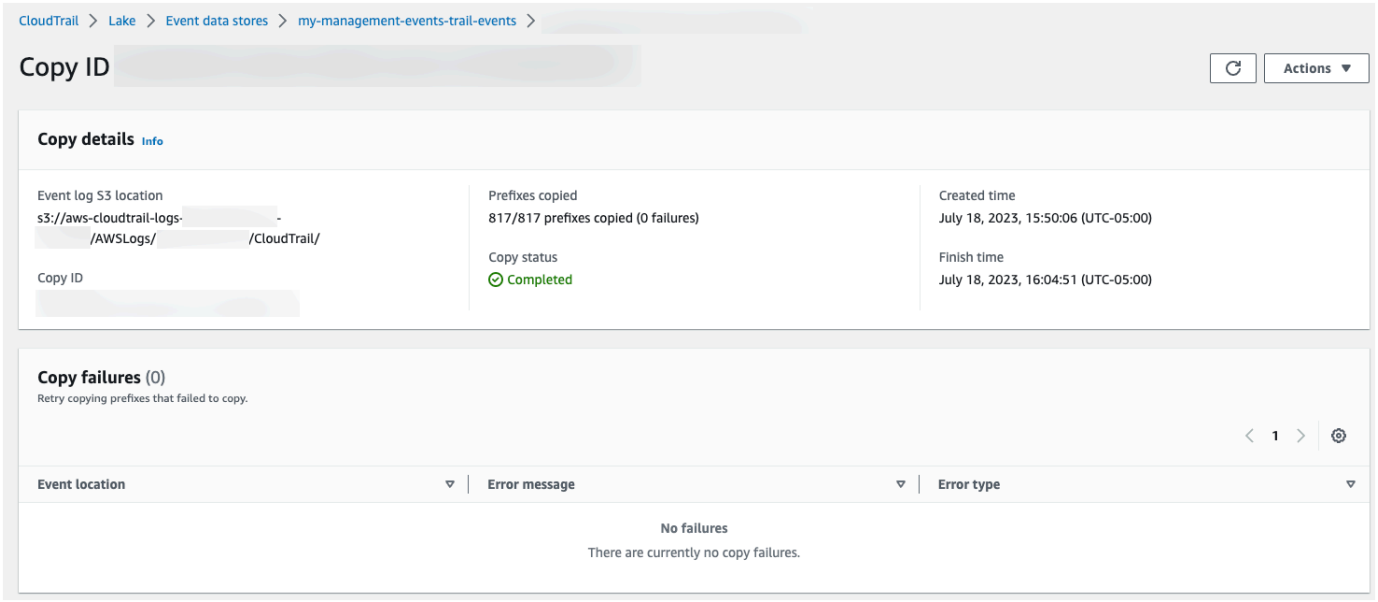


20. イベントデータストア名を選択すると、詳細ページが表示されます。詳細ページには、イベントデータストアの詳細とコピーのステータスが表示されます。イベントのコピーステータスは、[イベントコピーのステータス] 領域に表示されます。

    証跡イベントのコピーが完了すると、その[Copy status] (コピー ステータス) は、エラーがない場合は[Completed] (完了) に設定され、エラーが発生した場合は[Failed] (失敗) に設定されます。



21. コピーの詳細を表示するには、[イベントログ S3 の場所] 列を選択するか、[アクション] メニューで [詳細を表示] を 選択します。証跡イベントコピーの詳細を表示する方法については、「イベントコピーの詳細」を参照してください。



22. [コピー失敗] 領域には、証跡イベントのコピー時に発生したすべてのエラーが表示されます。[Copy status] (コピーのステータス) が[Failed] (失敗) の場合は、[Copy failures] (コピーの失敗) に示されているエラーを修正し、[Retry copy] (コピーの再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。

Lake ダッシュボードを表示します。 CloudTrail

このウォークスルーでは、Lake CloudTrail ダッシュボードを表示する方法を説明します。CloudTrailLake ダッシュボードでは、イベントデータストア内のイベントを視覚化し、トップユーザーやトップエラーなどの傾向を確認できます。

各ダッシュボードは複数のウィジェットで構成され、各ウィジェットは SQL クエリを表します。ダッシュボードに入力するには、 CloudTrail システムによって生成されたクエリを実行します。クエリには、スキャンされたデータ量に基づいて料金がかかります。

> **Note**
>
> 現在、ダッシュボードは、 CloudTrail管理イベント、Amazon S3 データイベント、および Insights イベントを収集するイベントデータストアでのみ使用できます。

Lake ダッシュボードを表示する

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] の下にある [ダッシュボード] を選択します。
3. ダッシュボードページを初めて表示すると、 CloudTrail クエリの実行に関連するコストを確認するように求められます。クエリの実行コストを確認するには、[同意する] を選択します。これは 1 回限りの確認です。料金について詳しくは、「 CloudTrail 価格設定」を参照してください CloudTrail。
4. リストからイベントデータストアを選択し、表示するダッシュボードタイプを選択します。

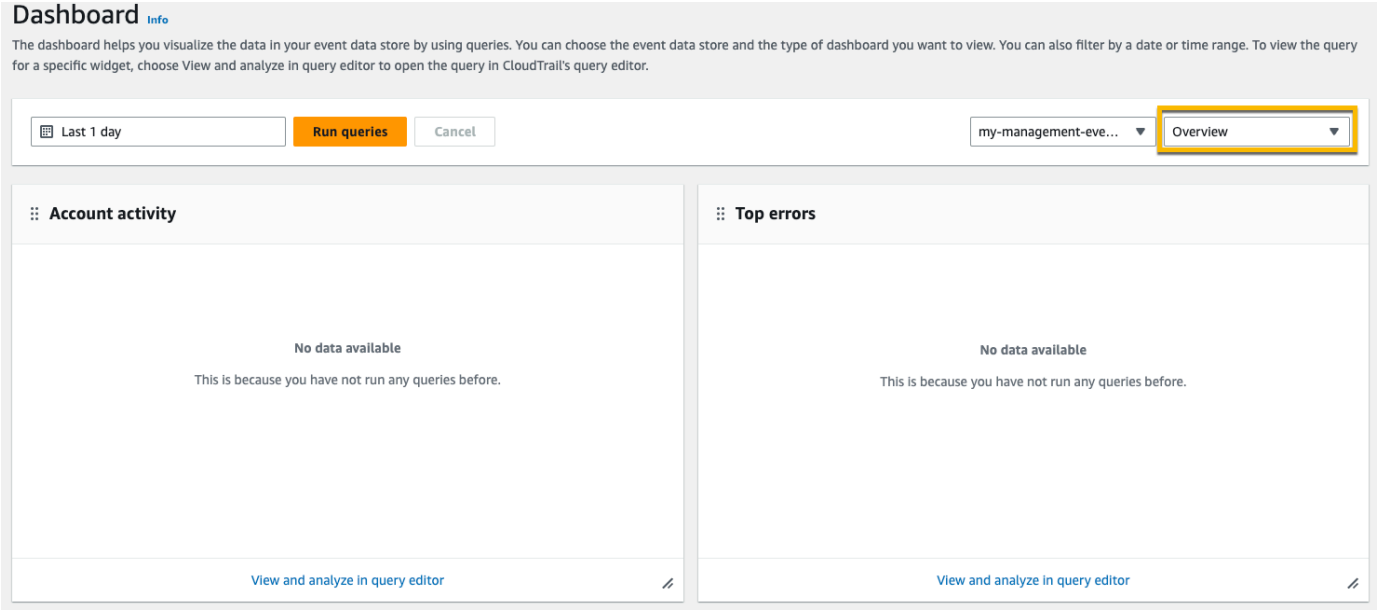
   ダッシュボードのタイプを以下に示します。

   - 概要ダッシュボード-最もアクティブなユーザーと AWS リージョン、 AWS のサービス およびイベント数が表示されます。また、`read` と `write` の管理イベントのアクティビティ、最もスロットリングされているイベント、上位のエラーに関する情報も表示できます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。
   - [管理イベント] ダッシュボード - ユーザーごとのコンソールのログインイベント、アクセス拒否イベント、破壊的なアクション、上位エラーが表示されます。ユーザーごとに TLS バージョンと古い TLS 呼び出しに関する情報を表示することもできます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。

- [S3 データイベント] ダッシュボード - S3 アカウントのアクティビティ、最もアクセスされた S3 オブジェクト、上位の S3 ユーザー、上位の S3 アクションが表示されます。このダッシュボードは、Amazon S3 データイベントを収集するイベントデータストアで使用できます。
- [Insights イベント]ダッシュボード – 全体的な Insights タイプ別の Insights イベントの比率、上位ユーザーとサービスに関する Insights タイプ別の Insights イベントの比率、および 1 日あたりの Insights イベント数が表示されます。ダッシュボードには、最大 30 日間の Insights イベントを一覧表示するウィジェットも含まれます。このダッシュボードは、Insights イベントを収集するイベントデータストアでのみ利用可能です。

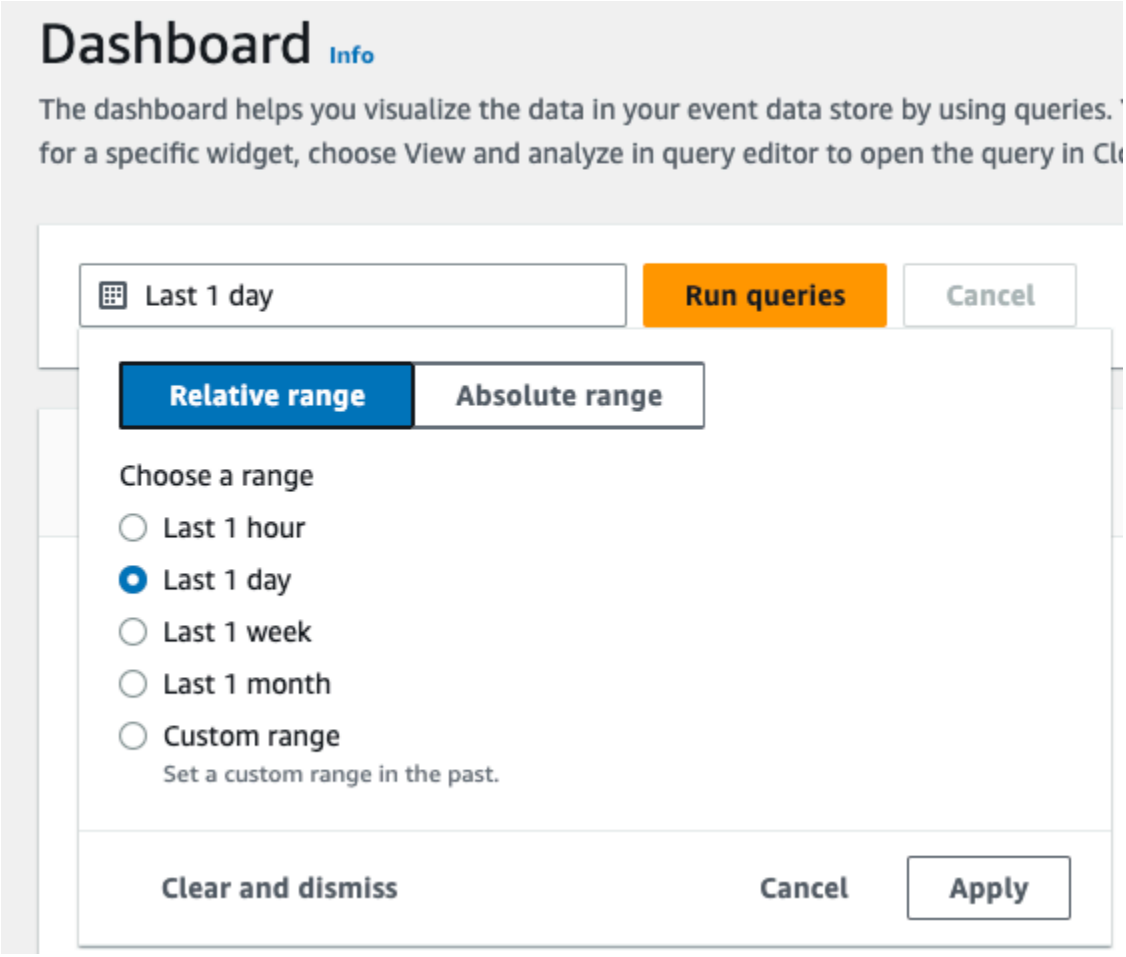
> **Note**
>
> - CloudTrail ソースイベントデータストアで初めてインサイトを有効にした後、異常なアクティビティが検出された場合は、最初の CloudTrail Insights イベントの配信までに最大 7 日かかることがあります。詳細については、「Insights イベントの配信を理解する」を参照してください。
> - [Insights イベント] ダッシュボードには、ソースイベントデータストアの設定によって決定される、選択したイベントデータストアによって収集された Insights イベントに関する情報のみが表示されます。例えば、ソースイベントデータストアで、`ApiErrorRateInsight` ではなく `ApiCallRateInsight` の Insights イベントを有効にしている場合には、`ApiErrorRateInsight` の Insights イベントに関する情報は表示されません。

この例では、[概要]ダッシュボードを選択しています。



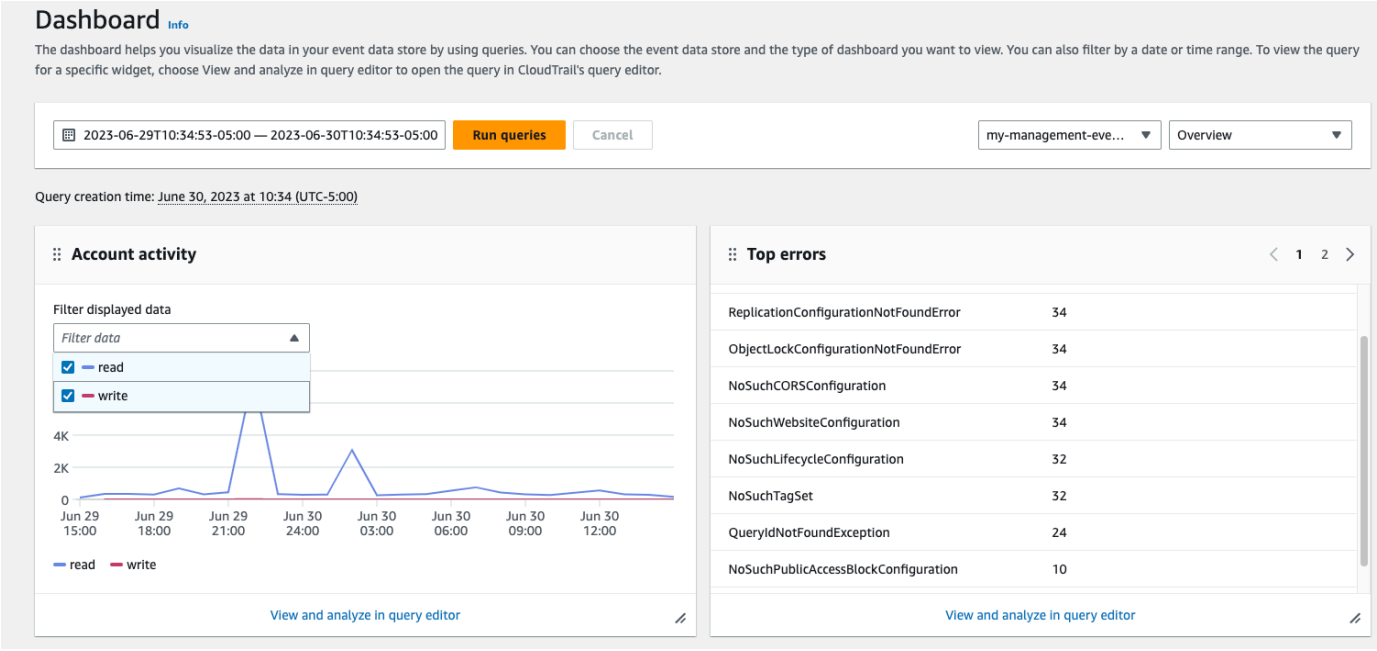
5. 日付フィールドを選択して時間範囲でフィルタリングし、[適用] を選択します。特定の日付と時刻の範囲を選択するには、[絶対範囲] を選択します。事前定義済みの時間範囲またはカスタム範囲を選択するには、[相対範囲] を選択します。デフォルトでは、ダッシュボードには過去 24 時間のイベントデータが表示されます。

> **Note**
>
> CloudTrail クエリはスキャンされたデータ量に基づいて課金されるため、より狭い時間範囲でフィルタリングすることでコストを削減できます。

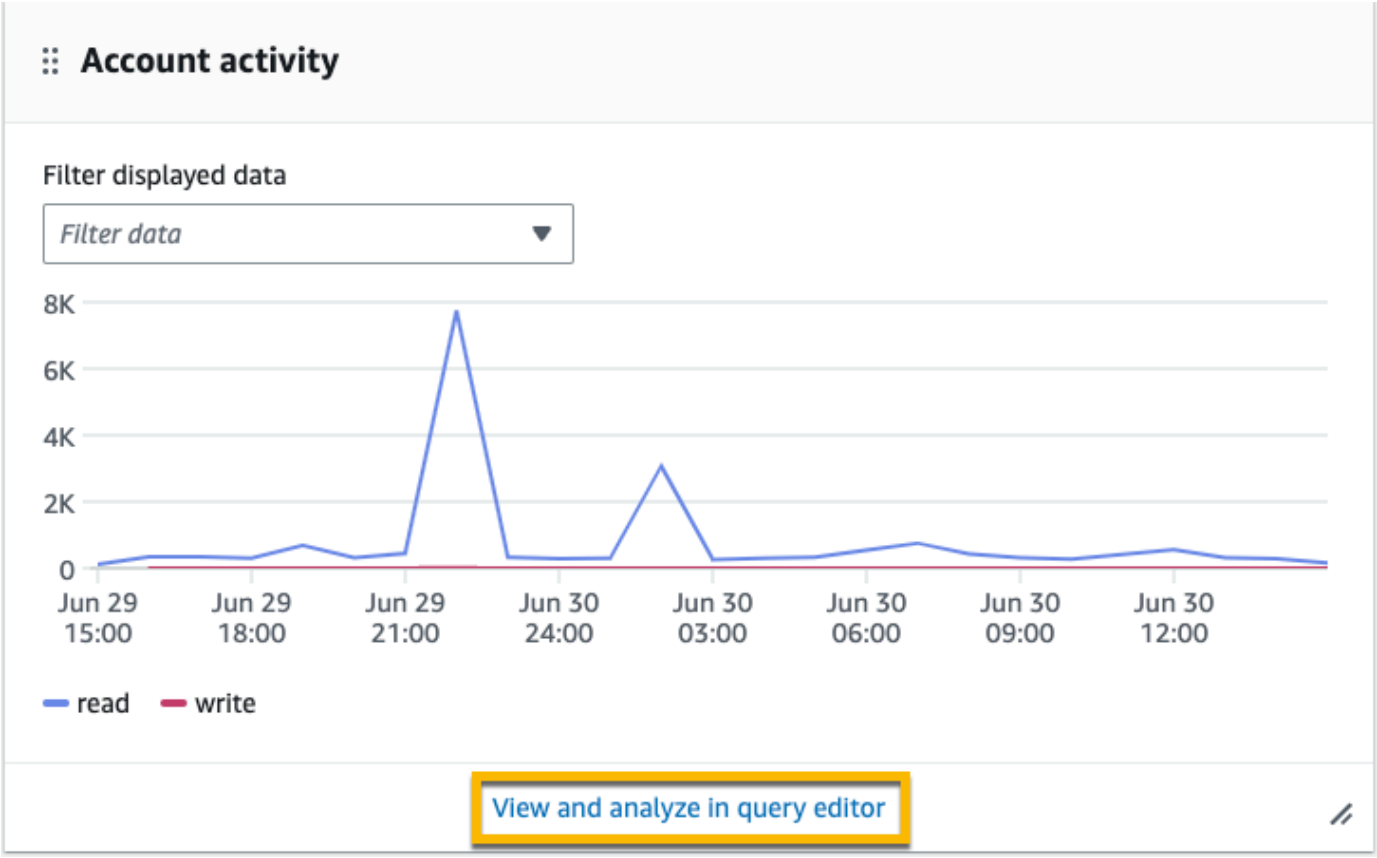


6. [クエリを実行] を選択すると、ダッシュボードに入力されます。各ウィジェットは、関連するクエリのステータスを個別に表示し、クエリが完了するとデータを表示します。

   [アカウントアクティビティ] など、一部のウィジェットでは、追加のフィルタリングを行い、`read` と `write` のイベントアクティビティをフィルタリングできます。

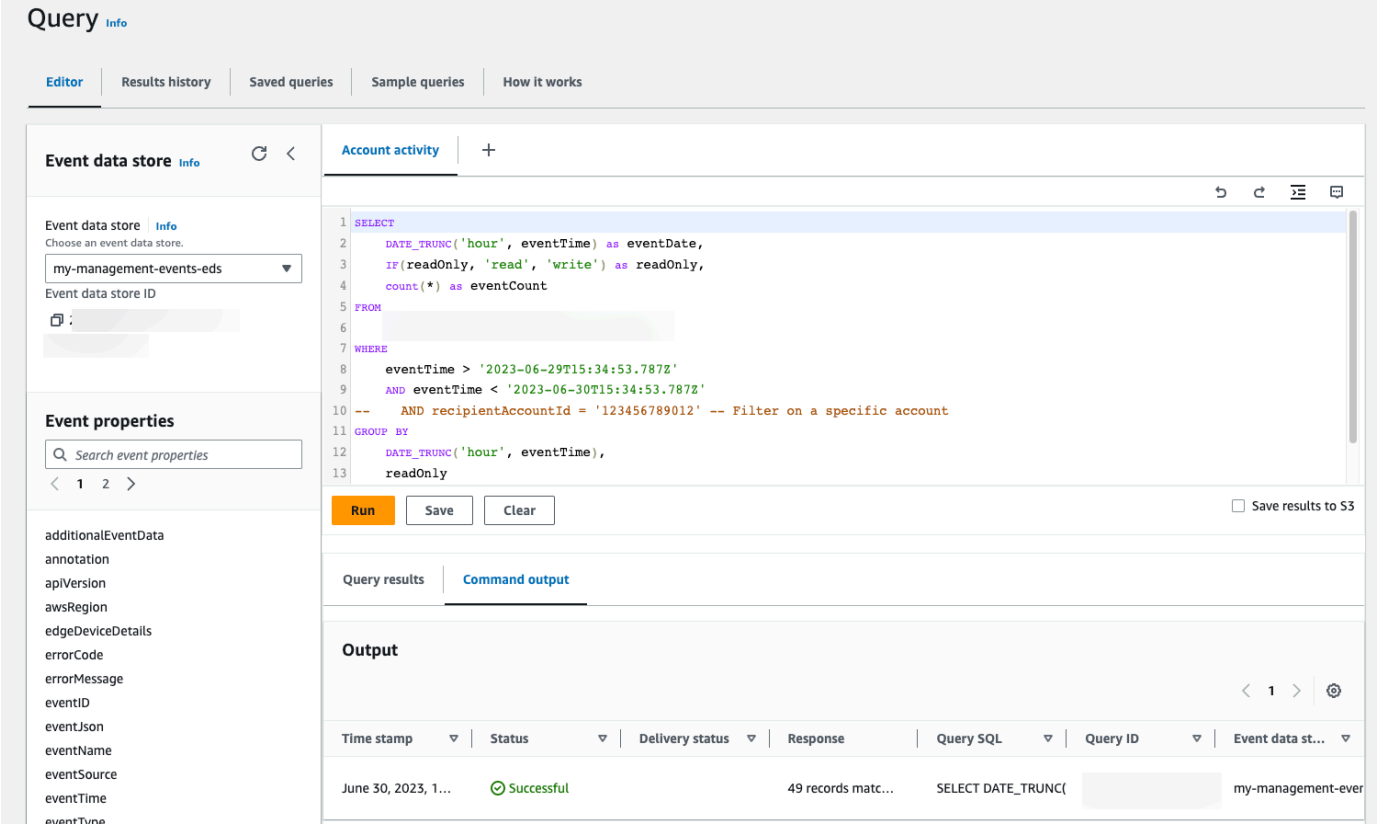


7. ウィジェットのクエリを表示するには、[クエリエディターで表示して分析] を選択します。



クエリエディターで [表示して分析] を選択すると、 CloudTrail Lake のクエリエディターでクエリが開き、ダッシュボードの外でクエリ結果をさらに分析できます。クエリ編集の詳細について

は、「クエリを作成または編集する」を参照してください。クエリの実行およびクエリ結果の保存に関する詳細については、「クエリを実行し、クエリ結果を保存する」を参照してください。



ダッシュボードの詳細については、「CloudTrail Lake ダッシュボードを表示する」を参照してください。

CloudTrail Lake のサンプルクエリを表示して実行する

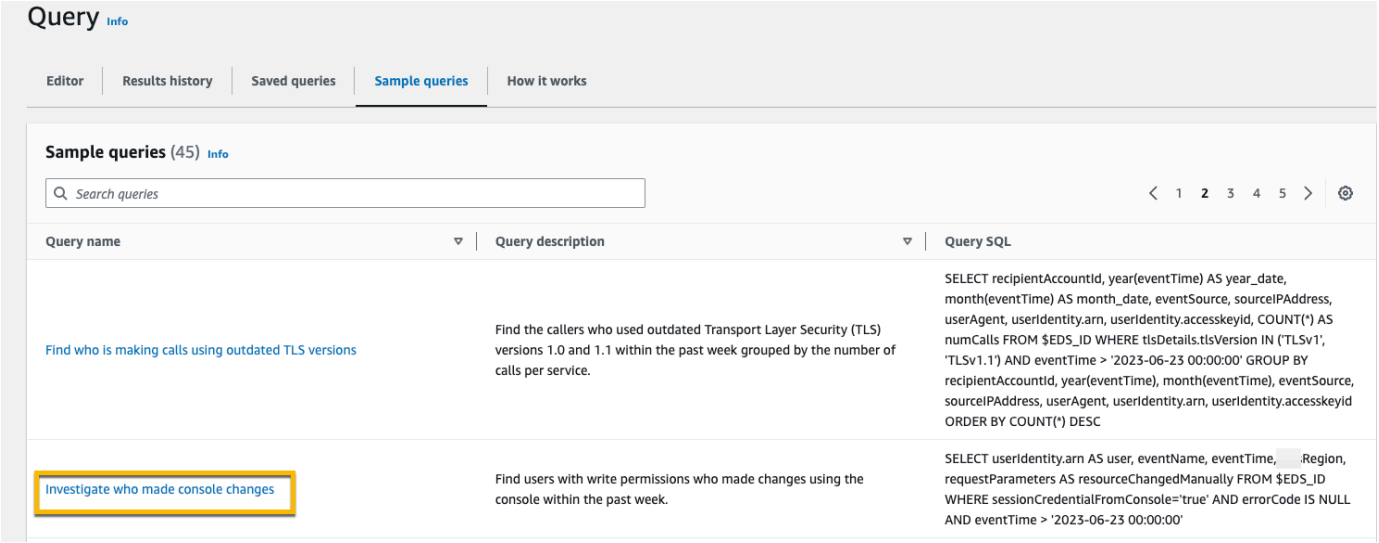
CloudTrail Lake には、独自のクエリの作成を始めるのに役立つサンプルクエリが多数用意されています。このチュートリアルでは、サンプルクエリを選択して実行する方法を説明します。

CloudTrail クエリでは、スキャンされたデータ量に基づいて料金が発生します。コストを抑えるため、クエリに開始および終了 `eventTime` タイムスタンプを追加することで、クエリを制限することをお勧めします。料金について詳しくは、「 CloudTrail 料金表」を参照してくださいAWS CloudTrail 。

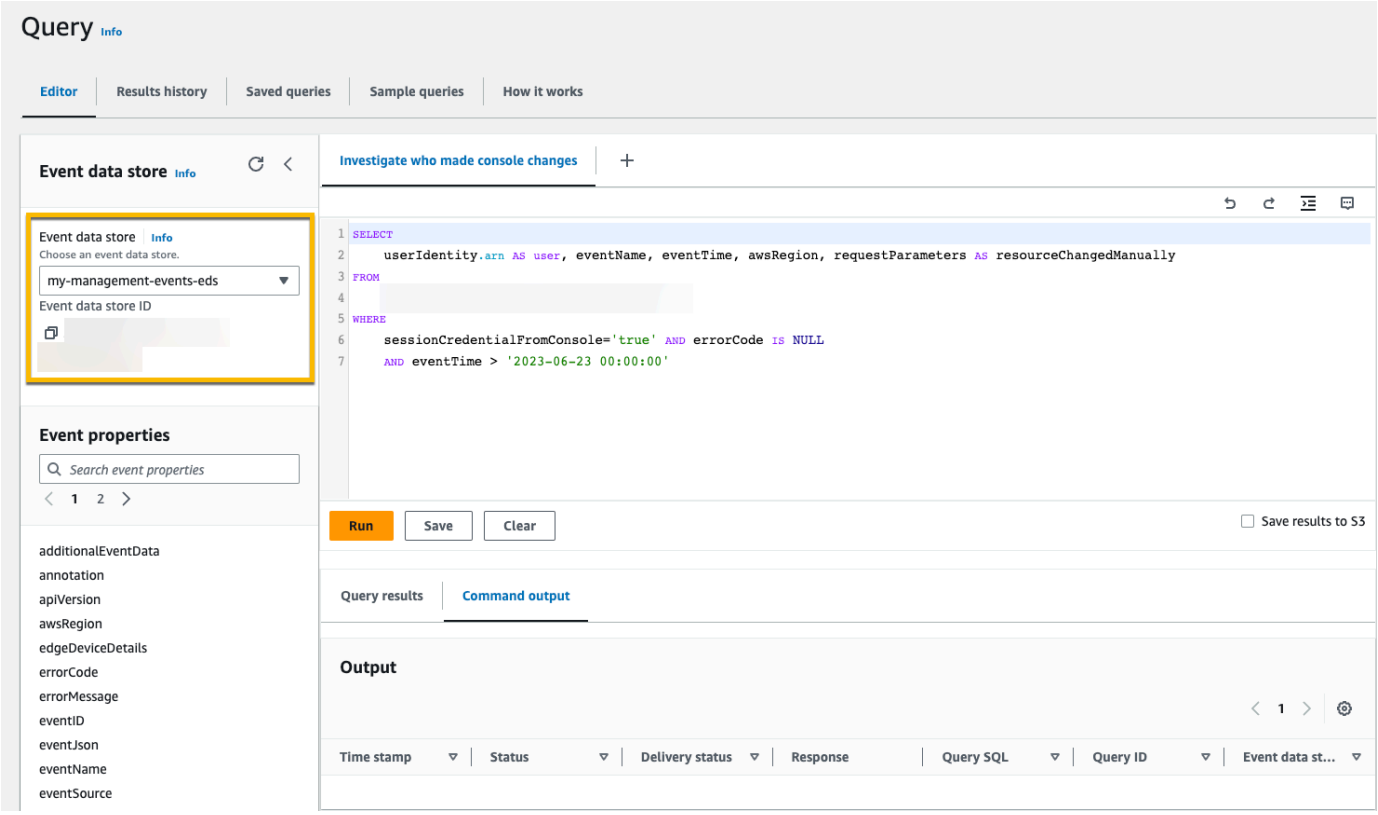
サンプルクエリを表示、実行する

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。

2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。
3. [Query] (クエリ) ページで、[Sample queries] (サンプルクエリ) タブを開きます。
4. リストからサンプルクエリを選択するか、クエリを検索してリストをフィルタリングします。この例では、[クエリ名] を選択し、[コンソール変更者の調査] クエリを開きます。そうすると、[Editor] (エディタ) タブでこのクエリが開きます。

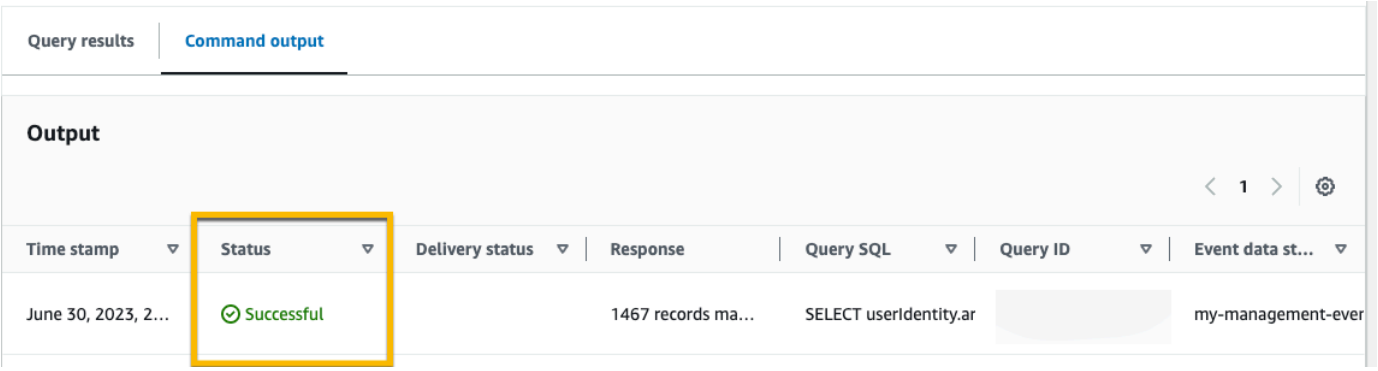


5. [エディター] タブで、クエリを実行するイベントデータストアを選択します。リストからイベントデータストアを選択すると、FROMクエリエディターの行にイベントデータストア ID CloudTrail が自動的に入力されます。

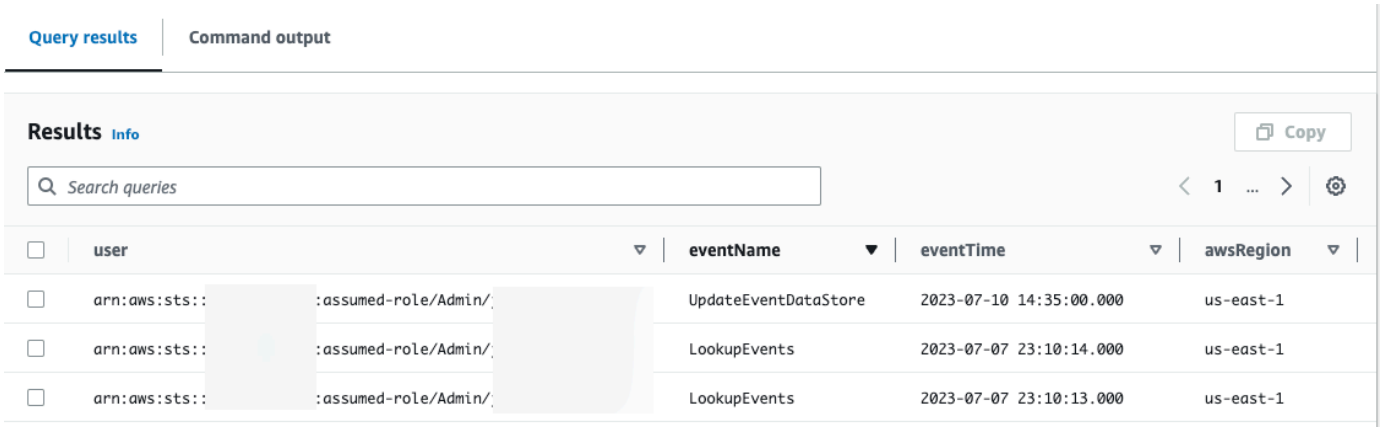


6. クエリを実行するには、[実行] を選択します。

[コマンド出力] タブには、クエリが成功したかどうか、一致したレコードの数、クエリの実行時間など、クエリに関するメタデータが表示されます。



[クエリ結果] タブには、選択したイベントデータストア内のクエリと一致したイベントデータが表示されます。



クエリ編集の詳細については、「クエリを作成または編集する」を参照してください。クエリの実行およびクエリ結果の保存に関する詳細については、「クエリを実行し、クエリ結果を保存する」を参照してください。

CloudTrail Lake のクエリ結果を S3 バケットに保存する

このチュートリアルでは、 CloudTrail Lake クエリの結果を S3 バケットに保存し、そのクエリ結果をダウンロードする方法を示します。

CloudTrail Lake でクエリを実行すると、クエリによってスキャンされたデータ量に基づいて料金が発生します。クエリ結果を S3 バケットに保存しても CloudTrail Lake に追加料金はかかりませんが、S3 ストレージには料金がかかります。S3 の価格設定に関する詳細については、「Amazon S3 pricing」(Amazon S3 価格設定) を参照してください。

CloudTrail クエリスキャンの完了後にクエリ結果が配信されるため、クエリ結果を保存すると、S3 CloudTrail バケットに表示される前にクエリ結果がコンソールに表示される場合があります。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。 CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。クエリスキャンの完了後、S3 バケットに配信されるデータは、1 GB あたり平均 60～90 秒の遅延が見込まれます。

CloudTrail Lake のクエリ結果を Amazon S3 バケットに保存する

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。

3. [サンプルクエリ] または [保存したクエリ] タブ で、[クエリ名] を選択して実行するクエリを選択します。この例では、[ユーザーアクションの調査] という名前のサンプルクエリを選択します。

4. [Event data store] (イベントデータストア) の [Editor] (エディタ) タブで、ドロップダウンリストからイベントデータストアを選択します。リストからイベントデータストアを選択すると、From行にイベントデータストア ID CloudTrail が自動的に入力されます。

5. このサンプルクエリでは、userIdentity.ARN 値を編集し、Admin という名前のユーザーを指定し、eventTime の値はデフォルトのままとします。クエリを実行すると、スキャンされたデータ量に応じて料金が発生します。コストを抑えるため、クエリに開始および終了 eventTime タイムスタンプを追加することで、クエリを制限することをお勧めします。

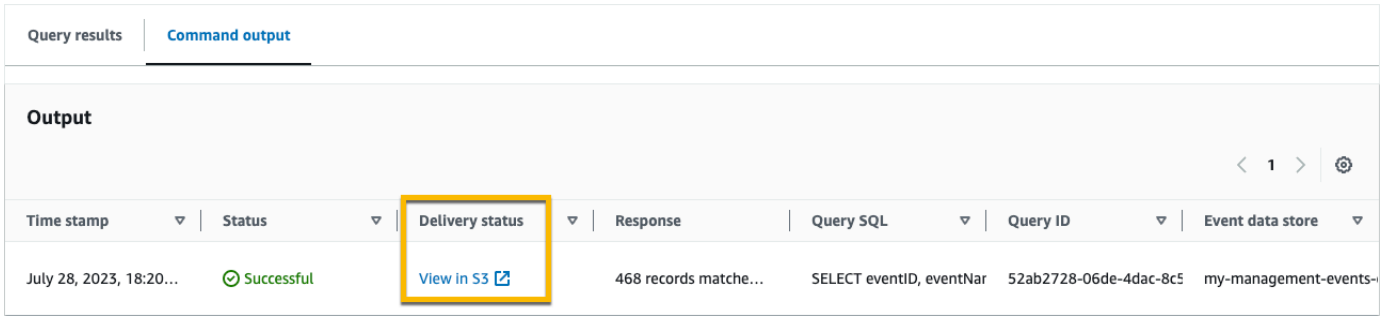
6. [結果を S3 に保存] を選択し、クエリ結果を S3 バケットに保存します。デフォルトの S3 バケットを選択すると、 CloudTrail 必要なバケットポリシーが作成され、適用されます。デフォルトの S3 バケットを選択した場合、IAM s3:PutEncryptionConfiguration ポリシーにはアクションのアクセス権限を含める必要があります。デフォルトではバケットのサーバー側の暗号化が有効になっているためです。クエリ結果保存の詳細については、「保存されたクエリ結果に関する追加情報」を参照してください。この例では、デフォルトの S3 バケットを使用します。

> **Note**
>
> 別のバケットを使用するには、バケット名を指定するか、[Browse S3] (S3 を閲覧) を選択してバケットを選択します。バケットポリシーは、 CloudTrail クエリ結果をバケットに配信するアクセス権限を付与する必要があります。バケットポリシーを手動で編集する方法については、 CloudTrail レイククエリ結果の Amazon S3 バケットポリシー を参照してください。

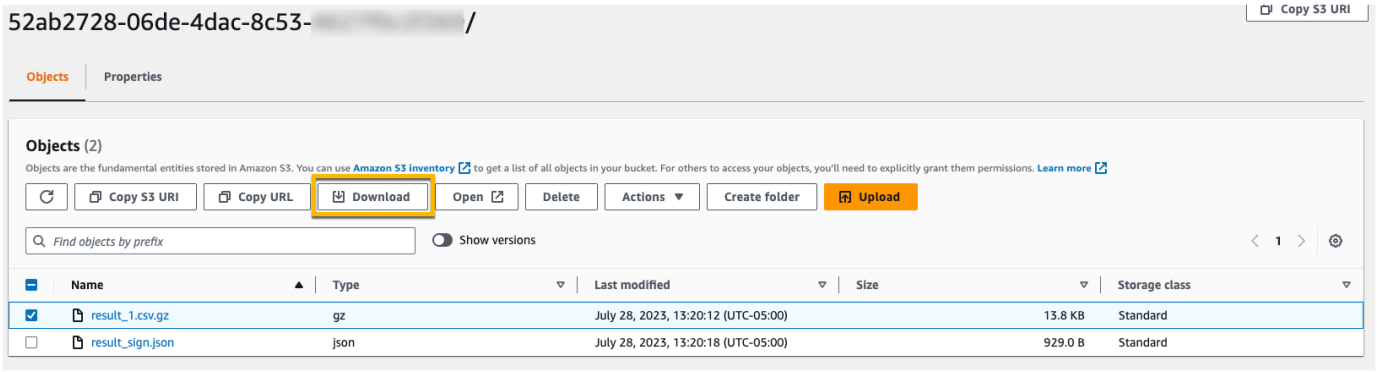
7. [実行] を選択します。イベントデータストアのサイズと、それに含まれるデータの日数によっては、クエリの実行に数分かかる場合があります。[Command output] (コマンド出力) タブには、クエリのステータスと、クエリの実行が終了したかどうかが表示されます。クエリの実行が終了したら、[Query results] (クエリ結果) タブを開いて、アクティブなクエリ (現在エディタに表示されているクエリ) の結果の表を表示します。

8. 保存したクエリ結果を S3 バケットに配信すると CloudTrail 、Delivery status 列には、保存したクエリ結果ファイルと、保存したクエリ結果の検証に使用できる署名ファイルが格納されている S3 バケットへのリンクが表示されます。[S3 で表示] を選択すると、S3 バケット内のクエリ結果ファイルと署名ファイルが表示されます。

> **Note**
>
> クエリ結果を保存すると、S3 CloudTrail バケットに表示される前にクエリ結果がコンソールに表示される場合があります。これは、 CloudTrail クエリスキャンの完了後にクエリ結果が配信されるためです。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。 CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。クエリスキャンの完了後、S3 バケットに配信されるデータは、1 GB あたり平均 60～90 秒の遅延が見込まれます。



9. クエリ結果をダウンロードするには、クエリ結果ファイル (この例では、`result_1.csv.gz`) を選択し、[ダウンロード] を選択します。



保存したクエリ結果の検証の詳細については、「保存されたクエリ結果の検証」を参照してください。

での CloudTrail コストと使用状況の表示 AWS Cost Explorer

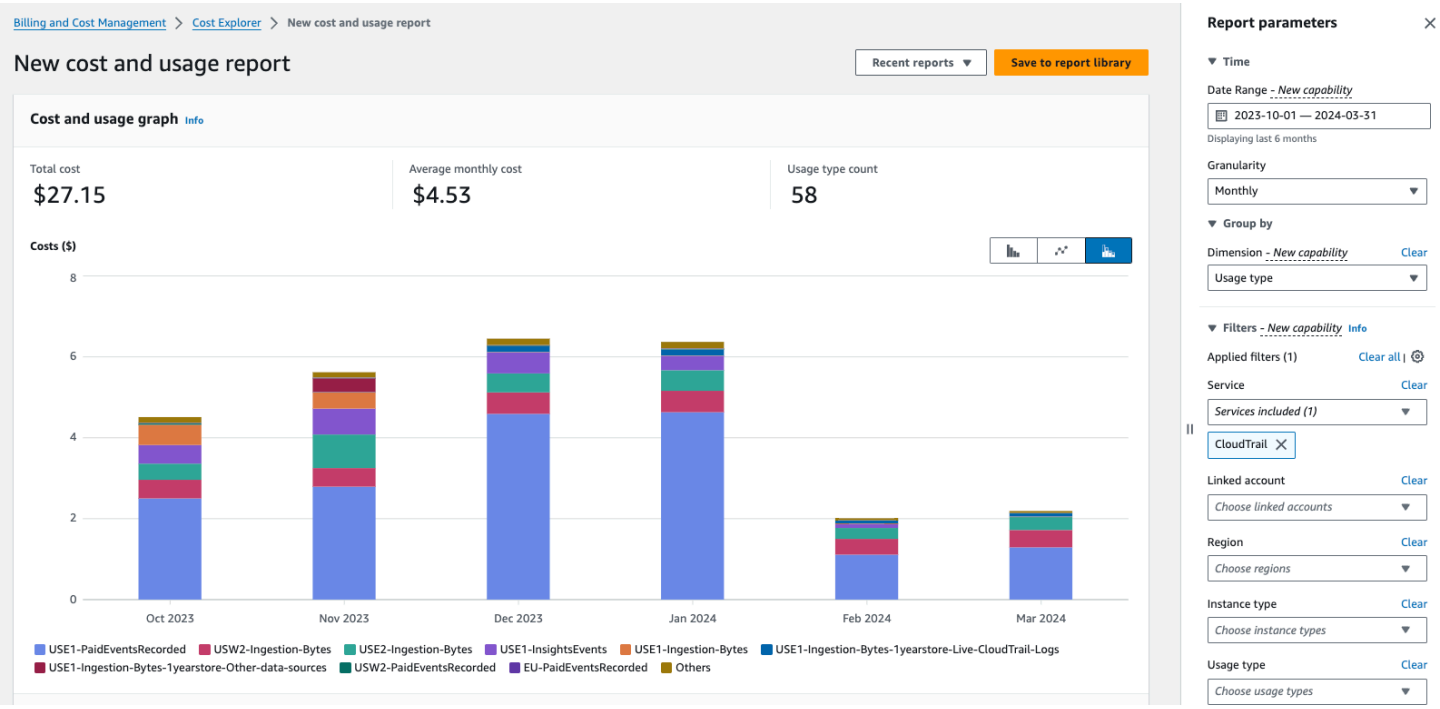
このセクションでは、 を使用して CloudTrail コストと使用状況を表示する方法について説明しますAWS Cost Explorer。Cost Explorer を使用すると、 AWS コストと使用状況を時間の経過とともに視覚化、理解、管理できます。

CloudTrail 料金の詳細については、「 AWS CloudTrail の料金」を参照してください。

Cost Explorer で CloudTrail コストと使用状況を表示するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cost-management/home#/custom で Cost Explorer コンソールを開きます。
2. 時間 で、分析する日付範囲を選択します。
3. 「 によるグループ化」で、ディメンション で「使用タイプ」を選択します。
4. フィルター で、サービス で を選択しますCloudTrail。

次の図は、 に対してフィルタリング CloudTrail され、使用タイプ でグループ化されたコストレポートの例を示しています。



使用タイプを確認して、コストが最も高くなった CloudTrail 機能を確認します。各使用タイプは、料金 AWS リージョン が発生した のコードで始まります。

次の表に、各 CloudTrail 機能 CloudTrail の使用タイプを示します。

CloudTrail 機能	使用タイプ	説明
CloudTrail 証跡	*region*-FreeEventsRecorded	に無料で配信される管理イベントの最初のコピー AWS リージョン。
	region-PaidEventsRecorded	に配信される管理イベントの追加コピーの料金 AWS リージョン。
	region-DataEventsRecorded	へのデータイベントの配信料金 AWS リージョン。データイベントには常に料金が発生します。
CloudTrail レイク	*region*-Ingestion-Bytes	7 年間の保持料金オプションを使用して CloudTrail Lake イベントデータストアにイベントを取り込むための料金。取り込み料金は、取り込まれたデータの量に基づいており、すべてのイベントタイプで同じです。

CloudTrail 機能	使用タイプ	説明
	region-Ingestion-Bytes-1yearstore-Live-CloudTrail-Logs	1 年間の拡張可能な保持料金オプションを使用して、 CloudTrail データイベントと管理イベントを CloudTrail Lake イベントデータストアに取り込むための料金。
	region-Ingestion-Bytes-1yearstore-Other-data-sources	1 年間の拡張可能な保持料金オプションを使用して、他のイベントソースを CloudTrail Lake イベントデータストアに取り込むための料金。これには、 CloudTrail Insights イベント、 の設定項目 AWS Config、 からの証拠 AWS Audit Manager、S3 からインポートされた (非圧縮) 履歴 CloudTrail ログ、および 外のイベントが含まれます AWS。

CloudTrail 機能	使用タイプ	説明
	region-QueryScanned-Bytes	CloudTrail Lake クエリの実行料金。CloudTrail Lake でクエリを実行すると、スキャンされた最適化および圧縮されたデータの量に基づいて料金が発生します。
CloudTrail インサイト	*region*-InsightsEvents	CloudTrail Insights イベントの料金。Insights イベントの場合、インサイトタイプごとに分析された管理イベントの数に基づいて料金が発生します。

追加リソース

- AWS CloudTrail 料金表
- CloudTrail 証跡コストの管理
- CloudTrail Lake コストの管理

CloudTrail イベント履歴の操作

CloudTrail AWS アカウントではデフォルトで有効になっており、 CloudTrail 自動的にイベント履歴にアクセスできるようになります。[イベント履歴] では、 AWS リージョンで過去 90 日間に記録された管理イベントに関する表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。これらのイベントは、、、 AWS SDK AWS Management Console AWS Command Line Interface、API を通じて行われたアクティビティをキャプチャします。イベント履歴には、 AWS リージョン イベントが発生した場所のイベントが記録されます。 CloudTrail イベント履歴の閲覧には料金はかかりません。

CloudTrail コンソールでイベント履歴ページを表示することで、リソース (IAM ユーザーや Amazon EC2 インスタンスなど) の作成、変更、削除に関連するイベントをリージョンごとに検索できます AWS アカウント 。aws cloudtrail lookup-events コマンドを実行するか、`LookupEvents` API を使用してこれらのイベントを調べることもできます。

CloudTrail コンソールのイベント履歴ページを使用して、インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、および対応できます AWS 。各ページに表示するイベントの数を選択し、コンソールに表示する列を選択することで、[イベント履歴] の表示をカスタマイズできます。イベント履歴のイベントの詳細を比較することもできます side-by-side。 AWS SDK またはを使用して、プログラムでイベントを検索できます。 AWS Command Line Interface

> **Note**
>
> 時間が経つにつれて、 AWS のサービス さらにイベントが追加される可能性があります。 CloudTrail これらのイベントはイベント履歴に記録されますが、追加されたイベントを含む 90 日間のアクティビティの完全な記録は、イベントが追加されてから 90 日後まで確認できません。
>
> [イベント履歴] は、作成した証跡やイベントデータとは独立したものです。イベントデータストアまたは証跡を変更しても、[イベント履歴] には影響しません。

以下のセクションでは、 CloudTrail コンソールとを使用して最近の管理イベントを検索する方法と AWS CLI、イベントのファイルをダウンロードする方法について説明します。`LookupEvents`API CloudTrail を使用してイベントから情報を取得する方法については、AWS CloudTrail API LookupEventsリファレンスのを参照してください。

トピック

イベント履歴の制限

[イベント履歴] には次の制限が適用されます。

- CloudTrail コンソールのイベント履歴ページには管理イベントのみが表示されます。データイベントや Insights イベントは表示されません。
- [イベント履歴] では過去 90 日間のイベントのみを表示します。のイベントを継続的に記録するには AWS アカウント、イベントデータストアまたはトレイルを作成します。
- CloudTrail コンソールのイベント履歴ページからイベントをダウンロードすると、1 つのファイルに最大 200,000 件のイベントをダウンロードできます。200,000 イベントの制限に達すると、CloudTrail コンソールに追加ファイルをダウンロードするオプションが表示されます。
- [イベント履歴] では、組織レベルのイベント集約は表示できません。組織全体のイベントを記録するには、組織イベントのデータストアまたは証跡を作成します。
- イベント履歴検索は 1 つに限定され AWS アカウント、1 つのイベントのみを返し AWS リージョン、複数の属性をクエリすることはできません。1 つの属性フィルターおよび時間範囲フィルターのみを適用できます。

  CloudTrail Lake イベントデータストアを作成して、複数の属性および属性に対してクエリを実行できます AWS リージョン。また、 AWS アカウント AWS Organizations 組織内の複数のグループにわたってクエリを実行することもできます。 CloudTrail Lakeでは、管理イベント、データイベント、インサイトイベント、 AWS Config 設定項目、Audit Manager エビデンス、非イベントなど、AWS 複数のイベントタイプをクエリできます。 CloudTrail Lake のクエリでは、イベント履歴や実行中の単純なキーや値の検索よりも、より詳細でカスタマイズ可能なイベントビューが得られます。`LookupEvents`詳細については、「AWS CloudTrail Lake の使用」および「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。
- Amazon RDS Data API AWS KMS イベントをイベント履歴から除外したり、Amazon RDS Data API イベントを除外したりすることはできません。トレイルまたはイベントデータストアに適用した設定は、イベント履歴には適用されません。

コンソールでの最近の管理イベントの表示

CloudTrail コンソールのイベント履歴ページでは、の過去 90 日間の管理イベントを表示できます AWS リージョン。その情報を使用してファイルをダウンロードしたり、選択したフィルターおよび時間範囲に基づいて情報のサブセットをダウンロードしたりできます。各ページに表示するイベントの数を選択し、コンソールに表示する列を選択することで、[イベント履歴] の表示をカスタマイズできます。特定のサービスで利用できるリソースタイプにより、イベントを検索し、フィルタリングすることもできます。イベント履歴では、最大 5 つのイベントを選択して詳細を比較できます side-by-side。

[イベント履歴] はデータイベントを表示しません。データイベントを表示するには、イベントデータストアまたは証跡を作成します。

90 日経過すると、イベントは [イベント履歴] に表示されなくなります。[イベント履歴] からイベントを手動で削除することはできません。

CloudTrail 特定のサービスのイベントの記録方法の詳細については、そのサービスのドキュメントを参照してください。詳細については、「AWS のサービストピック CloudTrail」を参照してください。

> **Note**
>
> 過去 90 日間のアクティビティやイベントを継続的に記録するには、イベントデータストアまたはトレイルを作成してください。

[イベント履歴] を表示するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインで [Event history (イベント履歴)] を選択します。最新のイベントが最初に表示された、フィルタリングされたイベントのリストが表示されます。イベントのデフォルトのフィルターは読み取り専用で、[false] に設定されています。このフィルターをクリアするには、フィルターの右側にある [X] をクリックします。
3. 1 つの属性でイベントをフィルタリングできます。属性はドロップダウンリストから選択できます。属性に基づいてフィルタリングするには、ドロップダウンリストから属性を選択し、その属性の値をすべて入力します。たとえば、コンソールのログインイベントをすべて表示するに

は、イベント名フィルタを選択して指定しますConsoleLogin。または、最近の S3 管理イベントを表示するには、イベントソースフィルターを選択して指定しますs3.amazonaws.com。

4. 特定の管理イベントを表示するには、イベント名を選択します。イベントの詳細ページでは、イベントの詳細を表示したり、参照されているリソースを表示したり、イベントレコードを表示したりできます。
5. イベントを比較するには、[イベント履歴] テーブルの左余白のチェックボックスをオンにして、最大 5 つのイベントを選択します。選択したイベントの詳細は、「イベント詳細の比較」 side-by-side テーブルで確認できます。
6. イベント履歴を保存するには、CSV または JSON 形式のファイルとしてダウンロードします。イベント履歴のダウンロードには数分かかることがあります。

目次

ページ間の移動

表示したいページを選択することで、[イベント履歴] のページ間を移動できます。[イベント履歴] の次のページと前のページも表示できます。

< を選択すると、[イベント履歴] の前のページが表示されます。

< を選択すると、[イベント履歴] の次のページが表示されます。

表示をカスタマイズする

CloudTrail コンソールのイベント履歴の表示は、次の設定から選択してカスタマイズできます。

- ページサイズ - 各ページに表示するイベントの数を 10、25、50 から選択します。
- 行を折り返す - 各イベントのすべてのテキストが表示されるようにテキストを折り返します。
- 行のストライプ化 - テーブルの 1 行おきにシェーディングを行います。

- イベント時間表示 - イベント時間を UTC で表示するか、ローカルタイムゾーンで表示するかを選択します。
- 表示する列の選択 - 表示する列を選択します。デフォルトでは、次の列が表示されます。
  - イベント名
  - イベント時間
  - [ユーザーネーム]
  - [イベントソース]
  - リソースタイプ
  - リソース名

> **Note**
>
> 列の順序を変更したり、[イベント履歴] から手動でイベントを削除したりすることはできません。

表示をカスタマイズするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
2. ナビゲーションペインで [Event history (イベント履歴)] を選択します。
3. 歯車アイコンを選択します。
4. [ページサイズ] では、1 ページに表示するイベントの数を選択します。
5. [行を折り返す] を選択すると、各イベントのすべてのテキストが表示されます。
6. [行のストライプ化] を選択すると、テーブルの 1 行おきにシェーディングを行います。
7. [イベント時間表示] では、イベント時間を UTC で表示するか、ローカルタイムゾーンで表示するかを選択します。デフォルトでは、[UTC] が選択されています。
8. [Select visible columns] で、表示する列を選択します。非表示にする列の選択を解除します。
9. 変更が完了したら、[確認] を選択します。

CloudTrail イベントのフィルタリング

[イベント履歴] のイベントのデフォルトの表示では、属性フィルターを使用して、表示されるイベントのリストから読み取り専用イベントを除外します。この属性フィルターは [読み取り専用] という

名前で、false に設定されます。このフィルターを削除すると、読み取りと書き込みの両方のイベントを表示できます。[読み取り] イベントのみを表示するには、フィルターの値を true に変更できます。他の属性でイベントをフィルタリングすることもできます。さらに、時間範囲でフィルタリングすることができます。

> **Note**
>
> 1 つの属性フィルターおよび時間範囲フィルターのみを適用できます。複数の属性フィルターを適用することはできません。

AWS アクセスキー

AWS リクエストの署名に使用されたアクセスキー ID。リクエストが、一時的セキュリティ認証情報で行われた場合、これは、一時的認証情報のアクセスキー IDです。

イベント ID

イベントの CloudTrail ID。各イベントには一意の ID があります。

イベント名

イベントの名前。例えば、`CreatePolicy` などの IAM イベントや、`RunInstances` などの Amazon EC2 イベントでフィルタリングできます。

[イベントソース]

AWS リクエストが行われたサービス (`iam.amazonaws.com`やなど) `s3.amazonaws.com`。[Event source] フィルタを選択すると、イベントソースのリストをスクロールできます。

読み取り専用

イベントの読み取りタイプ。イベントは、読み取りイベントまたは書き込みイベントとして分類されます。false に設定すると、読み取りイベントは表示されるイベントのリストに含まれません。デフォルトでは、この属性フィルターが適用され、値は false に設定されます。

リソース名

イベントによって参照されるリソースの名前または ID。たとえば、リソース名はAuto Scaling グループの場合は "auto-scaling-test-group"、EC2 インスタンスの場合は「i-12345678910」である可能性があります。

リソースタイプ

イベントによって参照されるリソースのタイプ。たとえば、リソースタイプは、EC2 の場合は、Instance、RDS の場合は、DBInstance となります。リソースタイプはサービスごとに異なります。 AWS

[Time range] (時間範囲)

イベントをフィルタリングする時間範囲。[相対範囲] または[絶対範囲] を選択することができます。過去 90 日間のイベントをフィルタリングすることができます。

[ユーザーネーム]

イベントによって参照される ID。例えば、これは、 ユーザー、 ロール名、またはサービスロールとすることができます。

選択した属性または時間に記録されたイベントがない場合、結果リストは空です。時間範囲に加えて、1 つの属性フィルタのみを適用できます。別の属性フィルタを選択した場合は、指定した時間範囲が保持されます。

次のステップでは、属性でフィルタリングする方法について説明します。

属性でフィルタリングするには

1. 属性で結果をフィルタリングするには、[ルックアップ属性] ドロップダウンリストをクリックし、テキストボックスに属性の値を入力するか、または選択します。
2. 属性フィルタを削除するには、属性フィルタボックスの右側にある [X] を選択します。

次のステップでは、開始と終了の日時でフィルタリングする方法について説明します。

開始と終了の日時でででフィルタリングするには

1. 表示したいイベントの時間範囲を絞り込むには、タイムレンジバーの時間範囲を選択します。[相対範囲] または[絶対範囲] を選択することができます。

   事前定義済みの値またはカスタム範囲を選択するには、[相対範囲] を選択します。プリセット値は、30 分、1 時間、12 時間、または 1 日です。カスタムの時間範囲を指定するには、[Custom] を選択します。

   [絶対範囲] を選択して開始時刻と終了時刻を指定します。ローカルタイムゾーンと UTC を切り替えることもできます。

2. 時間範囲フィルターを削除するには、時間範囲バーで [クリアして閉じる] を選択します。

イベントの詳細の表示

1. 結果リストでイベントを選択して、詳細を表示します。
2. イベントで参照されるリソースは、[Resources referenced] テーブルでイベントの詳細ページに移動します。
3. 一部の参照されているリソースのリンクがあります。リンクを選択すると、そのリソースのコンソールが開きます。
4. 詳細ページの [Event record] までスクロールして、JSON イベントレコードや、呼び出したイベントペイロードも確認できます。
5. ページパンくずの [イベント履歴] を選択してイベントの詳細ページを閉じ、[イベント履歴] に戻ります。

イベントのダウンロード

記録されたイベント履歴は、CSV または JSON 形式のファイルとしてダウンロードできます。1 つのファイルに最大 200,000 件のイベントをダウンロードできます。200,000 イベントの制限に達すると、 CloudTrail コンソールに追加のファイルをダウンロードするオプションが表示されます。ダウンロードするファイルのサイズを減らすには、フィルタと時間範囲を使用します。

> **Note**
>
> CloudTrail イベント履歴ファイルは、個々のユーザーが設定できる情報 (リソース名など) を含むデータファイルです。一部のデータは、このデータ (CSV インジェクション) の読み取りと分析に使用されるプログラムでコマンドとして解釈される可能性があります。たとえば、 CloudTrail イベントを CSV にエクスポートしてスプレッドシートプログラムにインポートすると、そのプログラムはセキュリティ上の問題について警告することがあります。システムの安全性を維持するため、このコンテンツの無効化を選択してください。ダウンロードしたイベント履歴ファイルでは、リンクまたはマクロを常に無効にします。

1. ダウンロードするイベントのフィルターと時間範囲を [イベント履歴] に追加します。たとえば、イベント名 `StartInstances` を指定し、過去 3 日間のアクティビティの時間範囲を指定できます。

2. [Download events] 選択し、その後 [Download as CSV] または [Download as JSON] を選択します。ダウンロードがすぐに開始されます。

> **Note**
>
> ダウンロードが完了するまで時間がかかる場合があります。迅速な結果を得るには、より特定のフィルタまたは短い時間範囲を使って結果を絞り込んでから、ダウンロードプロセスを開始します。ダウンロードはキャンセルできます。ダウンロードをキャンセルすると、一部のイベントデータのみを含む部分的なダウンロードがローカルコンピュータにある可能性があります。すべてのイベント履歴をダウンロードするには、ダウンロードを再起動します。

3. ダウンロードが完了したら、ファイルを開いて、指定したイベントを表示します。
4. ダウンロードをキャンセルするには、[Cancel] を選択し、[Cancel download] を選択して確認します。ダウンロードを再開する必要がある場合は、1 つ前のダウンロードのキャンセルが完了するまで待ちます。

AWS Configで参照されたリソースの表示

AWS Config 設定の詳細、関係、 AWS リソースの変更を記録します。

「参照リソース」ペインで、「AWS Config リソースタイムライン」列にあるを選択し、 AWS Config コンソールにリソースを表示します。

アイコンが灰色になっているか、 AWS Config オンになっていないか、リソースタイプを記録していない場合。 AWS Config アイコンを選択してコンソールに移動し、サービスをオンにするか、そのリソースタイプの記録を開始します。詳細については、『AWS Config 開発者ガイド』の「AWS Config コンソールを使ったセットアップ」を参照してください。

列に [Link not available] が表示された場合、次のいずれかの理由でリソースを表示できません。

- AWS Config リソースタイプはサポートされていません。詳細については、AWS Config デベロッパーガイドの「サポートされたリソース、項目の設定、関係」を参照してください。

- AWS Config 最近、リソースタイプのサポートが追加されましたが、 CloudTrail コンソールではまだ使用できません。 AWS Config コンソールでリソースを検索すると、そのリソースのタイムラインを確認できます。
- AWS アカウントリソースは別の人が所有しています。
- リソースは、マネージド IAM ポリシーなど AWS のサービス、別のユーザーが所有しています。
- リソースが作成され、すぐに削除されました。
- リソースは、最近作成または更新されました。

AWS Config コンソールでリソースを表示する読み取り専用権限をユーザーに付与する方法については、を参照してください。AWS Config コンソール上の情報を表示する権限を付与する CloudTrail

詳細については AWS Config、『AWS Config 開発者ガイド』を参照してください。

での最近の管理イベントの表示 AWS CLI

AWS リージョン aws cloudtrail lookup-eventsコマンドを使用して、過去 90 CloudTrail 日間の現在の管理イベントを検索できます。aws cloudtrail lookup-eventsこのコマンドは、 AWS リージョン 発生した場所のイベントを表示します。

検索は、管理イベントの以下の属性に対応しています：

- AWS アクセスキー
- イベント ID
- イベント名
- [イベントソース]
- 読み取り専用
- リソース名
- リソースタイプ
- [ユーザーネーム]

すべての属性はオプションです。

`lookup-events` コマンドには、以下のオプションがあります。

- `--max-items` *`<integer>`* – コマンドの出力で返される項目の総数。使用可能な項目の総数が指定された値を上回る場合、コマンドの出力で `NextToken` が提供されます。ページ分割を再開す

るには、後続コマンドの starting-token 引数で NextToken 値を指定します。 AWS CLIの範囲外で NextToken レスポンス要素を直接使用しないでください。

- --start-time *<timestamp>* – 指定された時刻以降に発生したイベントのみを返すよう指定します。指定された開始時刻が指定された終了時刻よりも後である場合は、エラーが返されます。
- --lookup-attributes*<integer>* — 検索属性のリストが含まれます。現在、リストに含めることができるアイテムは 1 つだけです。
- --generate-cli-skeleton *<string>* – API リクエストを送信せずに JSON スケルトンを標準出力に出力します。値なしまたは値入力を指定した場合、--cli-input-json の引数として使用できる入力 JSON のサンプルを表示します。同様に、yaml-input を指定すると、--cli-input-yaml で使用できる入力 YAML のサンプルが出力されます。値出力が提供された場合、コマンド入力を検証し、そのコマンドの出力 JSON のサンプルを返します。生成された JSON スケルトンはのバージョン間で安定しておらず、 AWS CLI 生成される JSON スケルトンの下位互換性は保証されません。
- --cli-input-json *<string>* – 指定された JSON 文字列から引数を読み取ります。JSON 文字列は、--generate-cli-skeletonパラメータで指定された形式に従います。コマンドラインで他の引数が指定されている場合、それらの値は JSON の値よりも優先されます。文字列は文字どおりに解釈されるため、JSON が提供する値を使用して任意のバイナリ値を渡すことはできません。これは --cli-input-yaml パラメータと一緒に指定することはできません。

AWS コマンドラインインターフェイスの使用に関する一般的な情報については、『ユーザーガイド』を参照してください。AWS Command Line Interface

目次

前提条件

- AWS CLI コマンドを実行するには、をインストールする必要があります AWS CLI。詳細については、「はじめに」を参照してください AWS CLI。
- AWS CLI バージョンが 1.6.6 以降であることを確認してください。CLI のバージョンを確認するには、コマンドラインで aws --version を実行します。
- アカウント AWS リージョン、 AWS CLI およびセッションのデフォルト出力形式を設定するには、aws configureコマンドを使用します。詳細については、「AWS コマンドラインインターフェイスの設定」を参照してください。

> **Note**
>
> CloudTrail AWS CLI コマンドでは大文字と小文字が区別されます。

コマンドラインのヘルプを取得する

lookup-events のコマンドライン ヘルプを表示するには 、次のコマンドを入力します。

```
aws cloudtrail lookup-events help
```

イベントの参照

> **Important**
>
> 検索リクエストのレートは、1 アカウント、1 リージョンあたり、1 秒間に2 回に制限されています。この制限を超えると、スロットリングエラーが発生します。

最新 10 件のイベントを表示するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --max-items 10
```

返されるイベントは、次に示す架空のサンプルのようになります。このサンプルは読みやすい形式にしてあります。

```
{
```

```
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
    "Events": [
        {
            "EventId": "0ebbaee4-6e67-431d-8225-ba0d81df5972",
            "Username": "root",
            "EventTime": 1424476529.0,
            "CloudTrailEvent": "{
                  \"eventVersion\":\"1.02\",
                  \"userIdentity\":{
                        \"type\":\"Root\",
                        \"principalId\":\"111122223333\",
                        \"arn\":\"arn:aws:iam::111122223333:root\",
                        \"accountId\":\"111122223333\"},
                  \"eventTime\":\"2015-02-20T23:55:29Z\",
                  \"eventSource\":\"signin.amazonaws.com\",
                  \"eventName\":\"ConsoleLogin\",
                  \"awsRegion\":\"us-east-2\",
                  \"sourceIPAddress\":\"203.0.113.4\",
                  \"userAgent\":\"Mozilla/5.0\",
                  \"requestParameters\":null,
                  \"responseElements\":{\"ConsoleLogin\":\"Success\"},
                  \"additionalEventData\":{
                         \"MobileVersion\":\"No\",
                         \"LoginTo\":\"https://console.aws.amazon.com/console/home",
                         \"MFAUsed\":\"No\"},
                  \"eventID\":\"0ebbaee4-6e67-431d-8225-ba0d81df5972\",
                  \"eventType\":\"AwsApiCall\",
                  \"recipientAccountId\":\"111122223333\"}",
            "EventName": "ConsoleLogin",
            "Resources": []
        }
    ]
}
```


出力内の参照関連フィールドの説明については、このドキュメントで後述する「参照の出力フィールド」セクションを参照してください。 CloudTrail イベント内のフィールドの説明については、を参照してください。CloudTrail レコードの内容

返されるイベントの数を指定する

返されるイベントの数を指定するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --max-items <integer>
```

有効な値は 1 から 50 です。次の例では、1 つのイベントが返されます。

```
aws cloudtrail lookup-events --max-items 1
```

時間範囲でイベントを参照する

イベントは過去 90 日間の記録から参照できます。時間範囲を指定するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

`--start-time` *<timestamp>* を UTC で指定すると、指定された時刻かその後に発生したイベントのみが返されます。指定された開始時刻が指定された終了時刻よりも後である場合は、エラーが返されます。

`--end-time` *<timestamp>* を UTC で指定すると、指定された時刻かその前に発生したイベントのみが返されます。指定された終了時刻が指定された開始時刻よりも前である場合は、エラーが返されます。

デフォルトの開始時刻は、過去 90 日間のうち、データが利用できる最も早い日付です。デフォルトの終了時刻は、現在の時刻に最も近いイベント発生時刻です。

すべてのタイムスタンプは UTC で表示されます。

属性でイベントを参照する

属性でフィルタリングするには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

各 lookup-events コマンドに対し、属性キーと値のペアを 1 つだけ指定できます。次に示すのは、`AttributeKey` の有効な値です。値名では大文字と小文字が区別されます。

- `AccessKeyId`
- `EventId`
- `EventName`

- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

の最大長は 2000 AttributeValue 文字です。次の文字 ('_', ' ', , \\n ') は 2000 文字の制限に対して 2 文字としてカウントされます。

属性参照の例

次のコマンド例では、AccessKeyId の値が AKIAIOSFODNN7EXAMPLE であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=AccessKeyId,AttributeValue=AKIAIOSFODNN7EXAMPLE
```

以下のコマンド例は、指定のイベントを返します CloudTrailEventId。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventId,AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

次のコマンド例では、EventName の値が RunInstances であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=RunInstances
```

次のコマンド例では、EventSource の値が iam.amazonaws.com であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=EventSource,AttributeValue=iam.amazonaws.com
```

次のコマンド例では、書き込みイベントが返されます。GetBucketLocation や DescribeStream などの読み取りイベントは除外されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ReadOnly,AttributeValue=false
```

次のコマンド例では、ResourceName の値が CloudTrail_CloudWatchLogs_Role であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceName,AttributeValue=CloudTrail_CloudWatchLogs_Role
```

次のコマンド例では、ResourceType の値が AWS::S3::Bucket であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::S3::Bucket
```

次のコマンド例では、Username の値が root であるイベントが返されます。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

次の結果ページを指定する

lookup-events コマンドの次の結果ページを取得するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events <same parameters as previous command> --next-token=<token>
```

<token> の箇所に入る値は、前のコマンドの出力の最初のフィールドから取得されます。

コマンド内で --next-token を使用する場合は、前のコマンドと同じパラメータを使用する必要があります。例えば、次のコマンドを実行したとします。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root
```

次の結果ページを取得したい場合、コマンドは次のようになります。

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=Username,AttributeValue=root --next-token=kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juy3CIZ
```

JSON 入力をファイルから取得する

AWS CLI for some service AWS には、--generate-cli-skeletonと 2 つのパラメータがあり--cli-input-json、これを使用して JSON テンプレートを生成できます。このパラメータを変更し

て、--cli-input-jsonパラメータへの入力として使用できます。このセクションでは、これらのパラメータを aws cloudtrail lookup-events で使用する方法について説明します。一般的な情報については、「AWS CLI スケルトンと入力ファイル」を参照してください。

ファイルから JSON CloudTrail 入力を取得してイベントを検索するには

1. 次の例のように、lookup-events の出力をファイルにリダイレクトして、--generate-cli-skeleton で使用するための入力テンプレートを作成します。

```
aws cloudtrail lookup-events --generate-cli-skeleton > LookupEvents.txt
```

生成されたテンプレートファイル (LookupEventsこの場合は.txt) は以下のようになります。

```
{
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. テキストエディタを使用し、必要に応じて JSON を変更します。JSON 入力には、指定された値のみが含まれている必要があります。

> **Important**
>
> 空の値や Null 値は、使用する前にテンプレートからすべて削除する必要があります。

次の例では、時間範囲と、返される結果の最大数を指定しています。

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
```

```
}
```

3. 編集したファイルを入力として使用するには、次の例のように、構文 `--cli-input-json file://<filename>` を使用します。

```
aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

> **Note**
>
> `--cli-input-json` と同じコマンドラインで、他の引数を使用することもできます。

参照の出力フィールド

イベント

指定された参照属性と時間範囲に基づく参照イベントのリストです。イベントリストは時刻でソートされ、最新のイベントが最初に表示されます。各エントリには、検索要求に関する情報と、 CloudTrail 取得されたイベントの文字列表現が含まれます。

以下のエントリは、各参照イベント内のフィールドです。

CloudTrailEvent

返されたイベントのオブジェクト表現を含んだ JSON 文字列です。返される各要素については、「Record Body Contents」を参照してください。

EventId

返されたイベントの GUID を含んだ文字列です。

EventName

返されたイベントの名前を含んだ文字列です。

EventSource

AWS リクエストが行われたサービス。

EventTime

イベントの日時です (UNIX 時刻形式)。

リソース

返されたイベントによって参照されるリソースのリストです。各リソースエントリは、リソースタイプとリソース名を指定します。

ResourceName

イベントによって参照されるリソースの名前を含んだ文字列です。

ResourceType

イベントによって参照されるリソースのタイプを含んだ文字列です。リソースタイプを特定できない場合は、null が返されます。

ユーザー名

返されたイベントに対するアカウントのユーザー名を含んだ文字列です。

NextToken

前の `lookup-events` コマンドから次の結果ページを取得するための文字列です。トークンを使用するには、パラメータが元のコマンドと同じである必要があります。`NextToken` エントリが出力に表示されない場合、返す結果はそれ以上存在しません。

AWS CloudTrail Lake の使用

AWS CloudTrail Lake では、イベントに対して SQL ベースのクエリを実行できます。 CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いたイベントのイミュータブルなコレクションです。イベントデータをイベントデータストアに保存できる期間は、[1 年間の延長可能な保存料金] オプションを選択した場合は最大 3,653 日 (約 10 年)、[7 年間の保存料金] オプションを選択した場合は最大 2,557 日 (約 7 年間) です。イベントデータストアに適用するセレクタは、どのイベントが保持され、クエリに使用できるかを制御します。 CloudTrail Lake は、コンプライアンススタックを補完し、ほぼリアルタイムのトラブルシューティングを支援する監査ソリューションです。

CloudTrail Lake イベントデータストア

イベントデータストアを作成する際には、イベントデータストアに保存するイベントのタイプを選択します。イベントデータストアを作成して、CloudTrail イベント 、CloudTrail Insights イベント 、AWS Config 設定項目 、AWS Audit Manager 証拠 、または の外部からのイベント AWSを含めることができます。イベントスキーマはイベントカテゴリに固有であるため、各イベントデータストアには特定のイベントカテゴリ (AWS Config 設定項目など) のみを含めることができます。複数のリージョンとアカウントからのイベントなど、組織からのイベントを組織のイベントデータストア AWS Organizations に保存できます。サポートされている SQL JOIN キーワードを使用して、複数のイベントデータストアで SQL クエリを実行できます。複数のイベントデータストアに対してクエリを実行する方法については、「高度なマルチテーブルクエリのサポート」を参照してください。

証跡イベントを新規または既存のイベントデータストアにコピーして、証跡に記録されたイベントの point-in-time スナップショットを作成できます。詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。

イベントデータストアをフェデレーションして、 AWS Glue データカタログ内のイベントデータストアに関連付けられたメタデータを確認し、Amazon Athena を使用してイベントデータに対する SQL クエリを実行できます。 AWS Glue Data Catalog に保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

デフォルトでは、イベントデータストア内のすべてのイベントは によって暗号化されます CloudTrail。イベントデータストアを設定するときに、独自の AWS Key Management Service キー

を使用することを選択できます。独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

タグに基づいた承認を使用することによって、イベントデータストアに対するアクションへのアクセスを制御できます。詳細と例については、本ガイドの「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。

CloudTrail Lake ダッシュボードを使用して、イベントデータストア内のデータを視覚化できます。各ダッシュボードは複数のウィジェットで構成され、各ウィジェットは SQL クエリを表します。Lake ダッシュボードの詳細については、「 CloudTrail Lake ダッシュボードを表示する」を参照してください。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail の料金設定とコスト管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

CloudTrail Lake は、取り込まれたデータとストレージバイトに関する情報を提供する Amazon CloudWatch メトリクスをサポートしています。サポートされている CloudWatch メトリクスの詳細については、「」を参照してください CloudWatch サポート対象の指標。

> **Note**
>
> CloudTrail は通常、API コールから平均約 5 分以内にイベントを配信します。この時間は保証されません。

CloudTrail Lake 統合

CloudTrail Lake 統合を使用して、 の外部からのユーザーアクティビティデータを ログに記録して保存できます AWS。オンプレミスまたはクラウドでホストされている社内アプリケーションや SaaS アプリケーション、仮想マシン、コンテナなど、ハイブリッド環境の任意のソースからのユーザーアクティビティデータです。 CloudTrail Lake でイベントデータストアを作成し、アクティビティイベントを ログに記録するチャネルを作成したら、 `PutAuditEvents` API を呼び出してアプリケーションアクティビティを に取り込みます CloudTrail。その後、 CloudTrail Lake を使用して、アプリケーションから記録されたデータを検索、クエリ、分析できます。

統合では、数十 CloudTrailを超えるパートナーからのイベントデータストアにイベントを口グ記録することもできます。パートナーによる統合では、送信先となるイベントデータストア、チャネル、およびリソースポリシーを、ユーザーが作成します。統合の作成が完了したら、チャネルの ARN をパートナーに提供します。統合のタイプには、直接とソリューションの 2 種類が存在します。直接統合では、パートナーは PutAuditEvents API を呼び出して、 AWS アカウントのイベントデータストアにイベントを配信します。ソリューション統合では、アプリケーションは AWS アカウントで実行され、アプリケーションは PutAuditEvents API を呼び出して、 AWS アカウントのイベントデータストアにイベントを配信します。

統合の詳細については、「 の外部でイベントソースとの統合を作成する AWS」を参照してください。

CloudTrail Lake クエリ

CloudTrail Lake クエリは、イベント履歴 の単純なキーと値のルックアップ、または の実行よりも、イベントのより詳細でカスタマイズ可能なビューを提供しますLookupEvents。イベント履歴検索は 1 つの に限定され AWS アカウント、1 つの からのイベントのみを返し AWS リージョン、複数の属性をクエリすることはできません。対照的に、 CloudTrailLake ユーザーは複数のイベントフィールドで複雑な SQL クエリを実行できます。 CloudTrail Lake は、有効なすべての Presto SELECTステートメントと関数をサポートしています。サポートされている SQL 関数と演算子の詳細については、Presto ドキュメントウェブサイトの「関数と演算子」を参照してください。

CloudTrail Lake クエリを将来の使用のために保存し、クエリの結果を最大 7 日間表示できます。クエリを実行すると、クエリ結果を Amazon S3 バケットに保存できます。

CloudTrail コンソールには、独自のクエリの作成を開始するのに役立つ多数のサンプルクエリが用意されています。詳細については、「 CloudTrail コンソールにサンプルクエリが表示されます。」を参照してください。

CloudTrail Lake クエリには料金が発生します。Lake でクエリを実行すると、スキャンされたデータ量に基づいて料金が発生します。Lake CloudTrail の料金設定とコスト管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

追加リソース

以下のリソースは、 CloudTrail Lake とは何か、またその使用方法をよりよく理解するのに役立ちます。

- CloudTrail Lake を使用した監査口グ管理のモダナイズ (YouTube ビデオ)

- AWS CloudTrail Lake のAWS ソース以外の からのアクティビティイベントのログ記録 (YouTube ビデオ)
- AWS CloudTrail Lake と Amazon Athena でアクティビティログを分析する (YouTube ビデオ)
- ワークフォースと顧客 ID のアクティビティログを可視化する (AWS ブログ)
- AWS CloudTrail Lake を使用して AWS サービスエンドポイントへの古い TLS 接続を特定する (AWS ブログ)
- Arctic Wolf が AWS CloudTrail Lake を使用してセキュリティと運用を簡素化する方法 (AWS ブログ)
- CloudTrail Lake FAQs
- AWS CloudTrail API リファレンス
- AWS CloudTrail データ API リファレンス
- AWS CloudTrail パートナーオンボーディングガイド

CloudTrail Lake がサポートするリージョン

現在、 CloudTrail Lake は次の でサポートされています AWS リージョン。

リージョン名	リージョン
米国東部 (バージニア北部)	us-east-1
米国東部 (オハイオ)	us-east-2
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (ジャカルタ)	ap-southeast-3
アジアパシフィック (ムンバイ)	ap-south-1

リージョン名	リージョン
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (東京)	ap-northeast-1
カナダ (中部)	ca-central-1
欧州 (フランクフルト)	eu-central-1
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
ヨーロッパ (ミラノ)	eu-south-1
欧州 (パリ)	eu-west-3
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
欧州 (チューリッヒ)	eu-central-2
イスラエル (テルアビブ)	il-central-1
中東 (バーレーン)	me-south-1
中東 (アラブ首長国連邦)	me-central-1
南米 (サンパウロ)	sa-east-1
AWS GovCloud （米国東部）	us-gov-east-1
AWS GovCloud （米国西部）	us-gov-west-1

CloudTrail サービスエンドポイントの詳細については、AWS CloudTrail 「 エンドポイントとクォータ」を参照してください。

CloudTrail での の使用の詳細については AWS GovCloud (US) Regions、 AWS GovCloud (US) ユーザーガイドの「サービスエンドポイント」を参照してください。

CloudTrail 湖の概念と用語

このセクションでは、 AWS CloudTrail Lake を使用する際に役立つ主要な概念と用語について説明します。

概念と用語

- イベントデータストア
- 統合
- クエリ
- ダッシュボード

イベントデータストア

イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いたイベントのイミュータブルなコレクションです。

イベントデータストアを作成して、CloudTrail 管理イベントやデータイベント、CloudTrail インサイトイベント、AWS Audit Manager エビデンス、AWS Config 設定項目、または外部のイベントを記録できます AWS。

アドバンストイベントセレクタ

高度なイベントセレクタで、イベントデータストアに含めるベントが決まります。高度なイベントセレクタによって、重要なイベントのみがログに記録されるため、コスト管理に役立ちます。

管理イベントとデータイベントは、高度なイベントセレクタを使用してフィルタリングできます。たとえば、管理イベントを収集するイベントデータストアを作成する場合、 AWS Key Management Service (AWS KMS) または Amazon Relational Database Service (Amazon RDS) データ API イベントを除外できます。通常、`EncryptDecrypt`、 AWS KMS などのアクションはイベントの 99% `GenerateDataKey` 以上を生成します。

AWS Config 構成項目、Audit Manager エビデンス、または外部イベントの場合 AWS、高度なイベントセレクターは、そのタイプのイベントをイベントデータストアに含めるためにのみ使用されます。

フェデレーション

フェデレーションでは、 AWS Glue Data Catalog 内のイベントデータストアに関連付けられたメタデータを確認し、Amazon Athena を使用してイベントデータに対して SQL クエリを実行できます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンは、クエリするデータを検索、読み取り、処理する方法を知ることができます。

Lake クエリフェデレーションを有効にすると、 CloudTrail ユーザーに代わってフェデレーションリソースを作成し、それらのリソースをに登録します。AWS Lake FormationLake フェデレーションを有効にすると、追加の手順を実行しなくても Athena のイベントデータを直接クエリできます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

料金オプション

イベントデータストアを作成するときは、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかるコスト、および、そのイベントデータストアの保持期間のデフォルトと最大が決まります。料金については、「AWS CloudTrail の料金」と「 CloudTrail Lake コストの管理」を参照してください。

保持期間

イベントデータストアの保存期間によって、イベントデータがイベントデータストアに保持される期間が決まります。 CloudTrail Lake は、`eventTime`イベントが指定された保存期間内であるかどうかをチェックして、イベントを保持するかどうかを決定します。例えば、保存期間を 90 日に指定した場合、90 CloudTrail `eventTime` 日以上経過したイベントは削除されます。

デフォルト保持期間

イベントデータストアのデフォルト保持期間は、イベントデータがイベントデータストアに保持されるデフォルトの日数です。イベントデータストアのデフォルト保持期間の間は、ストレージは取り込み料金に含まれており追加料金はありません。デフォルトの保存期間を過ぎると、ストレージの料金はです pay-as-you-go。

最大保持期間

イベントデータストアの最大保持期間は、イベントデータストアにデータを保持できる最大日数を表します。

終了保護

デフォルトでは、イベントデータストアでは終了保護が有効になり、イベントデータストアが誤って削除されるのを防ぎます。終了保護が有効になっているイベントデータストアを削除するには、イベントデータストアの詳細ページの [アクション] メニューから [終了保護の変更] を選択します。そうすると、イベントデータストアの削除に進むことができます。詳細については、「コンソールで終了保護を変更する」を参照してください。

統合

CloudTrail Lake インテグレーションを使用すると、以下のソースからのユーザーアクティビティデータを記録して保存できます。

- 外部 AWS
- オンプレミスやクラウド、仮想マシン、コンテナでホストされている社内アプリケーションや Software as a Service (SaaS) アプリケーションなど、ハイブリッド環境のすべてのソース。

統合には、イベントを伝送するチャネルと、イベントを受信するイベントデータストアが必要です。インテグレーションを設定したら、PutAuditEventsAPI オペレーションを呼び出して、アプリケーションのアクティビティをに取り込みます CloudTrail。その後、 CloudTrail Lake を使用して、アプリケーションからログに記録されたデータを検索、クエリ、分析できます。詳細については、「外部のイベントソースとの統合を作成 AWS」を参照してください。

統合タイプ

統合には、直接とソリューションの 2 種類が存在します。直接統合では、パートナーが PutAuditEvents API オペレーションを呼び出して、お客様の AWS アカウントのイベントデータストアにイベントを配信します。ソリューション統合では、 AWS アカウント アプリケーションがユーザー内で実行され、アプリケーションが PutAuditEvents API オペレーションを呼び出して、のイベントデータストアにイベントを配信します AWS アカウント。

チャネル

業務外のソースからのイベントを、 AWS CloudTrail チャネルを使って連携する外部パートナーや独自のソースからLakeにイベントを取り込むことで CloudTrail、業務外のソースからのイベントをアクティビティできます。チャネルを作成するときは、チャネルソースから着信するイベントを保存するイベントデータストアを 1 つまたは複数選択しま

す。eventCategory="ActivityAuditLog" イベントを口グ記録するように送信先イベントデータストアが設定されているのであれば、必要に応じて、チャネルの送信先をそれらのストアに変更することが可能です。外部パートナーからのイベント用のチャネルを作成するときは、チャネル Amazon リソースネーム (ARN) をパートナーまたはソースアプリケーションに提供します。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチする JSON ポリシードキュメントです。チャネルにアタッチされたリソースベースのポリシーにより、ソースはチャネルを介してイベントを送信できます。チャネルにリソースポリシーがない場合、そのチャネルの所有者だけが、チャネル内で PutAuditEvents API を呼び出すことができます。詳細については、「AWS CloudTrail リソースベースのポリシーの例」を参照してください。

クエリ

CloudTrail Lake のクエリは SQL で作成されます。 CloudTrail Lake Editor タブでクエリを作成するには、SQL でクエリを一から記述するか、保存済みまたはサンプルクエリを開いて編集します。含まれているサンプルクエリを独自の変更で上書きすることはできませんが、新しいクエリとして保存することはできます。詳細については、「クエリを作成または編集する」を参照してください。

CloudTrail Lake Presto SELECT はすべての有効なステートメントと関数をサポートしています。サポートされている SQL 関数と演算子の詳細については、Presto ドキュメントウェブサイトの「関数と演算子」を参照してください。

ダッシュボード

CloudTrail Lake ダッシュボードを使用すると、イベントデータストア内のイベントを視覚化し、トップ、ユーザー AWS のサービス、エラーなどのイベントの傾向を確認できます。詳細については、「 CloudTrail Lake ダッシュボードを表示する」を参照してください。

ダッシュボードタイプ

イベントデータストアで使用できるダッシュボードタイプは、イベントデータストアの高度なイベントセレクタの設定によって異なります。たとえば、 CloudTrail 管理イベントに関する情報が表示されるダッシュボードでは、 CloudTrail 現在選択されているイベントデータストアが管理イベントを収集している場合にのみダッシュボードを選択できます。

使用できるダッシュボードのタイプを以下に示します。

- 概要ダッシュボード — 最もアクティブなユーザーを AWS リージョン、 AWS のサービス イベント数別に表示します。また、`read` と `write` の管理イベントのアクティビティ、最もスロットリングされているイベント、上位のエラーに関する情報も表示できます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。
- [管理イベント] ダッシュボード – ユーザーごとに、コンソールへのサインインイベント数、アクセス拒否イベント数、破壊的なアクション数、上位のエラーが表示されます。ユーザーごとに TLS バージョンと古い TLS 呼び出しに関する情報を表示することもできます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。
- [S3 データイベント] ダッシュボード – Amazon S3 アカウントのアクティビティ、最もアクセスされた S3 オブジェクト、上位の S3 ユーザー、上位の S3 アクションが表示されます。このダッシュボードは、Amazon S3 データイベントを収集するイベントデータストアで使用できます。
- [Insights イベント]ダッシュボード – 全体的な Insights タイプ別の Insights イベントの比率、上位ユーザーとサービスに関する Insights タイプ別の Insights イベントの比率、および 1 日あたりの Insights イベント数が表示されます。ダッシュボードには、最大 30 日間の Insights イベントを一覧表示するウィジェットも含まれます。このダッシュボードは、Insights イベントを収集するイベントデータストアでのみ利用可能です。

> **Note**
>
> - CloudTrail ソースイベントデータストアで初めてインサイトを有効にした後、異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントの配信には最大 7 日かかることがあります。詳細については、「Insights イベントの配信を理解する」を参照してください。
> - [Insights イベント] ダッシュボードには、ソースイベントデータストアの設定によって決定される、選択したイベントデータストアによって収集された Insights イベントに関する情報のみが表示されます。例えば、ソースイベントデータストアで、`ApiErrorRateInsight` ではなく `ApiCallRateInsight` の Insights イベントを有効にしている場合には、`ApiErrorRateInsight` の Insights イベントに関する情報は表示されません。

ウィジェット

ウィジェットは、折れ線グラフや棒グラフなど、ダッシュボードを構成して可視化するコンポーネントです。各ウィジェットは、基になるクエリを表します。[クエリを実行] を選択すると、CloudTrail システムによって生成されたクエリが実行され、各ウィジェットのデータが入力されます。

CloudTrail Lake イベントデータストア

イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いた、イベントのイミュータブルなコレクションです。

CloudTrail Lake でイベントデータストアを作成するときは、イベントデータストアに含めるイベントのタイプを選択します。イベントデータストアを作成して、データまたは管理イベント、Insights CloudTrail イベント、 AWS Config 設定項目、または 外のイベントを含める CloudTrailことができます AWS。イベントスキーマはイベントカテゴリに固有であるため、各イベントデータストアタイプには特定のイベントカテゴリ (AWS Config 設定項目など) のみを含めることができます。サポートされている SQL JOIN キーワードを使用して、複数のイベントデータストアで SQL クエリを実行できます。複数のイベントデータストアに対してクエリを実行する方法については、「高度なマルチテーブルクエリのサポート」を参照してください。

各イベントデータストアタイプでサポートされるイベントカテゴリを以下の表に示します。「eventCategory」列は、そのタイプのイベントを収集するためにアドバンスイベントセレクタで指定する値を示します。

イベントタイプ (コンソール)	eventCategory (API)	説明

CloudTrail イベント	`Management`
	
	`Data`
		このイベントデータストアタイプは、CloudTrail 管理イベントとデータイベントを収集できます。詳細については、「イベント のイベントデータストアを作成する CloudTrail 」を参照してください。

CloudTrail Insights イベント	`Insight`	このイベントデータストアタイプは Insights CloudTrail イベントを収集できます。Insights イベントを受信するには、 CloudTrail 管理イベントをログに記録し、Insights を有効にするソースイベントデータストアが必要です。送信元および送信先のイベントデータストアの作成については、 CloudTrail 「Insights イベント用のイベントデータストアを作成する」を参照してください。

イベントタイプ (コンソール)	eventCategory (API)	説明
設定項目	`ConfigurationItem`	このイベントデータストアタイプは、 AWS Config 設定項目を収集できます。詳細については、AWS Config「設定項目 のイベントデータストアを作成する」を参照してください。
[統合からのイベント]	`ActivityAuditLog`	このイベントデータストアタイプは、統合から非AWS イベントを収集できます。詳細については、「 以外のイベントのイベントデータストアを作成する AWS」を参照してください。

Audit Manager コンソールを使用して、 AWS Audit Manager 証拠用のイベントデータストアを作成することもできます。Audit Manager を使用して CloudTrail Lake で証拠を集約する方法の詳細については、 AWS Audit Manager ユーザーガイドの「証拠ファインダーと CloudTrail Lake の連携について」を参照してください。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail の料金設定と管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

以下のセクションでは、イベントデータストアを作成、更新、管理する方法について説明します。

トピック

- コンソールを使用してイベントデータストアを作成、更新、管理する
- を使用して、イベントデータストアを作成、更新、管理します AWS CLI
- イベントデータストアのライフサイクルを管理する
- イベントデータストアへ証跡イベントをコピーします
- イベントデータストアのフェデレーション
- 組織のイベントデータストア

コンソールを使用してイベントデータストアを作成、更新、管理する

CloudTrail コンソールを使用して、イベントデータストアを作成、更新、管理できます。イベントデータストアでイベント取り込みを開始および停止し、コンソールを使用して Lake クエリフェデレーションを有効にすることもできます。

CloudTrail コンソールを使用してイベントデータストアを作成または更新すると、次の利点があります。

- イベントデータストアを初めて作成する場合は、 CloudTrail コンソールを使用して使用可能な機能とオプションを表示できます。
- データイベントをログに記録するようにイベントデータストアを設定する場合は、 CloudTrail コンソールを使用して使用可能なデータ型を表示できます。詳細については、「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」および「データイベントをログ記録する」を参照してください。
- の外部でイベントをログに記録するようにイベントデータストアを設定する場合 AWS、CloudTrail コンソールを使用すると、利用可能なパートナーに関する情報を表示できます。詳細については、「コンソール AWS を使用して、 の外部でイベントのイベントデータストアを作成する」を参照してください。

トピック

コンソールを使用してイベントのイベントデータストア CloudTrailを作成する

イベントの CloudTrail イベントデータストアは、 CloudTrail 管理イベントとデータイベントをログに記録できます。イベントデータをイベントデータストアに保存できる期間は、[延長可能な 1 年間

の保持料金] オプションを選択した場合は最大 3,653 日 (約 10 年)、[7 年間の保持料金] オプションを選択した場合は最大 2,557 日 (約 7 年) です。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail の料金とコスト管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

CloudTrail 管理イベントまたはデータイベント用のイベントデータストアを作成するには

この手順を使用して、 CloudTrail 管理イベント、データイベント、または管理イベントとデータイベントの両方をログに記録するイベントデータストアを作成します。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [Configure event data store] (イベントデータストアの設定) ページの [General details] (全般的な詳細) で、イベントデータストアの名前を入力します。名前は必須です。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。

- デフォルトの保持期間: 2,557 日間
- 最長保持期間: 2,557 日間

6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかを確認することで、`eventTime`イベントを保持するかどうかを決定します。例えば、保持期間を 90 日と指定すると、 `eventTime`は 90 日を経過するとイベント CloudTrail を削除します。

   > **Note**
   >
   > このイベントデータストアに証跡イベントをコピーする場合、 `eventTime`は指定された保持期間より古いイベントをコピー CloudTrail しません。適切な保持期間を決定するには、コピーする最も古いイベントの合計を日数で、イベントデータストアにイベントを保持する日数 (保持期間 = *`oldest-event-in-days`* +) を計算します*`number-days-to-retain`*。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

7. (オプション) を使用して暗号化を有効にするには AWS Key Management Service、自分の を使用する AWS KMS keyを選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定します`alias/`*`MyAliasName`*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

> **Note**
>
> 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

   b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

   c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [Tag] (タグ) セクションでは、イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法の詳細については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. 「イベントの選択」ページでAWS 「イベント」を選択し、CloudTrail「イベント」を選択します。

12. CloudTrail イベント では、少なくとも 1 つのイベントタイプを選択します。[Management events] (管理イベント) がデフォルトで選択されています。イベントストアには、管理イベントとデータイベントの両方を追加できます。管理イベントの詳細については、「管理イベントのログ記録」を参照してください。データイベントの詳細については、「データイベントをログ記録する」を参照してください。
13. (オプション) 既存のトレイルからイベントをコピーして過去のイベントに関するクエリを実行する場合は、[Copy trail events] (トレイルイベントのコピー) を選択します。証跡イベントを組織のイベントデータストアにコピーするには、組織の管理アカウントを使用する必要があります。委任された管理者アカウントは、証跡イベントを組織のイベントデータストアにコピーできません。証跡イベントのコピーに関する考慮事項の詳細については、「証跡イベントのコピーに関する留意事項」を参照してください。
14. イベントデータストアが AWS Organizations 内のすべてのアカウントからのイベントを収集するようにするには、[Enable for all accounts in my organization] (組織内のすべてのアカウントについて有効化) を選択します。組織に関するイベントを収集するイベントデータストアを作成するには、その組織の管理アカウントまたは委任された管理者アカウントにサインインする必要があります。

    > **Note**
    >
    > 証跡イベントをコピーしたり Insights イベントを有効にしたりするには、組織の管理アカウントにサインインする必要があります。

15. 追加設定を展開して、イベントデータストアですべての のイベントを収集するか AWS リージョン、現在の のみのイベントを収集するかを選択し AWS リージョン、イベントデータストアでイベントを取り込むかを選択します。デフォルトでは、イベントデータストアは、アカウントのすべてのリージョンからイベントを収集し、データストアの作成時にイベントの取り込みを開始します。

    a. 現在のリージョンでログ記録されたイベントのみを含めるときは、[イベントデータストアに現在のリージョンのみを含める] を選択します。このオプションを選択しない場合、イベントデータストアにはすべてのリージョンからのイベントが含まれます。

    b. イベントデータストアでイベントの取り込みを開始したくないときは、[イベントを取り込む] の選択を解除します。例えば、証跡イベントをコピーしており、イベントデータストアに未来のイベントを含めたくないときは、[イベントを取り込む] の選択を解除するとよいでしょう。デフォルトでは、イベントデータストアは作成されたときにイベントの取り込みを開始します。

16. イベントデータストアに管理イベントが含まれている場合は、次のオプションを選択できます。管理イベントの詳細については、「管理イベントのログ記録」を参照してください。

    a. [読み取り] イベント、[書き込み]、またはその両方を含めるかどうかを選択します。少なくとも 1 つが必要です。

    b. イベントデータストアから AWS Key Management Service または Amazon RDS Data API イベントを除外するかどうかを選択します。

    c. Insights を有効にするかどうかを選択します。Insights を有効にするには、このイベントデータストア内の管理イベントアクティビティに基づいて Insights イベントを収集する送信先イベントデータストアを設定する必要があります。

       Insights を有効にすることを選択した場合は、次の手順を実行します。

       i. [Insights を有効にする] で、Insights イベントをログに記録する送信先イベントストアを選択します。送信先イベントデータストアは、このイベントデータストア内の管理イベントアクティビティに基づいて Insights イベントを収集します。送信先イベントデータストアの作成方法については、「Insights イベントをログに記録する送信先イベントデータストアを作成するには」を参照してください。

       ii. Insights タイプを選択します。[API コールレート]、[API エラー率] のいずれかまたは両方を選択できます。[API コール率] の Insights イベントをログに記録するには、[Write] 管理イベントをログ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、[Read] または [Write] 管理イベントをログ記録している必要があります。

17. イベントデータストアにデータイベントを含めるには、次の手順を実行します。

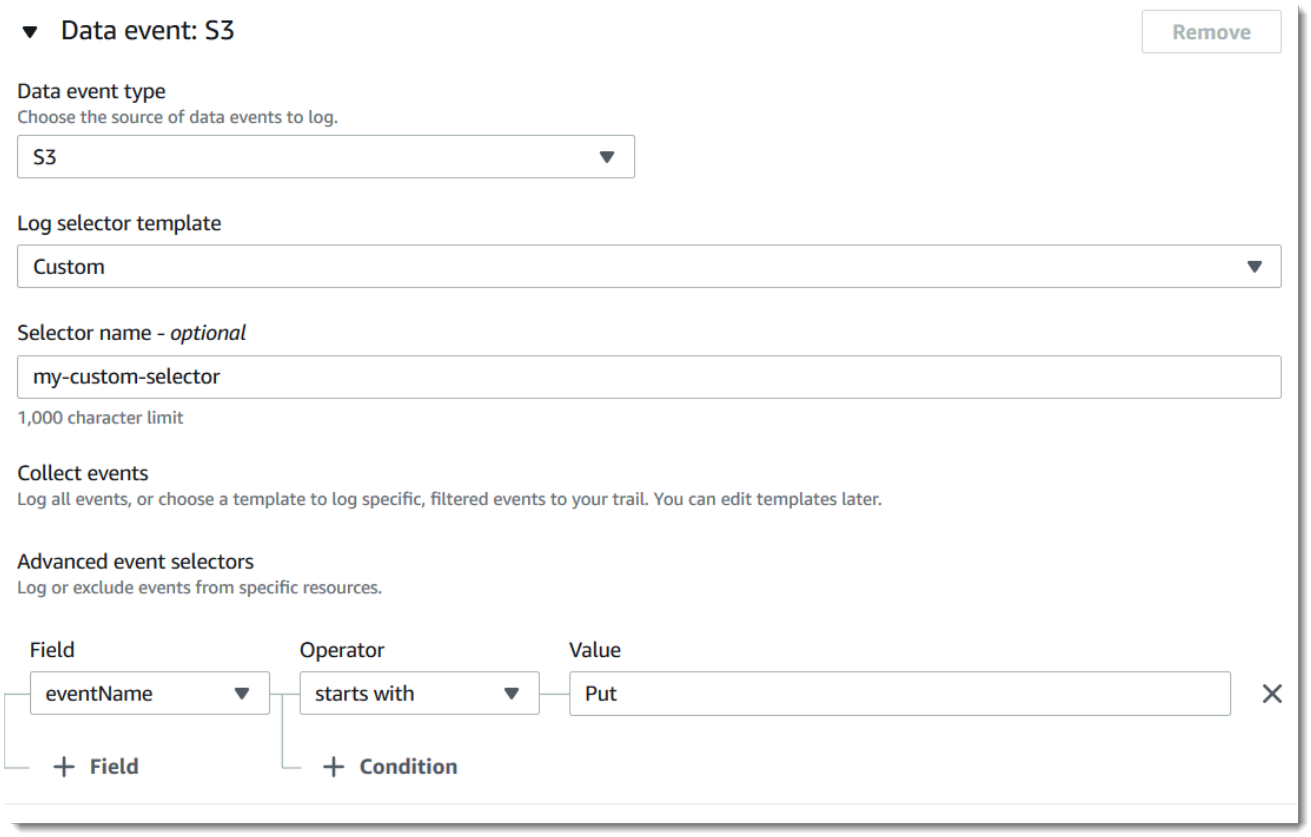
    a. データイベントタイプを選択します。これは、データイベントがログに記録される AWS のサービス および リソースです。Lake Formation によって作成された AWS Glue テーブルのデータイベントをログに記録するには、データ型に Lake Formation を選択します。

    b. [Log selector template] (ログセレクタテンプレート) でテンプレートを選択します。すべてのデータイベント、`readOnly` イベント、もしくは `writeOnly` イベントをログに記録することを選択、または [Custom] (カスタム) を選択してカスタムログセレクタを構築することができます。

    c. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「`Name`」と表示され、[JSON ビュー] を展開すると表示されます。

d. [Advanced event selectors] (高度なイベントセレクタ) で、[Field] (フィールド)、[Operator] (オペレーター)、および [Value] (値) の値を選択して式を作成します。イベントデータストアの高度なイベントセレクタは、証跡に適用する高度なイベントセレクタと同じように機能します。高度なイベントセレクタを構築する方法の詳細については、「高度なイベントセレクタを使用したデータイベントのフィルタリング」を参照してください。

以下の例は、[Custom] (カスタム) ログセレクタテンプレートを使用して、`Put` で始まる S3 オブジェクト (`PutObject` など) からのイベント名のみを選択します。高度なイベントセレクタは、他のイベントタイプやリソース ARN を含めたり除外したりしないため、イベント名が `Put` で始まるすべての S3 データイベント (読み取りと書き込みの両方) がイベントデータストアに保存されます。



> **Important**
>
> S3 バケット ARN を使用することによって高度なイベントセレクタでデータイベントを除外または含めるには、常に [Starts with] (次で始まる) オペレーターを使用してください。

e. オプションで、[JSON view] (JSON ビュー) を展開して、高度なイベントセレクタを JSON ブロックとして表示します。

f. データイベントを ログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。データイベントタイプの高度なイベントセレクタを設定するには、ステップ からこのステップを繰り返します。

18. イベントデータストアに既存の証跡イベントをコピーするには、次を実行します。

a. コピーするトレイルを選択します。デフォルトでは、 は S3 バケットの`CloudTrail`プレフィックスとプレフィックス内の`CloudTrail`プレフィックスに含まれる CloudTrail イベント CloudTrail のみをコピーし、他の AWS サービスのプレフィックスはチェックしません。別のプレフィックスに含まれる CloudTrail イベントをコピーする場合は、S3 URI を入力」を選択し、S3 を参照」を選択してプレフィックスを参照します。証跡のソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS キーポリシーで がデータを復号 CloudTrail 化できることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、各キーのポリシーを更新して、 CloudTrail がバケット内のデータを復号できるようにする必要があります。KMS キーポリシーの更新の詳細については、「ソース S3 バケット内のデータを復号化するための KMS キーポリシー」を参照してください。

b. イベントをコピーする時間範囲を選択します。 は、証跡イベントをコピーする前に、プレフィックスとログファイル名 CloudTrail をチェックして、名前に選択した開始日と終了日の間の日付が含まれていることを確認します。[Relative range] (相対範囲) または[Absolute range] (絶対範囲) を選択することができます。ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の時間範囲を選択します。

> **Note**
>
> CloudTrail は、イベントデータストアの保持期間`eventTime`内の を持つ証跡イベントのみをコピーします。例えば、イベントデータストアの保持期間が 90 日の場合、 CloudTrail は 90 日より`eventTime`古い の証跡イベントをコピーしません。

- 相対範囲 を選択した場合、過去 6 か月、1 年、2 年、7 年、またはカスタム範囲に ログ記録されたイベントをコピーできます。 は、選択した期間内に ログ記録されたイベント CloudTrail をコピーします。

- 絶対範囲 を選択した場合、特定の開始日と終了日を選択できます。選択した開始日と終了日の間に発生したイベント CloudTrail をコピーします。

c. [Permissions] (アクセス許可) については、以下の IAM ロールのオプションから選択します。既存の IAM ロールを選択する場合は、IAM ロールポリシーが必要なアクセス許可を提供していることを確認してください。IAM ロールの許可の更新の詳細については、「証跡イベントをコピーするための IAM 許可」を参照してください。

- [Create a new role (recommended)] (新しいロールの作成 (推奨)) を選択して、新しい IAM ロールを作成します。「IAM ロール名を入力」で、ロールの名前を入力します。 は、この新しいロールに必要なアクセス許可 CloudTrail を自動的に作成します。
- カスタム IAM ロール ARN の使用 を選択して、リストにないカスタム IAM ロールを使用します。[Enter IAM role ARN] (IAM ロールの ARN を入力) で、IAM ARN を入力します。
- ドロップダウンリストから既存の IAM ロールを選択します。

19. [Next] (次へ) を選択して、選択内容を確認します。
20. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。
21. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    これ以降、イベントデータストアは、高度なイベントセレクタに一致するイベントをキャプチャします ([イベントを取り込む] オプションを選択したままにしている場合)。イベントデータストアを作成する前に発生したイベントは、既存の証跡イベントをコピーすることを選択しない限り、イベントデータストアには保存されません。

これで、新しいイベントデータストアに対してクエリを実行できるようになりました。[Sample queries] (サンプルクエリ) タブは、使用を開始するためのサンプルクエリを提供します。クエリの作成と編集の詳細については、「クエリを作成または編集する」を参照してください。

CloudTrail Lake ダッシュボードを表示して、イベントデータストア内のイベントを視覚化することもできます。Lake ダッシュボードの詳細については、「 CloudTrail Lake ダッシュボードを表示する」を参照してください。

例: 管理イベント用のイベントデータストアを作成する

このチュートリアルでは、すべての AWS リージョンのすべての管理イベントをログに記録し、データイベントをログに記録しないイベントデータストアを作成する方法を示します。管理イベ

ントの例には、IAM `CreateUser` や `AttachRolePolicy` イベントなどのセキュリティイベント、`RunInstances` や `CreateBucket` などのリソースイベントが含まれています。

管理イベント用にイベントデータストアを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. 「イベントデータストアの設定」ページの一般的な詳細「」で、イベントデータストアに などの名前を付けます*my-management-events-eds*。イベントデートストアの意図をすぐに識別できる名前を使用するのがベストプラクティスです。 CloudTrail 命名要件については、「」を参照してください命名の要件。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかを確認することで、eventTimeイベントを保持するかどうかを決定します。例えば、保持期間を 90 日と指定すると、 eventTimeは 90 日を経過するとイベント CloudTrail を削除します。

7. (オプション) [暗号化] で、独自の KMS キーを使用してイベントデータストアを暗号化するかどうかを選択します。デフォルトでは、イベントデータストア内のすべてのイベントは、 AWS が所有および管理する KMS キー CloudTrail を使用して暗号化されます。

   独自の KMS キーを使用して暗号化を有効にするには、[独自の AWS KMS key を使用する] を選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定しますalias/*MyAliasName*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

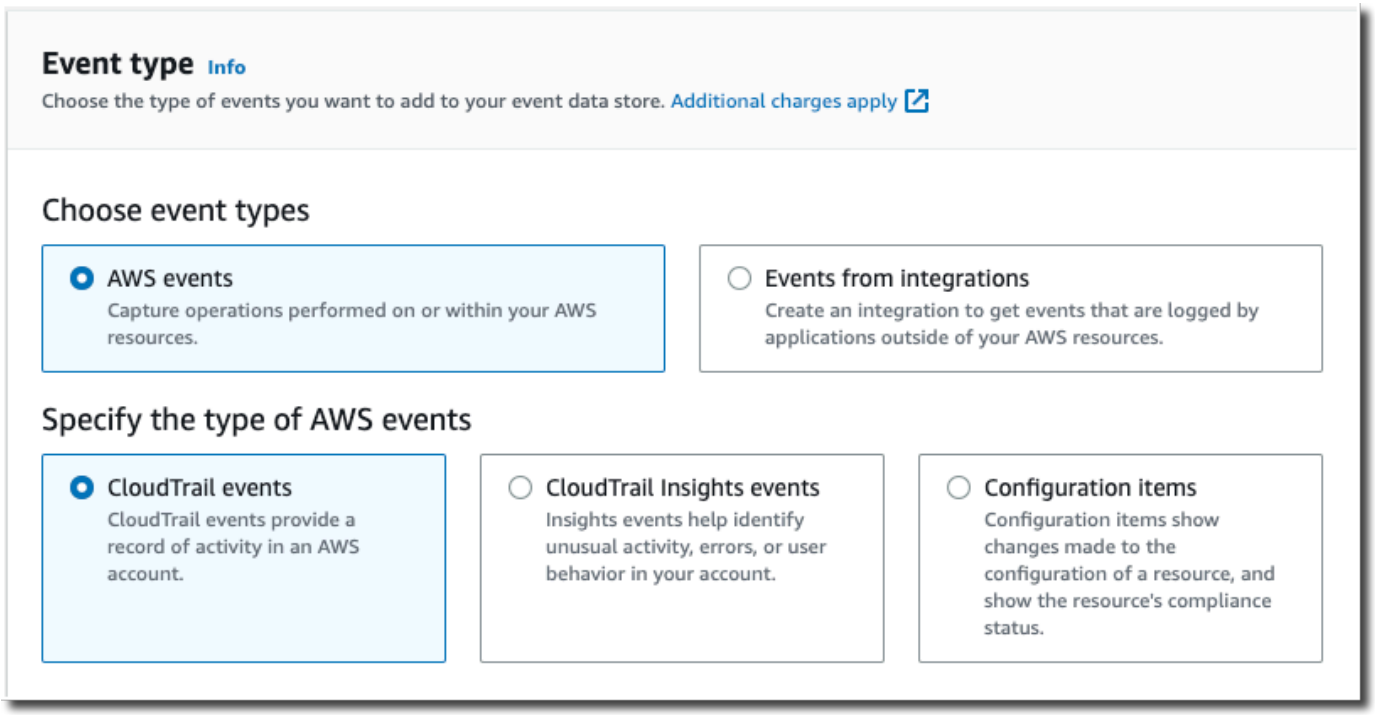
c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) をデータセットに追加します。タグは、 CloudTrail イベントデータストアを識別するのに役立ちます。例えば、**`stage`** という名前の **`prod`** という値のタグをアタッチできます。タグを使用して、イベントデータストアへのアクセスを制限できます。タグを使用して、イベントデータストアのクエリコストと取り込みコストを追跡することもできます。

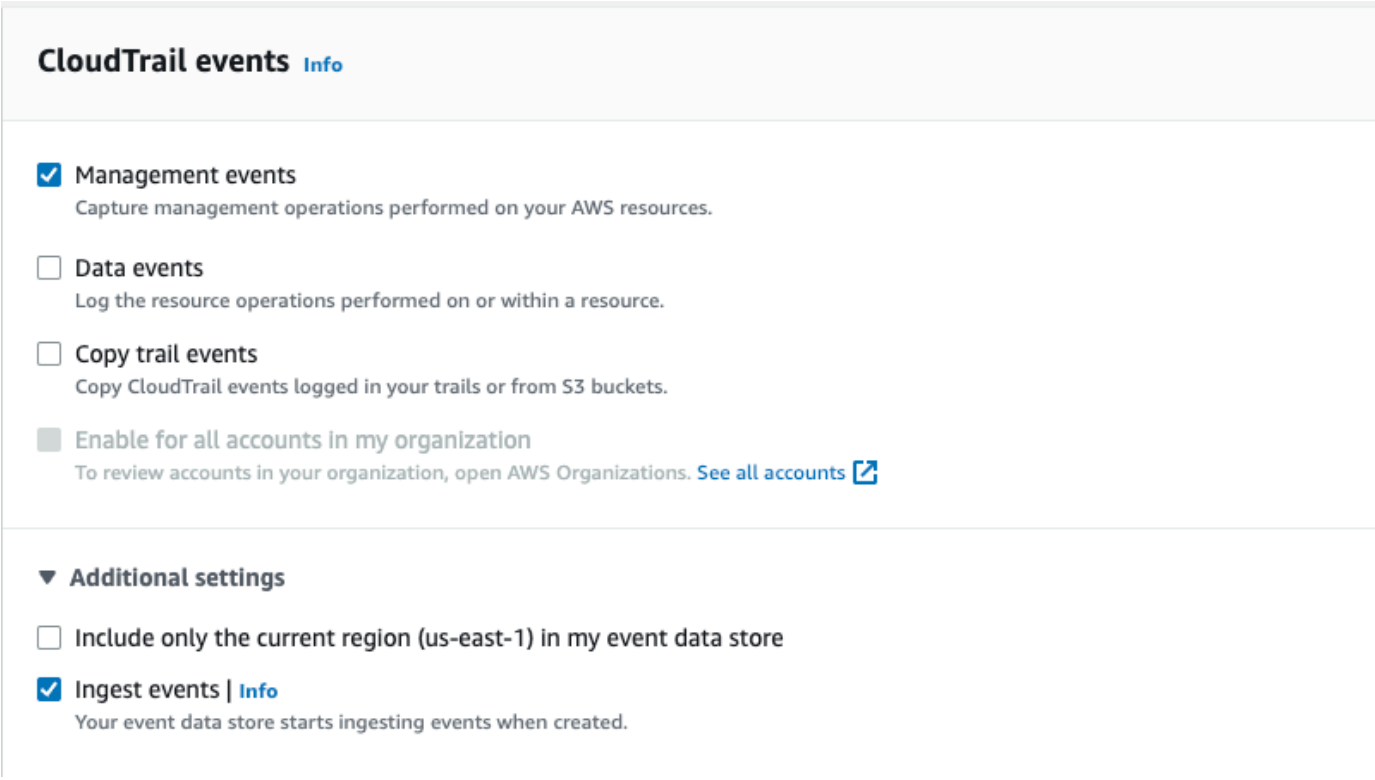
   タグを使用してコストを追跡する方法については、「 CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

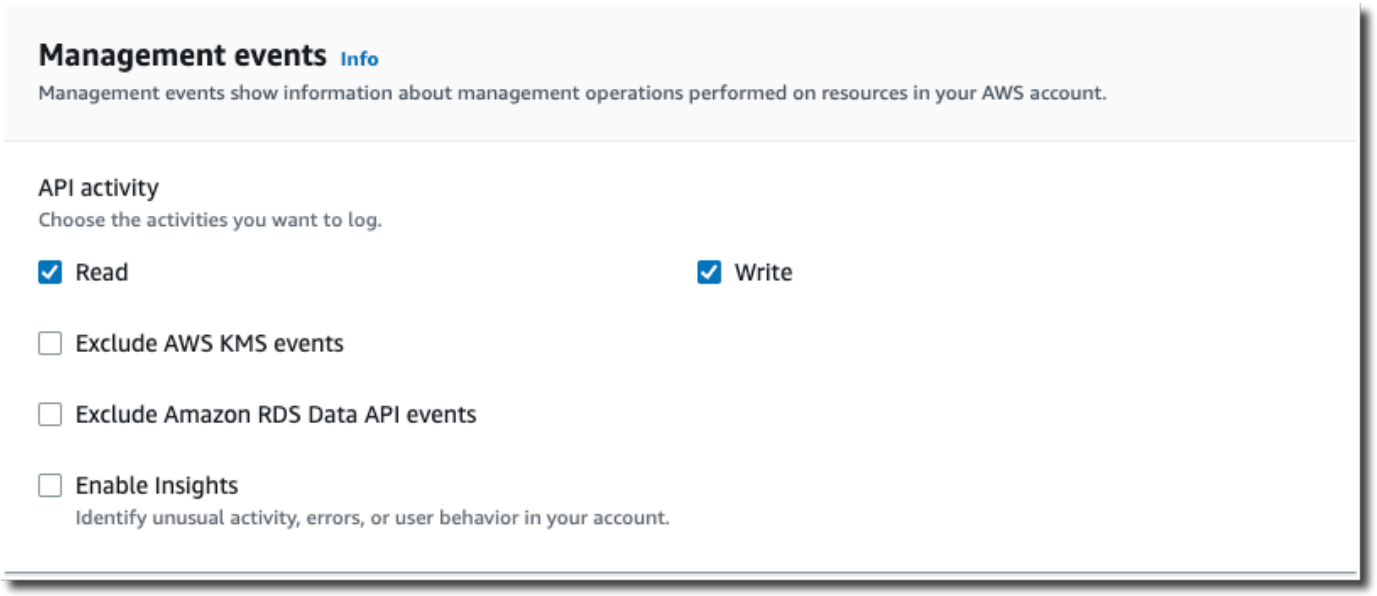
11. [イベントの選択]ページで、[イベントタイプ] はデフォルトの選択のままにします。



12. CloudTrail イベント の場合、デフォルトの選択のままにします。デフォルトでは、 CloudTrail イベントデータストアは管理イベントを収集し、データイベントは収集しません。管理イベントの詳細については、「管理イベントのログ記録」を参照してください。データイベントの詳細については、「データイベントをログ記録する」を参照してください。



13. [証跡イベントのコピー] は、デフォルト設定のままにします。このオプションを使用して、既存の証跡イベントをイベントデータストアにコピーします。詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。
14. 組織のイベントデートストアの場合は、[組織内の全アカウントで有効にする] を選択します。このオプションは、 AWS Organizations でアカウントを設定していない場合は変更できません。
15. [追加設定] は、デフォルトの選択のままにします。デフォルトでは、イベントデータストアはすべての のイベントを収集 AWS リージョン し、作成時にイベントの取り込みを開始します。
16. [管理イベント] では、[読み込み] と [書き込み] イベント両方を収集するよう選択します。すべての管理 AWS KMS イベントを収集するには、Exclude events と Exclude Amazon RDS Data API events のチェックボックスを空のままにします。[Insights イベントを有効にする] チェックボックスはオフのままにしておきます。



17. [Next] (次へ) を選択して、選択内容を確認します。
18. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。
19. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    イベントデータストアは、この時点以降の高度なイベントセレクタに一致するイベントを取得します。イベントデータストアを作成する前に発生したイベントは、既存の証跡イベントをコピーすることを選択しない限り、イベントデータストアには保存されません。

例: S3 データイベントのイベントデータストアを作成する

このチュートリアルでは、Amazon S3 データイベントのイベントデータストアを作成する方法を示します。このシナリオでは、すべての Amazon S3 データイベントをログに記録する代わりに、特定の S3 バケットからオブジェクトが削除された場合にのみイベントをログに記録するカスタムログセレクタテンプレートを選択します。

S3 データイベント用にイベントデータストアを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. 「イベントデータストアの設定」ページの全般的な詳細「」で、イベントデータストアに *s3-data-events-eds* などの名前を付けます。イベントデートストアの意図をすぐに識別できる名前を使用するのがベストプラクティスです。 CloudTrail 命名要件については、「」を参照してください命名の要件。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間

6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかを確認することで、`eventTime`イベントを保持するかどうかを決定します。例えば、保持期間を 90 日と指定すると、 `eventTime`は 90 日を経過するとイベント CloudTrail を削除します。

7. (オプション) [暗号化] で、独自の KMS キーを使用してイベントデータストアを暗号化するかどうかを選択します。デフォルトでは、イベントデータストア内のすべてのイベントは、 AWS が所有および管理する KMS キー CloudTrail を使用して暗号化されます。

   独自の KMS キーを使用して暗号化を有効にするには、[独自の AWS KMS key を使用する] を選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定しますalias/*MyAliasName*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

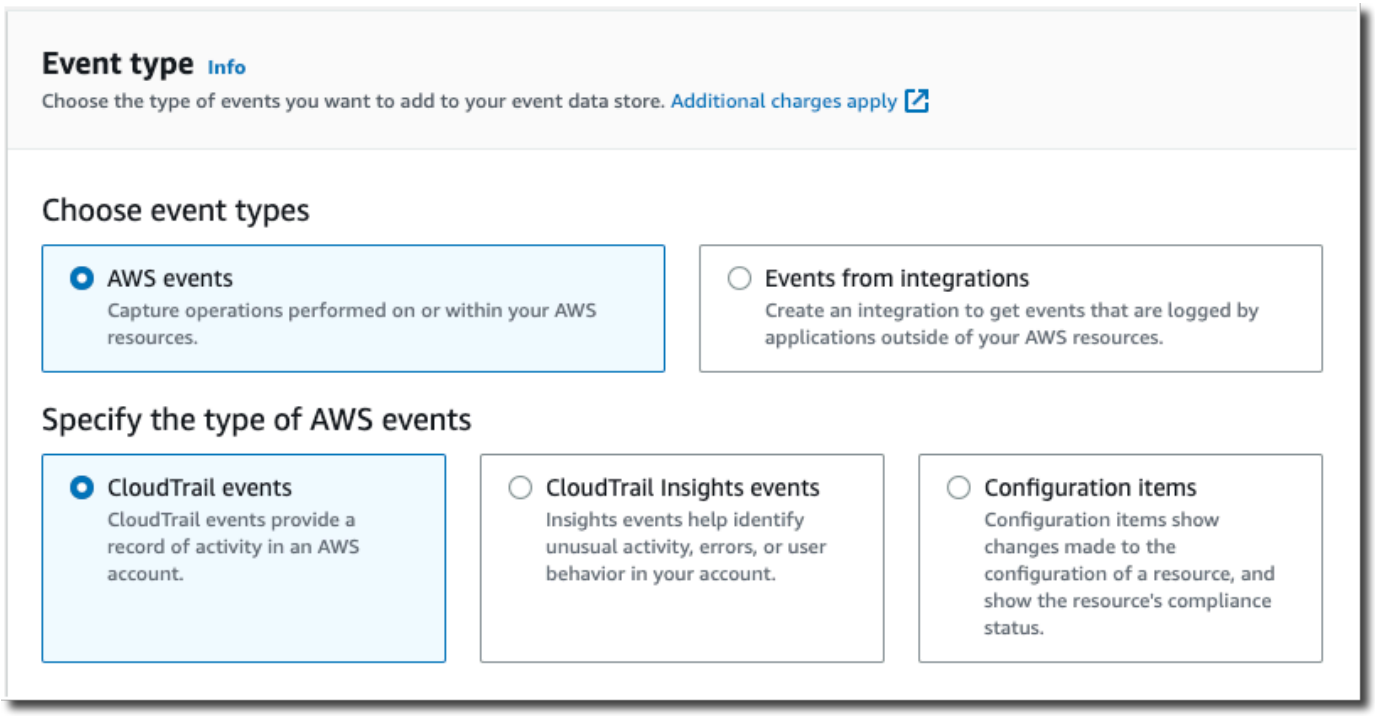
c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) をデータセットに追加します。タグは、 CloudTrail イベントデータストアを識別するのに役立ちます。例えば、**`stage`** という名前の **`prod`** という値のタグをアタッチできます。タグを使用して、イベントデータストアへのアクセスを制限できます。タグを使用して、イベントデータストアのクエリコストと取り込みコストを追跡することもできます。

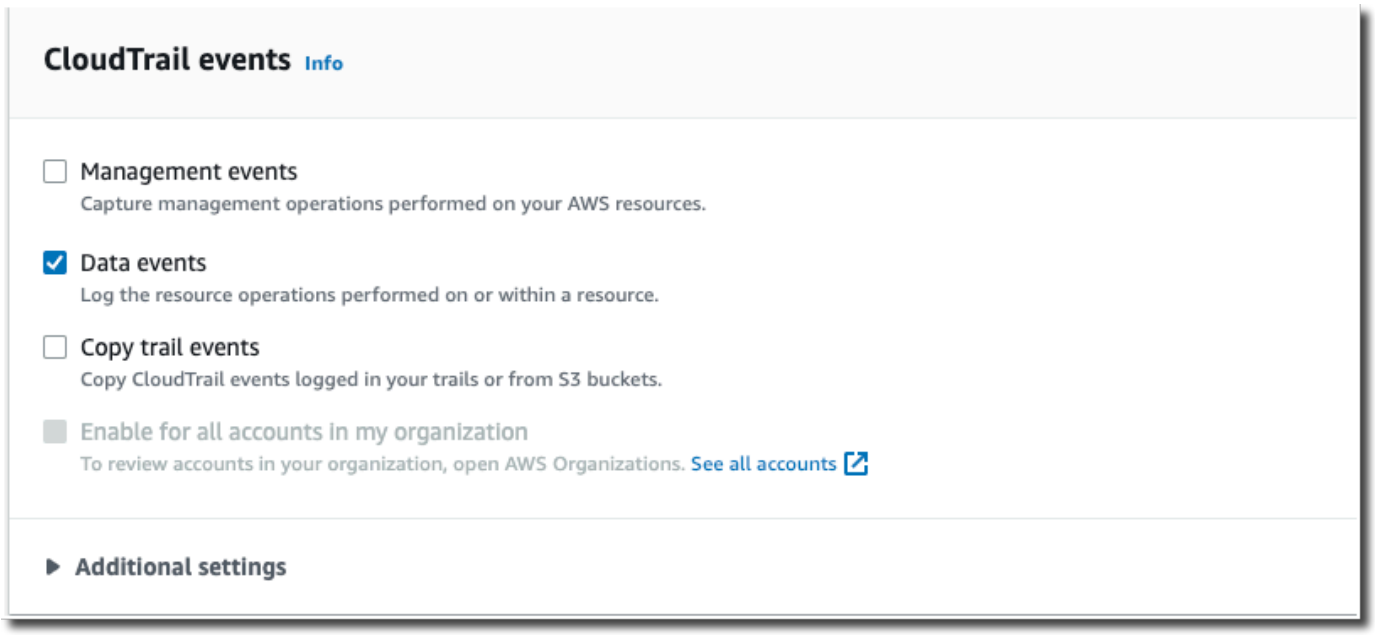
   タグを使用してコストを追跡する方法については、「CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. [イベントの選択]ページで、[イベントタイプ] はデフォルトの選択のままにします。



12. CloudTrail イベント では、データイベント を選択し、管理イベント の選択を解除します。データイベントの詳細については、「データイベントをログ記録する」を参照してください。



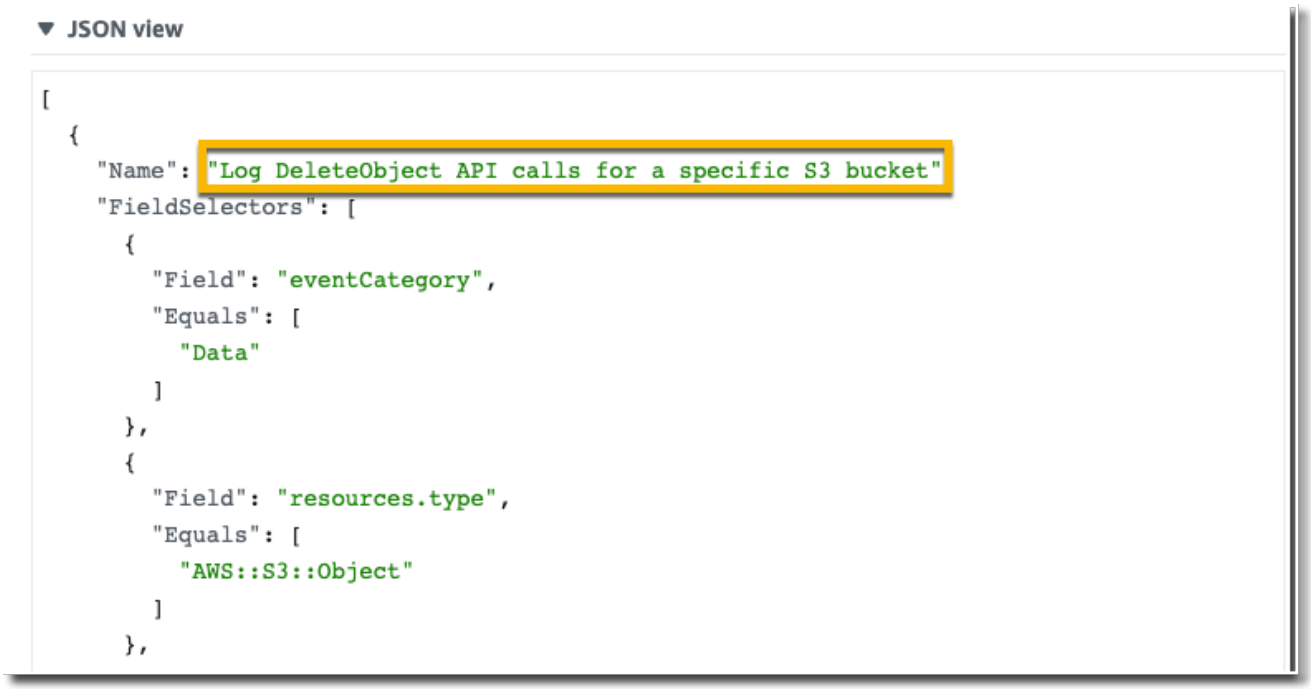
13. [証跡イベントのコピー] は、デフォルト設定のままにします。このオプションを使用して、既存の証跡イベントをイベントデータストアにコピーします。詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。
14. 組織のイベントデートストアの場合は、[組織内の全アカウントで有効にする] を選択します。このオプションは、 AWS Organizations でアカウントを設定していない場合は変更できません。

15. [追加設定] は、デフォルトの選択のままにします。デフォルトでは、イベントデータストアはすべての のイベントを収集 AWS リージョン し、作成時にイベントの取り込みを開始します。
16. [データイベント]で、次のように項目を選びます。

    a. [データイベントタイプ] に、[S3] を選択します。データイベントタイプは、データイベントがログに記録される AWS のサービス とリソースを識別します。

    b. [ログセレクターテンプレート]、で [カスタム] を選択します。[カスタム] を選択すると、eventName、resources.ARN、readOnly フィールドのフィルタリングを行うカスタムイベントセレクターを定義できます。これらのフィールドの詳細については、 AWS CloudTrail API リファレンスAdvancedFieldSelectorの「」を参照してください。

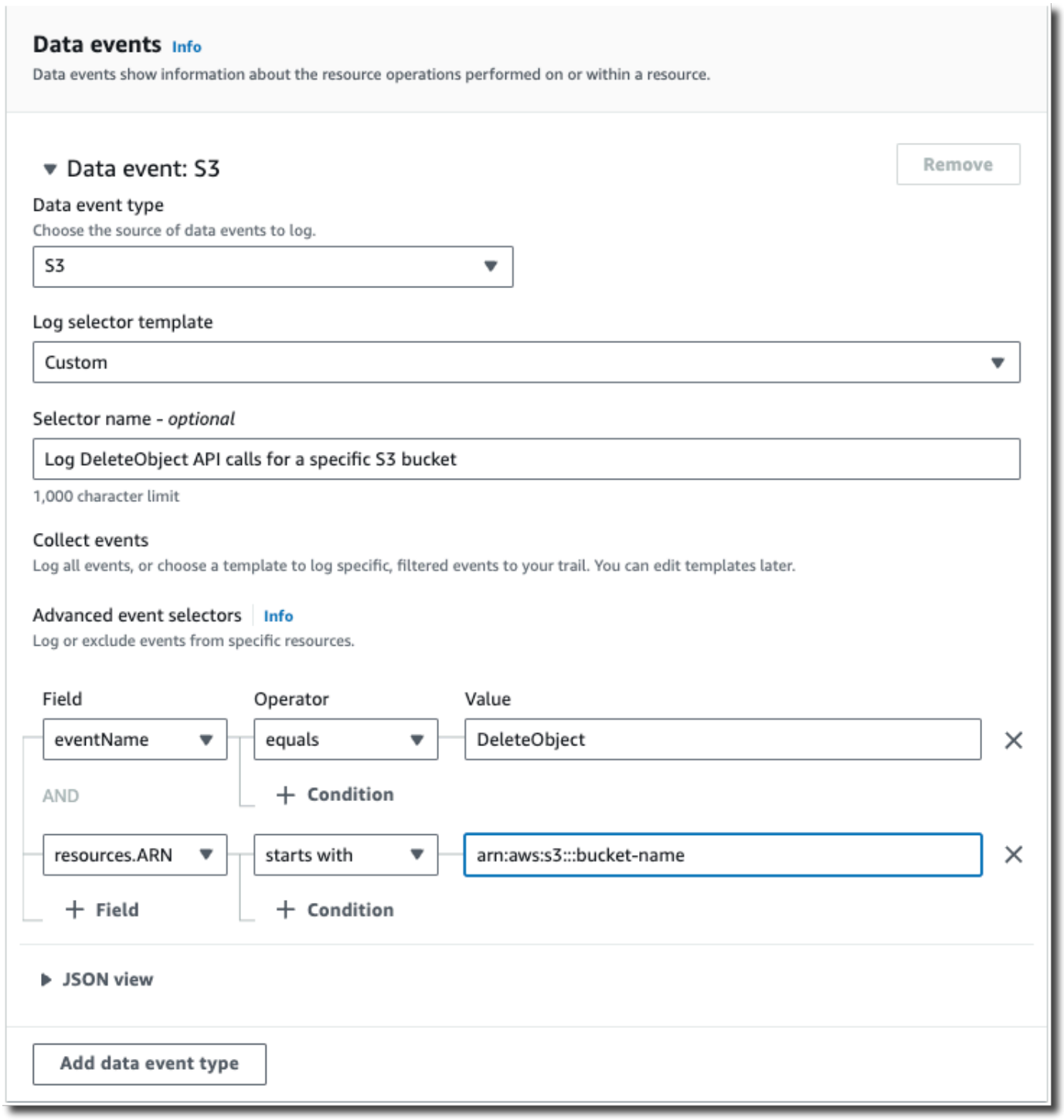
    c. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「特定の S3 バケットのログ DeleteObject API コール」など、高度なイベントセレクタのわかりやすい名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。



    d. アドバンストイベントセレクタ では、カスタムイベントセレクタを構築して、 eventName および resources.ARNフィールドでフィルタリングします。イベントデータストアの高度なイベントセレクタは、証跡に適用する高度なイベントセレクタと同じように機能します。高度なイベントセレクタを作成する方法の詳細については、「高度なイベントセレクタを使用してデータイベントを記録する」を参照してください。

i. [フィールド] に、[eventName] を選択します。[オペレーター]に、[equals] を選択します。[値] に「**`DeleteObject`**」と入力します。+ フィールドを選択して、別のフィールドでフィルタリングします。

ii. [フィールド]に、[resources.ARN] を選択します。演算子 で、 を選択しますStartsWith。[値] に、バケットの ARN を入力します (例: *`arn:aws:s3:::bucket-name`*)。ARN の取得方法については、「Amazon シンプルストレージサービスユーザーガイド」で「Amazon S3 リソース」を参照してください。



17. [Next] (次へ) を選択して、選択内容を確認します。
18. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。

19. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    イベントデータストアは、この時点以降の高度なイベントセレクタに一致するイベントを取得します。イベントデータストアを作成する前に発生したイベントは、既存の証跡イベントをコピーすることを選択しない限り、イベントデータストアには保存されません。

コンソールを使用して CloudTrail Insights イベントのイベントデータストアを作成する

AWS CloudTrail Insights は、 CloudTrail 管理イベントを継続的に分析することで、ユーザーが API コールと API エラー率に関連する異常なアクティビティ AWS を特定して応答するのに役立ちます。Insights CloudTrail は、ベースライン とも呼ばれる API コールボリュームと API エラー率の通常のパターンを分析し、コールボリュームまたはエラー率が通常のパターン外にある場合に Insights イベントを生成します。API コール量に関する Insights イベントは、`write` 管理 API に対して生成されます。一方、API エラー率に関する Insights イベントは、`read` と `write` の両方の管理 API に対して生成されます。

CloudTrail Lake で Insights イベントをログに記録するには、Insights イベントをログに記録する送信先イベントデータストアと、Insights を有効にして管理イベントをログに記録するソースイベントデータストアが必要です。

> **Note**
>
> API コールのボリュームで Insights イベントをログに記録するには、ソースイベントデータストアで `write` 管理イベントがログに記録される必要があります。API エラー率に関する Insights イベントをログに記録するには、ソースイベントデータストアで `read` または `write` の管理イベントがログに記録されている必要があります。

ソースイベントデータストアで CloudTrail Insights を有効にしていて、異常なアクティビティ CloudTrail を検出した場合、 は Insights イベントを送信先イベントデータストアに CloudTrail 配信します。イベントデータストアでキャプチャされた他のタイプの CloudTrail イベントとは異なり、Insights イベントは、 がアカウントの一般的な使用パターンと大きく異なるアカウントの API 使用量の変更 CloudTrail を検出した場合にのみログに記録されます。

イベントデータストアで CloudTrail Insights を初めて有効にすると、異常なアクティビティが検出された場合、 が最初の Insights イベントを配信 CloudTrail するまでに最大 7 日間かかることがあります。

CloudTrail Insights は、グローバルではなく単一のリージョンで発生する管理イベントを分析します。 CloudTrail Insights イベントは、サポートする管理イベントが生成されるのと同じリージョンで生成されます。

組織のイベントデータストアの場合、 は組織のすべての管理イベントの集計 CloudTrail を分析する代わりに、各メンバーのアカウントから管理イベントを分析します。

CloudTrail Lake での Insights イベントの取り込みには追加料金が適用されます。証跡と CloudTrail Lake イベントデータストアの両方で Insights を有効にすると、別途料金が発生します。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

トピック

- Insights イベントを口グに記録する送信先イベントデータストアを作成するには
- Insights イベントを有効にするソースイベントデータストアを作成するには

Insights イベントを口グに記録する送信先イベントデータストアを作成するには

Insights イベントデータストアを作成する場合、管理イベントを口グに記録する既存のソースイベントデータストアを選択し、受信する Insights タイプを指定することができます。または、Insights イベントデータストアを作成した後に、新規または既存のイベントデータストアで Insights を有効にし、そのイベントデータストアを送信先イベントデータストアとして選択することもできます。

この手順は、Insights イベントを口グに記録する送信先イベントデータストアを作成する方法を示しています。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインから [Lake] サブメニューを開き、[Event data stores] (イベントデータストア) を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [Configure event data store] (イベントデータストアの設定) ページの [General details] (全般的な詳細) で、イベントデータストアの名前を入力します。名前は必須です。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデ

フォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

以下のオプションが利用できます。

- [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
  - デフォルトの保持期間: 366 日間
  - 最長保持期間: 3,653 日間
- [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
  - デフォルトの保持期間: 2,557 日間
  - 最長保持期間: 2,557 日間

6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。イベントデータストアは指定された日数分、イベントデータを保存します。
7. (オプション) を使用して暗号化を有効にするには AWS Key Management Service、自分の を使用する AWS KMS keyを選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定しますalias/*MyAliasName*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

> **Note**
>
> 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue Data Catalog に保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

   b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

   c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [Tag] (タグ) セクションでは、イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法の詳細については AWS、「 AWS リソースのタグ付けユーザーガイド」の AWS 「 リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. 「イベントの選択」ページでAWS 「イベント」を選択し、CloudTrail「インサイトイベント」を選択します。

12. CloudTrail Insights イベント で、次の操作を行います。

a. 組織の委任された管理者にこのイベントデータストアへのアクセス権を付与する場合は、[委任された管理者アクセスを許可] を選択します。このオプションは、 AWS Organizations 組織の管理アカウントでサインインしている場合にのみ使用できます。

b. (オプション) 管理イベントをログに記録する既存のソースイベントデータストアを選択し、受信したい Insights タイプを指定します。

   ソースイベントデータストアを追加するには、次の手順を実行します。

   i. [ソースイベントデータストアを追加] を選択します。

   ii. ソースイベントデータストアを選択します。

   iii. 受信したい [Insights タイプ] を選択します。

   - `ApiCallRateInsight` – Insight タイプ `ApiCallRateInsight` は、ベースライン API コール量に対して 1 分ごとに集計された書き込み専用の管理 API コールを分析します。`ApiCallRateInsight` で Insights を受信するには、ソースイベントデータストアが [書き込み] 管理イベントをログに記録する必要があります。
   - `ApiErrorRateInsight` – Insight タイプ `ApiErrorRateInsight` は、エラーコードを発生させた管理 API コールを分析します。API 呼び出しに失敗すると、エラーが表示されます。`ApiErrorRateInsight` で Insights を受信するには、ソースイベントデータストアが [書き込み] または [読み取り] の管理イベントをログに記録する必要があります。

   iv. 受信したい Insights タイプを追加するには、前の 2 つのステップ (ii と iii) を繰り返します。

13. [Next] (次へ) を選択して、選択内容を確認します。

14. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。

15. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

16. ステップ 10 でソースイベントデータストアを選択しなかった場合は、Insights イベントを有効にするソースイベントデータストアを作成するには の手順に従ってソースイベントデータストアを作成します。

Insights イベントを有効にするソースイベントデータストアを作成するには

この手順は、Insights イベントを有効にするソースイベントデータストアを作成して管理イベントをログに記録する方法を示しています。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインから [Lake] サブメニューを開き、[Event data stores] (イベントデータストア) を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [Configure event data store] (イベントデータストアの設定) ページの [General details] (全般的な詳細) で、イベントデータストアの名前を入力します。名前は必須です。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかをチェックして、`eventTime`イベントを保持するかどうかを決定します。例えば、90 日間の保持期間を指定すると、 `eventTime`は 90 日を経過するとイベント CloudTrail を削除します。

7. (オプション) を使用して暗号化を有効にするには AWS Key Management Service、自分の を使用する AWS KMS keyを選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定します`alias/`*`MyAliasName`*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue Data Catalog に保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場

合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [Tag] (タグ) セクションでは、イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法の詳細については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

10. [次へ] を選択して、イベントデータストアを設定します。

11. 「イベントの選択」ページでAWS 「イベント」を選択し、CloudTrail「イベント」を選択します。

12. CloudTrail イベント では、管理イベントを選択したままにします。

13. イベントデータストアが AWS Organizations 内のすべてのアカウントからのイベントを収集するようにするには、[Enable for all accounts in my organization] (組織内のすべてのアカウントについて有効化) を選択します。Insights を有効にするイベントデータストアを作成するには、その組織の管理アカウントにサインインする必要があります。

14. 追加設定を展開して、イベントデータストアですべての のイベントを収集するか AWS リージョン、現在の のみのイベントを収集するかを選択し AWS リージョン、イベントデータストアでイベントを取り込むかを選択します。デフォルトでは、イベントデータストアは、アカウントのすべてのリージョンからイベントを収集し、データストアの作成時にイベントの取り込みを開始します。

a. 現在のリージョンでログに記録されたイベントのみを含める場合は、[イベントデータストアに現在のリージョンのみを含める] を選択します。このオプションを選択しない場合、イベントデータストアにはすべてのリージョンからのイベントが含まれます。

b. [イベントを取り込む] は選択したままにします。

15. イベントデータストアに保存する管理イベントのタイプを選択します。[読み取り]、[書き込み] のいずれか、または両方を選択できます。少なくとも 1 つが必要です。

> **Note**
>
> API コール量に関する Insights イベントをログに記録するには、イベントデータストアが `write` 管理イベントをログに記録している必要があります。API エラー率に関する Insights イベントをログに記録するには、イベントデータストアで `read` または `write` の管理イベントがログに記録されている必要があります。

16. イベントデータストアから AWS Key Management Service または Amazon RDS Data API イベントを除外することを選択できます。これらのパラメータの詳細については、「管理イベントのログ記録」を参照してください。
17. [Insights を有効にする] を選択します。
18. [Insights を有効にする] で、Insights イベントをログに記録する送信先イベントストアを選択します。送信先イベントデータストアは、このイベントデータストア内の管理イベントアクティビティに基づいて Insights イベントを収集します。送信先イベントデータストアの作成方法については、「Insights イベントをログに記録する送信先イベントデータストアを作成するには」を参照してください。
19. Insights タイプを選択します。[API コールレート]、[API エラー率] のいずれかまたは両方を選択できます。[API コール率] の Insights イベントをログに記録するには、[Write] 管理イベントをログ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、[Read] または [Write] 管理イベントをログ記録している必要があります。
20. [Next] (次へ) を選択して、選択内容を確認します。
21. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。
22. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    イベントデータストアは、この時点以降の高度なイベントセレクタに一致するイベントを取得します。ソースイベントデータストアで CloudTrail Insights を初めて有効にすると、異常なアクティビティが検出された場合、 が最初の Insights イベントを送信先イベントデータストアに配信 CloudTrail するまでに最大 7 日間かかることがあります。

    CloudTrail Lake ダッシュボードを表示して、送信先イベントデータストアの Insights イベントを視覚化できます。Lake ダッシュボードの詳細については、「CloudTrail Lake ダッシュボードを表示する」を参照してください。

CloudTrail Lake での Insights イベントの取り込みには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。 CloudTrail 料金の詳細については、「 AWS CloudTrail の料金」を参照してください。

コンソールを使用して設定項目のイベントデータストア AWS Config を作成する

AWS Config 設定項目を含めるイベントデータストアを作成し、そのイベントデータストアを使用して、本番環境に対する非準拠の変更を調査できます。イベントデータストアを使用すると、準拠していないルールが、その変更に関連付けられているユーザーおよびリソースと関連するようにできます。設定項目は、アカウントに存在するサポートされている AWS リソースの属性の point-in-time ビューを表します。 は、記録するリソースタイプへの変更を検出するたびに設定項目 AWS Config を作成します。 AWS Config また、 は、設定スナップショットがキャプチャされたときに設定項目を作成します。

AWS Config と CloudTrail Lake の両方を使用して、設定項目に対してクエリを実行できます。を使用して AWS Config 、単一の AWS アカウント と の設定プロパティ、または複数のアカウントとリージョンの設定プロパティに基づいて AWS リージョン、 AWS リソースの現在の設定状態をクエリできます。これとは対照的に、 CloudTrail Lake を使用して、 CloudTrail イベント、設定項目、ルール評価など、さまざまなデータソース間でクエリを実行できます。 CloudTrail Lake クエリは、リソース AWS Config 設定やコンプライアンス履歴を含むすべての設定項目をカバーします。

設定項目のイベントデータストアを作成しても、既存の AWS Config 高度なクエリや設定済みの AWS Config アグリゲータには影響しません。を使用して高度なクエリを引き続き実行し AWS Config、履歴ファイルを S3 バケットに配信 AWS Config し続けることができます。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail の料金とコスト管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

制限事項

設定項目のイベントデータストアには、次の制限が適用されます。

- カスタム設定項目のためのサポートはありません
- 高度なイベントセレクタを使用したイベントフィルタリングのためのサポートはありません

前提条件

イベントデータストアを作成する前に、すべてのアカウントとリージョン AWS Config の記録を設定します。の一機能である高速セットアップ を使用すると、 を使用する設定レコーダー AWS Systems Managerをすばやく作成できます AWS Config。

> **Note**
>
> が設定の記録 AWS Config を開始すると、サービス使用料が課金されます。料金の詳細については、「AWS Config 料金表」を参照してください。設定レコーダーの管理については、「AWS Config デベロッパーガイド]の「設定レコーダーの管理」を参照してください。

また、次のアクションも推奨されますが、イベントデータストアの作成には必須ではありません。

- 設定スナップショット (リクエストした場合) と設定履歴を受け取るように Amazon S3 バケットを設定する。スナップショットの詳細については、「AWS Config デベロッパーガイド」の「配信チャネルの管理」と「Amazon S3 バケットへの設定スナップショットの配信」を参照してください。
- 記録されたリソースタイプのコンプライアンス情報を評価 AWS Config するために使用するルールを指定します。の CloudTrail Lake サンプルクエリのいくつかでは AWS Config ルール 、 が AWS リソースのコンプライアンス状態を評価する AWS Config 必要があります。の詳細については AWS Config ルール、「 AWS Config デベロッパーガイド」の「 によるリソースの評価 AWS Config ルール」を参照してください。

設定項目用に一意のイベントデータストアを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [Configure event data store] (イベントデータストアの設定) ページの [General details] (全般的な詳細) で、イベントデータストアの名前を入力します。名前は必須です。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

以下のオプションが利用できます。

- [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
  - デフォルトの保持期間: 366 日間
  - 最長保持期間: 3,653 日間
- [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
  - デフォルトの保持期間: 2,557 日間
  - 最長保持期間: 2,557 日間

6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかをチェックして、`eventTime`イベントを保持するかどうかを決定します。例えば、90 日間の保持期間を指定すると、 `eventTime`は 90 日を経過するとイベント CloudTrail を削除します。

7. (オプション) を使用して暗号化を有効にするには AWS Key Management Service、自分の を使用する AWS KMS keyを選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定しますalias/*MyAliasName*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

> **Note**
>
> 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue Data Catalog に保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

   b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

   c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [Tag] (タグ) セクションでは、イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法の詳細については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

10. [次へ] をクリックします。

11. [イベントの選択] ページで、[AWS イベント] を選択し、次に [設定項目] を選択します。

12. CloudTrail は、イベントデータストアリソースを作成したリージョンに保存しますが、デフォルトでは、データストアで収集された設定項目は、記録が有効になっているアカウント内のすべて

のリージョンからのものです。必要に応じて、[Include only the current region in my event data store] (現在のリージョンのみをイベントデータストアに含める) を選択して、現在のリージョンでキャプチャされた設定項目のみを含めることができます。このオプションを選択しない場合、イベントデータストアには、記録が有効になっているすべてのリージョンからの設定項目が含まれます。

13. イベントデータストアが AWS Organizations 組織内のすべてのアカウントから設定項目を収集できるようにするには、組織内のすべてのアカウントに対して を有効にする を選択します。組織の設定項目を収集するイベントデータストアを作成するには、組織の管理アカウントまたは委任された管理者アカウントにサインインする必要があります。
14. [Next] (次へ) を選択して、選択内容を確認します。
15. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。
16. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

    この時点以降、イベントデータストアは設定項目を取得します。イベントデータストアを作成する前に発生した設定項目は、イベントデータストア内にありません。

サンプルクエリ

これで、新しいイベントデータストアに対してクエリを実行できるようになりました。 CloudTrail コンソールのサンプルクエリタブには、使用を開始するためのサンプルクエリが表示されます。設定項目のイベントデータストアに対して実行できるいくつかのサンプルクエリを次に示します。

説明	Query
設定項目のイベントデータストアをイベントデータストアに結合して、非準拠ステータスになったアクションを実行したユーザー CloudTrail を検索します。	`SELECT element_at(config1.eventData.configuration, 'targetResourceId') as targetResourceId, element_at(config1.eventData.configuration, 'complianceType') as complianceType, config2.eventData.resourceType, cloudtrail.userIdentity FROM`

説明	Query
	config_event_data_store_ID as config1 JOIN *config_event_data_store_ID* as config2 on element_at(config1.eventData.configuration, 'targetResourceId') = config2.eventData.resourceId JOIN *cloudtrail_event_data_store_ID* as cloudtrail on config2.eventData.arn = element_at(cloudtrail.resources, 1).arn WHERE element_at(config1.eventData.configuration, 'configRuleList') is not null AND element_at(config1.eventData.configuration, 'complianceType') = 'NON_COMPLIANT' AND cloudtrail.eventTime > '2022-11-14 00:00:00' AND config2.eventData.resourceType = 'AWS::DynamoDB::Table'

説明	Query

すべての AWS Config ルールを検索し、過去 1 日以内に生成された設定項目からコンプライアンス状態を返します。	SELECT
	    eventData.configuration,
	 eventData.accountId, eventData
	.awsRegion,
	    eventData.resourceName, eventData
	.resourceCreationTime,
	    element_at(eventData.config
	uration,'complianceType') AS
	 complianceType,
	    element_at(eventData.config
	uration, 'configRuleList') AS
	 configRuleList,
	    element_at(eventData.config
	uration, 'resourceId') AS resourceI
	d,
	    element_at(eventData.config
	uration, 'resourceType') AS resourceT
	ype
	FROM
	    config_event_data_store_ID
	WHERE
	    eventData.resourceType =
	 'AWS::Config::ResourceCompliance'
	AND
	    eventTime > '2022-11-22 00:00:00'
	ORDER BY
	    eventData.resourceCreationTime
	DESC
	    limit 10

説明	Query

AWS Config リソースタイプ、アカウント ID、リージョン別にグループ化されたリソースの合計数を検索します。	`SELECT`
	`    eventData.resourceType, eventData`
	`.awsRegion, eventData.accountId,`
	`COUNT (*) AS resourceCount`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-22 00:00:00'`
	`GROUP BY`
	`    eventData.resourceType, eventData`
	`.awsRegion, eventData.accountId`

特定の日付に生成されたすべての AWS Config 設定項目のリソース作成時刻を検索します。	`SELECT`
	`    eventData.configuration,`
	` eventData.accountId,`
	`    eventData.awsRegion, eventData`
	`.resourceId,`
	`    eventData.resourceName, eventData`
	`.resourceType,`
	`    eventData.availabilityZone,`
	` eventData.resourceCreationTime`
	`FROM`
	`    config_event_data_store_ID`
	`WHERE`
	`    eventTime > '2022-11-16 00:00:00'`
	`AND`
	`    eventTime < '2022-11-17 00:00:00'`
	
	`ORDER BY`
	`    eventData.resourceCreationTime`
	`DESC`
	`    limit 10;`

クエリの作成と編集の詳細については、「クエリを作成または編集する」を参照してください。

設定項目のスキーマ

次の表は、設定項目レコードのスキーマ要素と一致する必須およびオプションのスキーマ要素を示しています。の内容eventDataは設定項目によって提供され、他のフィールドは取り込み CloudTrail 後に によって提供されます。

CloudTrail イベントレコードの内容の詳細については、「」を参照してくださいCloudTrail レコードの内容。

- 取り込み CloudTrail 後に によって提供されるフィールド
- イベントによって提供されるフィールド

取り込み CloudTrail 後に によって提供されるフィールド

フィールド名	入力タイプ	要件	説明
eventVersion	string	必須	AWS イベント形式のバージョン。
eventCategory	string	必須	イベントカテゴリ。設定項目では、有効な値は ConfigurationItem です。
eventType	string	必須	イベントタイプです。設定項目では、有効な値は AwsConfigurationItem です。
eventID	string	必須	イベントの一意の ID。
eventTime	string	必須	イベントタイムスタンプ (yyyy-MM-DDTHH:mm:ss 形式、協定世界時 (UTC))。

フィールド名	入力タイプ	要件	説明
awsRegion	string	必須	イベントを割り当てる AWS リージョン先の 。
recipientAccountId	string	必須	このイベントを受信した AWS アカウント ID を表します。
addendum	補遺	オプションです。	イベントが遅延した理由に関する情報が表示されます。既存のイベントから情報が欠落している場合、補遺ブロックには、不足している情報と、不足している理由が表示されます。

`eventData` のフィールドは、設定項目によって提供されます

フィールド名	入力タイプ	要件	説明
eventData	-	必須	eventData のフィールドは、設定項目によって提供されます。
• configurationItemVersion	string	オプションです。	ソースからの設定項目のバージョン。
• configurationItemCapture時間	string	オプションです。	設定の記録が開始された時刻。
• configurationItemStatus	string	オプションです。	設定項目のステータス。有効な値

フィールド名	入力タイプ	要件	説明
			は、OK、ResourceDiscovered 、ResourceNotRecorded 、 ResourceDeleted 、ResourceDeletedNotRecorded です。
• accountId	string	オプションです。	リソースに関連付けられている 12 桁の AWS アカウント ID。
• resourceType	string	オプションです。	AWS リソースのタイプ。有効なリソースタイプの詳細については、 AWS Config API リファレンスConfigurationItemの「」を参照してください。
• resourceId	string	オプションです。	リソースの ID (例: sg-*xxxxxx*)。
• resourceName	string	オプションです。	リソースのカスタム名 (使用可能な場合)。
• arn	string	オプションです。	リソースに関連付けられた Amazon リソースネーム (ARN)。
• awsRegion	string	オプションです。	AWS リージョン リソースが存在する 。

フィールド名	入力タイプ	要件	説明
• availabilityZone	string	オプションです。	リソースに関連付けられたアベイラビリティーゾーン。
• resourceCreationTime	string	オプションです。	リソースが作成されたときのタイムスタンプ。
• 設定	JSON	オプションです。	リソースの設定の説明。
• supplementaryConfiguration	JSON	オプションです。	特定のリソースタイプに対して が AWS Config 返す設定属性は、設定パラメータに対して返される情報を補足します。
• relatedEvents	string	オプションです。	CloudTrail イベント IDsのリスト。
• 関係	-	オプションです。	関連 AWS リソースのリスト。
• • name	string	オプションです。	関連リソースとの関係のタイプ。
• • resourceType	string	オプションです。	関連リソースのリソースタイプ。
• • resourceId	string	オプションです。	関連するリソースの ID (例: sg-*xxxxxx*)。
• • resourceName	string	オプションです。	関連リソースのカスタム名 (使用可能な場合)。

フィールド名	入力タイプ	要件	説明
• タグ	JSON	オプションです。	リソースに関連付けられているキーバリュータグのマッピング。

次の例は、設定項目レコードのスキーマ要素の階層に一致する、スキーマ要素の階層を示しています。

```
{
  "eventVersion": String,
  "eventCategory: String,
  "eventType": String,
  "eventID": String,
  "eventTime": String,
  "awsRegion": String,
  "recipientAccountId": String,
  "addendum": Addendum,
  "eventData": {
      "configurationItemVersion": String,
      "configurationItemCaptureTime": String,
      "configurationItemStatus": String,
      "configurationStateId": String,
      "accountId": String,
      "resourceType": String,
      "resourceId": String,
      "resourceName": String,
      "arn": String,
      "awsRegion": String,
      "availabilityZone": String,
      "resourceCreationTime": String,
      "configuration": {
        JSON,
      },
      "supplementaryConfiguration": {
        JSON,
      },
      "relatedEvents": [
        String
      ],
```

```
      "relationships": [
        struct{
          "name" : String,
          "resourceType": String,
          "resourceId": String,
          "resourceName": String
        }
      ],
     "tags": {
       JSON
     }
    }
  }
}
```

コンソール AWS を使用して、 の外部でイベントのイベントデータストアを作成する

イベントデータストアを作成して の外部にイベントを含め AWS、 CloudTrail Lake を使用してアプリケーションからログに記録されたデータを検索、クエリ、分析できます。

CloudTrail Lake 統合を使用して、 の外部からのユーザーアクティビティデータを口グに記録して保存できます AWS。オンプレミスまたはクラウドでホストされている社内アプリケーションや SaaS アプリケーション、仮想マシン、コンテナなど、ハイブリッド環境の任意のソースからのユーザーアクティビティデータです。

統合用としてイベントデータストアを作成する際は、同時にチャネルも作成し、そのチャネルにリソースポリシーをアタッチします。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail の料金とコスト管理の詳細については、AWS CloudTrail 「 の料金」および「」を参照してください CloudTrail Lake コストの管理。

の外部でイベントのイベントデータストアを作成するには AWS

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Create event data store] (イベントデータストアの作成) をクリックします。

4. [Configure event data store] (イベントデータストアの設定) ページの [General details] (全般的な詳細) で、イベントデータストアの名前を入力します。名前は必須です。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、延長保持は pay-as-you-go 料金で利用できます。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントの が指定された保持期間内であるかどうかを確認することで、`eventTime`イベントを保持するかどうかを決定します。例えば、保持期間を 90 日と指定すると、 `eventTime`は 90 日を経過するとイベント CloudTrail を削除します。
7. (オプション) を使用して暗号化を有効にするには AWS Key Management Service、自分の を使用する AWS KMS keyを選択します。新規 を選択して AWS KMS key を作成するか、既存 を選択して既存の KMS キーを使用します。「KMS エイリアスを入力」で、 形式でエイリアスを指定します`alias/`*`MyAliasName`*。独自の KMS キーを使用するには、KMS キーポリシーを編集して、ログの暗号化と復号を許可 CloudTrail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AWS KMS の主要ポリシーの設定 CloudTrail。 は AWS KMS マルチリージョンキー CloudTrail もサポートしています。マルチリージョンキーの詳細については、AWS Key

Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

> **Note**
>
> 組織のイベントデータストアの AWS Key Management Service 暗号化を有効にするには、管理アカウントに既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

   Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

   a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

   b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

   c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

9. (オプション) [Tag] (タグ) セクションでは、イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアク

セスの拒否」を参照してください。でタグを使用する方法の詳細については AWS、「 AWS リソースのタグ付けユーザーガイド」の「 AWS リソースのタグ付け」を参照してください。

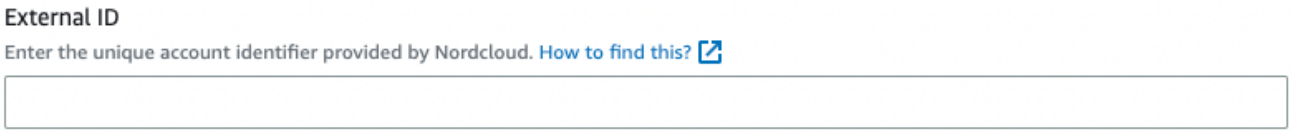
10. [次へ] を選択して、イベントデータストアを設定します。
11. [Choose events] (イベントの選択) ページで、[Events from integrations] (統合からのイベント) を選択します。
12. [Events from integration] (統合からのイベント) から、イベントデータストアにイベントを配信するソースを選択します。
13. 統合のチャネルを識別するための名前を指定します。名前には 3～128 の文字数が使用できます。使用できるのは文字、数字、ピリオド、アンダースコア、ダッシュのみです。
14. [Resource policy] (リソースポリシー) では、統合のチャネル用にリソースポリシーを設定します。リソースポリシーとは、JSON によるポリシードキュメントです。このドキュメントでは、指定したプリンシパルが対象のリソースにおいて実行できるアクションの種類と、その際の条件を指定します。リソースポリシーでプリンシパルとして定義されているアカウントは、`PutAuditEvents` API を呼び出してイベントをチャネルに配信することができます。IAM ポリシーで `cloudtrail-data:PutAuditEvents` アクションが許可されている場合、リソース所有者はリソースに暗黙的にアクセスできます。

    ポリシーに必要な情報は、統合タイプによって決まります。方向統合の場合、 はパートナーの AWS アカウント ID CloudTrail を自動的に追加し、パートナーから提供された一意の外部 ID を入力する必要があります。 IDs ソリューション統合では、少なくとも 1 つの AWS アカウント ID をプリンシパルとして指定する必要があります。また、必要に応じて外部 ID を入力して、混乱した代理を防ぐことができます。

    > **Note**
    >
    > チャネルのリソースポリシーを作成しない場合は、そのチャネルの所有者だけが、チャネル内で `PutAuditEvents` API を呼び出すことができます。

    a. 直接統合の場合には、パートナーから提供された外部 ID を入力します。統合パートナーは、一意の外部 ID (アカウント ID やランダムに生成された文字列など) を統合のために提供し、混乱した代理問題を防ぎます。パートナーが一意の外部 ID の作成と提供を責任もって行います。

        [How to find this?] (これを見つけるには?) を選択すると、外部 ID を検索する方法が記載された、パートナー提供のドキュメントを表示できます。



> **Note**
>
> リソースポリシーに外部 ID が含まれているのであれば、`PutAuditEvents` API に対するすべての呼び出しに、この外部 ID を含める必要があります。ただし、ポリシーで外部 ID が定義されていない場合でも、パートナーは、`PutAuditEvents` API を呼び出して `externalId` パラメータを指定することができます。

b. ソリューション統合の場合は、アカウントの追加 AWS を選択して、ポリシーでプリンシパルとして追加する各 AWS アカウント ID を指定します。

15. [Next] (次へ) を選択して、選択内容を確認します。
16. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。
17. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。
18. パートナーアプリケーションに対し、チャネルの Amazon リソースネーム (ARN) を指定します。チャネル ARN をパートナーアプリケーションに対し指定するための手順は、パートナードキュメントのウェブサイトで確認できます。詳細を参照するには、[Integrations] (統合) ページの [Available sources] (利用可能なソース) タブで、パートナーの [Learn more] (詳細はこちら) リンクを選択し AWS Marketplace内のパートナーページを開きます。

イベントデータストアは、ユーザー、パートナー、またはパートナーアプリケーションがチャネルで `PutAuditEvents` API を呼び出すと、統合のチャネル CloudTrail を介して へのパートナーイベントの取り込みを開始します。

コンソールでイベントデータストアを更新する

このセクションでは、 AWS Management Consoleを使用してイベントデータストアの設定を更新する方法について説明します。を使用してイベントデータストアを更新する方法については、 AWS CLI「」を参照してくださいイベントデータストアを次のように更新します。 AWS CLI。

イベントデータストアを更新するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. 更新するイベントデータストアを選択します。このアクションで、イベントデータストアの詳細ページが開きます。
4. [全般的な詳細] で、[編集] を選択して次の設定を変更します。

   - [イベントデータストア名] - イベントデータストアを識別する名前を変更します。
   - [料金オプション] - [7 年間の保持料金] オプションを使用しているイベントデータストアの場合は、代わりに [延長可能な 1 年間の保持料金] を使用するように選択できます。1 か月あたり取り込むイベントデータが 25 TB 未満のイベントデータストアには、延長可能な 1 年間の保持料金をお勧めします。また、最大 10 年の柔軟な保持期間をお求めの場合にも、延長可能な 1 年間の保持料金をお勧めします。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

     > **Note**
     >
     > [延長可能な 1 年間の保持料金] を使用するイベントデータストアの料金オプションは変更できません。[7 年間の保持料金] を使用したい場合は、現在のイベントデータストアへの取り込みを停止します。次に、[7 年間の保持料金] オプションで新しいイベントデータストアを作成します。

   - [保持期間] - イベントデータストアの保持期間を変更します。保持期間によって、イベントデータをイベントデータストアに保持する期間が決まります。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

     > **Note**
     >
     > イベントデータストアの保持期間を短くすると、 CloudTrail は新しい保持期間よりeventTime古い を持つイベントをすべて削除します。例えば、以前の保持期間が 365 日で、それを 100 日に減らすと、 CloudTrail は 100 日よりもeventTime古い のイベントを削除します。

- [暗号化] - 自分の KMS キーを使用してイベントデータストアを暗号化するには、[自分の AWS KMS keyを使用] を選択します。デフォルトでは、イベントデータストア内のすべてのイベントは によって暗号化されます CloudTrail。独自の KMS キーを使用すると、暗号化と復号化の AWS KMS コストが発生します。

  > **Note**
  >
  > イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

- 現在の AWS リージョンで ログに記録されたイベントのみを含めるには、[イベントデータストアに現在のリージョンのみを含める] を選択します。このオプションを選択しない場合、イベントデータストアにはすべてのリージョンからのイベントが含まれます。
- イベントデータストアが AWS Organizations 組織内のすべてのアカウントからイベントを収集できるようにするには、組織内のすべてのアカウントに対して有効にする を選択します。このオプションは、組織の管理アカウントでサインインしていて、イベントデータストアのイベントタイプがCloudTrailイベントまたは設定項目 である場合にのみ使用できます。

完了したら、[変更の保存] を選択します。

5. [Lake クエリフェデレーション] では、[編集] を選択して Lake クエリフェデレーションを有効または無効にします。Lake クエリフェデレーションを有効にすると、 AWS Glue Data Catalog 内のイベントデータストアのメタデータを表示し、Amazon Athena を使用してイベントデータに対して SQL クエリを実行できます。Lake クエリフェデレーションを無効にすると AWS Glue AWS Lake Formation、、、および Amazon Athena との統合が無効になります。Lake クエリフェデレーションを無効にした後は、Athena でデータをクエリできなくなります。フェデレーションを無効にすると CloudTrail Lake データは削除されず、引き続き CloudTrail Lake でクエリを実行できます。

   フェデレーションを有効にするには、次の手順を実行します。

   a. [Enable (有効化)] を選択します。

   b. 新しい IAM ロールを作成するか、既存のロールを使用するか選択します。新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを使用する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

   c. 新しい IAM ロールを作成する場合は、ロールの名前を入力します。

d. 既存の IAM ロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

完了したら、[Save changes] (変更の保存) を選択します。

6. [イベントタイプ] のその他の設定を編集します。

イベントタイプ	編集可能な設定
CloudTrail イベント	イベントの次の設定 CloudTrailを編集できます。 • イベントデータストアログのイベントを変更するには、イベント で編集 CloudTrail を選択します。 • [管理イベント] で、[編集] を選択して、管理イベントの設定を変更します。詳細については、「による管理イベントのロギング AWS Management Console」(ステップ 3) を参照してください。 • [データイベント] で、[編集] を選択して、データイベントの設定を変更します。ログに記録するデータイベントタイプと、使用するログセレクタテンプレートを選択することができます。詳細については、「内のデータイベントをログに記録するための既存のイベントデータストアの更新 AWS Management Console」を参照してください。 完了したら、[変更の保存] を選択します。
[統合からのイベント]	[統合] で、統合を選択します。次に [編集] を選択し、次の設定を変更します。 • [統合の詳細] で、統合のチャネルを識別する名前を変更します。

イベントタイプ	編集可能な設定
	• [イベントの配信場所] で、イベントの配信先を選択します。 • [Resource policy] (リソースポリシー) では、統合のチャネル用にリソースポリシーを設定します。 完了したら、[変更の保存] を選択します。 これらの設定の詳細については、「外部のイベントソースとの統合を作成 AWS」をご参照ください。

7. タグを追加、変更、または削除するには、[タグ] で [編集] を選択します。イベントデータストアへのアクセスを特定、ソート、および制御できるようにするタグキーのペアを最大 50 個追加できます。完了したら、[変更の保存] を選択します。

コンソールでイベントの取り込みを停止および開始する

デフォルトでは、イベントデータストアはイベントを取り込むように設定されています。イベントデータストアによるイベントの取り込みを停止するには、コンソール AWS CLI、、または APIsを使用します。

取り込みの開始と停止のオプションは、イベント (管理イベントとデータイベント) または AWS Config 設定項目を含む CloudTrail イベントデータストアでのみ使用できます。

イベントデータストアで取り込みを停止すると、イベントデータストアの状態が `STOPPED_INGESTION` に変化します。引き続き、イベントデータストアにすでに存在するイベントに対してクエリを実行することは可能です。証跡イベントをイベントデータストアにコピーすることもできます (CloudTrail 管理イベントまたはデータイベントのみが含まれている場合) 。

イベントデータストアのイベント取り込みを停止するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。

4. [アクション] で [取り込みを停止] を選択します。
5. 確認を求められたら、[取り込みを停止] を選択します。イベントデータストアは、ライブイベントの取り込みを停止します。
6. 取り込みを再開するときは、[取り込みを開始] を選択します。

イベントの取り込みを再開するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。
4. [アクション] で [取り込みを開始] を選択します。

コンソールで終了保護を変更する

デフォルトでは、 AWS CloudTrail Lake のイベントデータストアは終了保護が有効に設定されています。終了保護は、イベントデータストアが誤って削除されることを防ぎます。イベントデータストアを削除する場合は、終了保護を無効にする必要があります。終了保護を無効にするには AWS Management Console、、 AWS CLI、または API オペレーションを使用します。

終了保護を無効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。
4. [アクション] で、[終了保護の変更] を選択します。
5. [無効] を選択します。
6. [保存] を選択します。これで、イベントデータストアを削除できるようになりました。

終了保護を有効にするには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。

3. イベントデータストアを選択します。
4. [アクション] で、[終了保護の変更] を選択します。
5. 終了保護を有効にするには、[有効] を選択します。
6. [保存] を選択します。

コンソールでイベントデータストアを削除する

このセクションでは、 AWS CloudTrail コンソールを使用してイベントデータストアを削除する方法について説明します。を使用してイベントデータストアを削除する方法については、 AWS CLI「」を参照してくださいを使用してイベントデータストアを削除します。 AWS CLI。

> **Note**
>
> 終了保護または Lake クエリフェデレーションが有効になっている場合、イベントデータストアは削除できません。デフォルトでは、 は終了保護 CloudTrail を有効にして、イベントデータストアが誤って削除されないようにします。
> イベントタイプが [統合からのイベント] のイベントデータストアを削除するには、まず統合のチャネルを削除する必要があります。チャネルは、統合の [詳細] ページから、または aws cloudtrail delete-channel コマンドを使用して削除できます。詳細については、「チャンネルを削除すると、とのインテグレーションが削除されます。 AWS CLI」を参照してください。

イベントデータストアを削除するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。
4. [Actions (アクション)] では、[Delete (削除)] を選択します。
5. イベントデータストアの名前を入力して、削除することを確認します。
6. [削除] を選択します。

イベントデータストアを削除すると、イベントデータストアのステータスは PENDING_DELETION に変化し、7 日間その状態が続きます。7 日間の待機期間中は、イベントデータストアを復元できます。PENDING_DELETION 状態の間、イベントデータストアをクエリに使用することはできず、復元

操作以外の操作をイベントデータストアで実行することはできません。削除保留中のイベントデータストアはイベントの取り込みを行わないため、料金は発生しません。削除保留中のイベントデータストアは、1 つの に存在する可能性のあるイベントデータストアのクォータにカウントされます AWS リージョン。

コンソールを使用してイベントデータストアを復元する

AWS CloudTrail Lake でイベントデータストアを削除するPENDING_DELETIONと、そのステータスは に変わり、7 日間その状態のままになります。この間、、、または RestoreEventDataStore API オペレーションを使用して AWS Management Console AWS CLIイベントデータストアを復元できます。

このセクションでは、コンソールを使用してイベントデータストアを復元する方法について説明します。を使用してイベントデータストアを復元する方法については、 AWS CLI「」を参照してくださいを使用してイベントデータストアを復元します。 AWS CLI。

イベントデータストアを復元するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。
4. [アクション] で、[復元] を選択します。

を使用して、イベントデータストアを作成、更新、管理します AWS CLI

を使用してイベントデータストアを作成、更新、管理できます。 AWS CLI を使用する場合 AWS CLI、 AWS リージョン コマンドはプロファイルに設定されたで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

イベントデータストアで使用できるコマンド

CloudTrail Lake でイベントデータストアを作成および更新するコマンドには以下が含まれます。

- `create-event-data-store`イベントデータストアを作成します。
- `get-event-data-store`イベントデータストアに設定された高度なイベントセレクターなど、イベントデータストアに関する情報を返します。

- update-event-data-store既存のイベントデータストアの構成を変更します。
- list-event-data-storesイベントデータストアを一覧表示します。
- delete-event-data-storeイベントデータストアを削除する。
- restore-event-data-store削除が保留になっているイベントデータストアを復元します。
- start-importイベントデータストアへのトレイルイベントのインポートを開始するか、失敗したインポートを再試行します。
- get-import特定のインポートに関する情報を返すため。
- stop-importイベントデータストアへのトレイルイベントのインポートを停止します。
- list-importsすべてのインポート、ImportStatusまたはによる一部のインポートに関する情報を返すにはDestination。
- list-import-failures指定したインポートのインポート失敗を一覧表示します。
- stop-event-data-store-ingestionイベントデータストアへのイベントの取り込みを停止します。
- start-event-data-store-ingestionイベントデータストアへのイベント取り込みを再開します。
- enable-federationイベントデータストアのフェデレーションを有効にして、Amazon Athena のイベントデータストアをクエリできるようにします。
- disable-federationイベントデータストアのフェデレーションを無効にします。フェデレーションを無効にすると、Amazon Athena のイベントデータストアのデータに対してクエリを実行できなくなります。 CloudTrail Lake では引き続きクエリを実行できます。
- put-insight-selectors既存のイベントデータストアの Insights イベントセレクターを追加または変更し、Insights イベントを有効または無効にします。
- get-insight-selectorsイベントデータストアに設定された Insights イベントセレクターに関する情報を返すため。
- add-tags既存のイベントデータストアに 1 つ以上のタグ (キーと値のペア) を追加します。
- remove-tagsイベントデータストアから 1 つ以上のタグを削除すること。
- list-tagsイベントデータストアに関連するタグのリストを返します。

CloudTrail Lake クエリで使用できるコマンドのリストについては、を参照してください CloudTrail Lake クエリで使用できるコマンド。

CloudTrail Lake インテグレーションで使用できるコマンドのリストについては、を参照してください CloudTrail Lake インテグレーションで使用できるコマンド。

を使用してイベントデータストアを作成します。 AWS CLI

create-event-data-store コマンドを使用してイベントデータストアを作成します。

イベントデータストアを作成する際の必須パラメータは --name だけです。これは、イベントデータストアを識別するために使用されます。次のようなオプションパラメータも設定できます。

- --advanced-event-selectors - イベントデータストアに含めるイベントのタイプを指定します。イベントデータストアのデフォルトでは、すべての管理イベントをログ記録します。高度なイベントセレクターの詳細については、『 CloudTrail API リファレンス』AdvancedEventSelectorのを参照してください。
- --kms-key-id-によって配信されるイベントの暗号化に使用する AWS KMS キー ID を指定します。 CloudTrail値は、エイリアス名 (プレフィックス alias/ を付けます)、エイリアスに対して完全に指定された ARN、キーに対して完全に指定された ARN、またはグローバル一意識別子を指定できます。
- --multi-region-enabled- AWS リージョン アカウント内のすべてのイベントを記録するマルチリージョンイベントデータストアを作成します。デフォルトでは、このパラメータが追加されていなくても、--multi-region-enabled が設定されています。
- --organization-enabled - イベントデータストアが組織内のすべてのアカウントについてのイベントを収集できるようにします。デフォルトでは、組織内のすべてのアカウントについてイベントデータストアが有効になっているわけではありません。
- --billing-mode - イベントの取り込みと保存にかかるコスト、および、イベントデータストアでの保持期間のデフォルトと最大を決定します。

  取り得る値には以下のものがあります。

  - EXTENDABLE_RETENTION_PRICING - この課金モードは、1 か月あたりに取り込むイベントデータが 25 TB 未満で、最大 3653 日 (約 10 年) の柔軟な保持期間を希望する場合に一般的にお勧めします。この課金モードのデフォルトの保持期間は 366 日です。
  - FIXED_RETENTION_PRICING - この課金モードは 1 か月あたりに取り込むイベントデータが 25 TB を超えると予想され、必要な保持期間が最長 2557 日 (約 7 年) の場合にお勧めします。この課金モードのデフォルトの保持期間は 2557 日です。

  デフォルト値は、EXTENDABLE_RETENTION_PRICINGです。
- --retention-period - イベントデータストアにイベントを保持する日数。有効な値は、--billing-mode が EXTENDABLE_RETENTION_PRICING の場合は 7 から 3653 までの整数で、--billing-mode が FIXED_RETENTION_PRICING に設定されている場合は 7 から 2557 までの整

数です。指定しない場合--retention-period、 CloudTrail のデフォルトの保持期間が使用されます。--billing-mode

- --start-ingestion - --start-ingestion パラメータを指定すると、イベントデータストアが作成されたときにイベントデータストアでのイベントの取り込みが開始されます。このパラメータは、パラメータが追加されなくても設定されます。

  イベントデータストアにライブイベントを取り込みたくない場合は --no-start-ingestion を指定します。例えば、イベントをイベントデータストアにコピーして、過去のイベントの分析にのみイベントデータを使用する予定があるときは、このパラメータを設定するとよいでしょう。--no-start-ingestion パラメータは、eventCategory が Management、Data、または ConfigurationItem である場合にのみ有効です。

次の例では、さまざまなタイプのイベントデータストアを作成する方法を示します。

トピック

- を使用して S3 データイベントのイベントデータストアを作成します。 AWS CLI
- AWS Config を使用して設定項目用のイベントデータストアを作成します。 AWS CLI
- を使用して、管理イベント用の組織イベントデータストアを作成します。 AWS CLI
- を使用して Insights イベントのイベントデータストアを作成します。 AWS CLI

を使用して S3 データイベントのイベントデータストアを作成します。 AWS CLI

次の example AWS Command Line Interface (AWS CLI) create-event-data-store コマンドは、すべての Amazon S3 my-event-data-store データイベントを選択するという名前のイベントデータストアを作成し、KMS キーを使用して暗号化します。

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--kms-key-id "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias" \
--advanced-event-selectors '[
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith": ["arn:aws:s3"] }
            ]
        }
```

```
    ]'
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:19:39.417000-05:00",
    "UpdatedTimestamp": "2023-11-09T22:19:39.603000-05:00"
}
```

AWS Config を使用して設定項目用のイベントデータストアを作成します。 AWS CLI

AWS CLI create-event-data-store以下のコマンド例では、config-items-eds AWS Config 設定項目を選択するという名前のイベントデータストアを作成します。設定項目を収集するには、高度なイベントセレクタで eventCategory フィールドに対して Equals ConfigurationItem を指定します。

```
aws cloudtrail create-event-data-store \
--name config-items-eds \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "config-items-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select AWS Config configuration items",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "ConfigurationItem"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
```

```
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-07T19:03:24.277000+00:00",
    "UpdatedTimestamp": "2023-11-07T19:03:24.468000+00:00"
}
```

を使用して、管理イベント用の組織イベントデータストアを作成します。 AWS CLI

AWS CLI create-event-data-store以下のコマンド例は、すべての管理イベントを収集する組織イベントデータストアを作成し、--billing-modeFIXED_RETENTION_PRICINGパラメーターをに設定します。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-enabled
 --billing-mode FIXED_RETENTION_PRICING
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

を使用して Insights イベントのイベントデータストアを作成します。 AWS CLI

CloudTrail Lake で Insights イベントを記録するには、Insights イベントを収集する送信先イベントデータストアと、Insights を有効にして管理イベントをログに記録するソースイベントデータストアが必要です。

この手順では、送信先イベントデータストアとソースイベントデータストアを作成し、Insights イベントを有効にする方法を説明します。

1. aws cloudtrail create-event-data-store コマンドを実行して、Insights イベントを収集する送信先イベントデータストアを作成します。`eventCategory` の値は `Insight` にする必要があります。*`retention-period-days`*イベントをイベントデータストアに保持したい日数に置き換えてください。有効な値は、`--billing-mode` が `EXTENDABLE_RETENTION_PRICING` の場合は 7 から 3653 までの整数で、`--billing-mode` が `FIXED_RETENTION_PRICING` に設定されている場合は 7 から 2557 までの整数です。指定しない場合は`--retention-period`、CloudTrail のデフォルトの保持期間が使用されます`--billing-mode`。

   AWS Organizations 組織の管理アカウントでサインインしている場合、`--organization-enabled`委任管理者にイベントデータストアへのアクセス権を付与する場合はパラメータを含めてください。

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
         "Name": "Select Insights events",
         "FieldSelectors": [
             { "Field": "eventCategory", "Equals": ["Insight"] }
           ]
       }
     ]'
   ```

   以下に、応答の例を示します。

   ```
   {
       "Name": "insights-event-data-store",
       "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
   EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
   ```

```
    "AdvancedEventSelectors": [
        {
           "Name": "Select Insights events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "Insight"
                    ]
                }
             ]
        }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:22:33.714000+00:00"
}
```

この応答の ARN (または ARN の ID サフィックス) は、ステップ 3 で `--insights-destination` パラメータの値として使用します。

2. 管理イベントを口グ記録するソースイベントデータストアを作成するには、aws cloudtrail create-event-data-store コマンドを実行します。イベントデータストアのデフォルトでは、すべての口グ管理イベントを口グ記録します。すべての管理イベントを口グ記録するのであれば、高度なイベントセレクタを指定する必要はありません。*retention-period-days*イベントデータストアにイベントを保存したい日数に置き換えてください。有効な値は、`--billing-mode` が EXTENDABLE_RETENTION_PRICING の場合は 7 から 3653 までの整数で、`--billing-mode` が FIXED_RETENTION_PRICING に設定されている場合は 7 から 2557 までの整数です。指定しない場合は`--retention-period`、 CloudTrail のデフォルトの保持期間が使用されます`--billing-mode`。組織のイベントデータストアを作成する場合は、`--organization-enabled` パラメータを含めます。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-period retention-period-days
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-05-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-05-08T15:25:35.714000+00:00"
}
```

この応答の ARN (または ARN の ID サフィックス) は、ステップ 3 で `--event-data-store` パラメータの値として使用します。

3. put-insight-selectors コマンドを実行して Insights イベントを有効にします。Insights セレクターの値は、`ApiCallRateInsight`、`ApiErrorRateInsight`、または両方になります。`--event-data-store` パラメータには、管理イベントを口グに記録して Insights を有効にするソースイベントデータストアの ARN (または ARN の ID サフィックス) を指定します。`--insights-destination` パラメータには、Insights イベントを口グ記録する送信先イベントデータストアの ARN (または ARN の ID サフィックス) を指定します。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
```

```
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

次の結果は、イベントデータストア用に設定された Insights イベントセレクタを表示しています。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

イベントデータストアで CloudTrail Insights を初めて有効にしてから、異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントが配信されるまでに最大 7 日かかることがあります。

CloudTrail Insights は、グローバルではなく 1 つのリージョンで発生する管理イベントを分析します。 CloudTrail インサイトイベントは、それをサポートする管理イベントが生成されるのと同じリージョンで生成されます。

組織イベントデータストアでは、 CloudTrail 組織のすべての管理イベントの集計を分析する代わりに、各メンバーのアカウントからの管理イベントを分析します。

Lake で Insights イベントを取り込むには追加料金がかかります。 CloudTrail 証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。 CloudTrail 料金について詳しくは、「料金表」を参照してくださいAWS CloudTrail 。

を使用して、トレイルイベントをイベントデータストアにインポートします。 AWS CLI

では AWS CLI、トレイルイベントをイベントデータストアにインポートできます。このセクションの手順では、create-event-data-store コマンドを実行してイベントデータストアを作成および設定し、start-import コマンドを使用してそのイベントデータストアにイベントをインポートする方法を示しています。考慮事項や必要なアクセス許可など、証跡イベントのインポートの詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。

証跡イベントのインポートの準備

証跡イベントをインポートする前に、次の準備を行います。

- 証跡イベントをイベントデータストアにインポートするのに必要なアクセス許可を持つロールを持っていることを確認してください。
- イベントデータストアに指定する --billing-mode の値を決定します。`--billing-mode` によって、イベントの取り込みと保存にかかるコスト、および、イベントデータストアでの保持期間のデフォルトと最大が決まります。

  トレイルイベントを CloudTrail Lake にインポートすると、gzip (圧縮) CloudTrail 形式で保存されているログが解凍されます。次に、 CloudTrail ログに含まれるイベントをイベントデータストアにコピーします。非圧縮データのサイズは、実際の Amazon S3 ストレージサイズよりも大きくなる可能性があります。非圧縮データのサイズを概算するには、S3 バケット内のログのサイズに 10 を掛けます。この見積もりを使用して、ユースケースに合った `--billing-mode` の値を選択できます。
- 指定する `--retention-period` の値を決定します。 CloudTrail `eventTime`指定された保存期間より古いイベントはコピーされません。

  適切な保持期間を決定するには、次の式に示すように、コピーしたい最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数の合計を計算します。

  保存期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*

  例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。
- 今後のイベントの分析にイベントデータストアを使用するかどうかを決定します。今後のイベントを取り込みたくない場合は、イベントデータストアを作成するときに `--no-start-ingestion` パラメータを含めます。デフォルトでは、イベントデータストアは作成されたときにイベントの取り込みを開始します。

イベントデータストアを作成し、そのイベントデータストアに証跡イベントをインポートするには

1. create-event-data-store コマンドを実行して新しいイベントデータストアを作成します。この例では、コピーされる最も古いイベントが 90 日前のもので、イベントを 30 日間保持したいので、--retention-period は 120 に設定されています。今後のイベントは取り込みたくないので、--no-start-ingestion パラメータが設定されています。この例では、取り込むイベントデータは 25 TB 未満と予想されるため、デフォルト値の EXTENDABLE_RETENTION_PRICING を使用しているので、--billing-mode は設定されていません。

   > **Note**
   >
   > 証跡を置き換えるためにイベントデータストアを作成する場合は、証跡のイベントセレクタと一致するように --advanced-event-selectors を設定して、同じイベント範囲になるようにすることをお勧めします。イベントデータストアのデフォルトでは、すべての管理イベントをログ記録します。

   ```
   aws cloudtrail create-event-data-store  --name import-trail-eds  --retention-period
    120 --no-start-ingestion
   ```

   以下に、応答の例を示します。

   ```
   {
       "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
   EXAMPLEa-4357-45cd-bce5-17ec652719d9",
       "Name": "import-trail-eds",
       "Status": "CREATED",
       "AdvancedEventSelectors": [
           {
               "Name": "Default management events",
               "FieldSelectors": [
                   {
                       "Field": "eventCategory",
                       "Equals": [
                           "Management"
                       ]
                   }
               ]
           }
   ```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

最初の Status は CREATED なので、get-event-data-store コマンドを実行して取り込みが停止したことを確認します。

```
aws cloudtrail get-event-data-store --event-data-store eds-id
```

応答には Status が STOPPED_INGESTION になったことが表示され、イベントデータストアがライブイベントを取り込んでいないことが示されます。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9",
    "Name": "import-trail-eds",
    "Status": "STOPPED_INGESTION",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 120,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T16:52:25.444000+00:00",
```

```
    "UpdatedTimestamp": "2023-11-09T16:52:25.569000+00:00"
}
```

2. start-import コマンドを実行して、ステップ 1 で作成したイベントデータストアに証跡イベントをインポートします。--destinations パラメータの値として、イベントデータストアの ARN (または ARN の ID サフィックス) を指定します。--start-event-time にはコピーする最も古いイベントの eventTime を指定し、--end-event-time にはコピーする最新のイベントの eventTime を指定します。には、トレイルログを含むS3バケットのS3 URI、S3バケットのS3 URI、およびトレイルイベントのインポートに使用されるロールの ARN --import-source を指定します。 AWS リージョン

```
aws cloudtrail start-import \
--destinations ["arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"] \
--start-event-time 2023-08-11T16:08:12.934000+00:00 \
--end-event-time 2023-11-09T17:08:20.705000+00:00 \
--import-source {"S3": {"S3LocationUri": "s3://aws-cloudtrail-
logs-123456789012-612ff1f6/AWSLogs/123456789012/CloudTrail/","S3BucketRegion":"us-
east-1","S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"}}
```

以下に、応答の例を示します。

```
{
   "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
   "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
   "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
   "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3257fcd1",
   "ImportSource": {
      "S3": {
         "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds",
         "S3BucketRegion":"us-east-1",
         "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/"
      }
   },
   "ImportStatus": "INITIALIZING",
```

```
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "UpdatedTimestamp": "2023-11-09T17:08:20.806000+00:00"
}
```

3. get-import コマンドを実行して、インポートに関する情報を取得します。

```
aws cloudtrail get-import --import-id import-id
```

以下に、応答の例を示します。

```
{
    "ImportId": "EXAMPLEe-7be2-4658-9204-b38c3EXAMPLE",
    "Destinations": [
        "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEa-4357-45cd-bce5-17ec652719d9"
    ],
    "ImportSource": {
        "S3": {
            "S3LocationUri": "s3://aws-cloudtrail-logs-123456789012-111ff1f6/
AWSLogs/123456789012/CloudTrail/",
            "S3BucketRegion":"us-east-1",
            "S3BucketAccessRoleArn": "arn:aws:iam::123456789012:role/service-role/
CloudTrailLake-us-east-1-copy-events-eds"
        }
    },
    "StartEventTime": "2023-08-11T16:08:12.934000+00:00",
    "EndEventTime": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatus": "COMPLETED",
    "CreatedTimestamp": "2023-11-09T17:08:20.705000+00:00",
    "ImportStatistics": {
        "PrefixesFound": 1548,
        "PrefixesCompleted": 1548,
        "FilesCompleted": 92845,
        "EventsCompleted": 577249,
        "FailedEntries": 0
    }
}
```

インポートは、失敗がなかった場合、COMPLETED の ImportStatus で終了し、失敗があった場合、FAILED で終了します。

インポートに FailedEntries があった場合は、list-import-failures コマンドを実行して失敗のリストを返すことができます。

```
aws cloudtrail list-import-failures --import-id import-id
```

失敗したインポートを再試行するには、--import-id パラメータのみを指定して start-import コマンドを実行します。インポートを再試行すると、 CloudTrail 障害が発生した場所でインポートが再開されます。

```
aws cloudtrail start-import --import-id import-id
```

を使用してイベントデータストアを取得します。 AWS CLI

AWS CLI get-event-data-store次のコマンド例は、ARN または ARN の ID --event-data-store サフィックスを受け入れる必須パラメータで指定されたイベントデータストアに関する情報を返します。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下に、応答の例を示します。作成時刻と最終更新時刻は timestamp 形式です。

```
{
    "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "s3-data-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log DeleteObject API calls for a specific S3 bucket",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
```

```
                    "Field": "eventName",
                    "Equals": [
                        "DeleteObject"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3:::bucketName"
                    ]
                },
                {
                    "Field": "readOnly",
                    "Equals": [
                        "false"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-09T22:20:36.344000+00:00",
    "UpdatedTimestamp": "2023-11-09T22:20:36.476000+00:00"
}
```

のアカウントにあるすべてのイベントデータストアを一覧表示します。 AWS CLI

AWS CLI list-event-data-stores以下のコマンド例は、現在のリージョンのアカウント内のすべてのイベントデータストアに関する情報を返します。オプションのパラメータには、コマンドが単一のページに返す結果の最大数を指定する `--max-results` が含まれます。指定した `--max-results` 値よりも多くの結果がある場合は、返された `NextToken` 値を追加してコマンドを再度実行し、結果の次のページを取得します。

```
aws cloudtrail list-event-data-stores
```

以下に、応答の例を示します。

```
{
    "EventDataStores": [
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE7-cad6-4357-a84b-318f9868e969",
            "Name": "management-events-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE6-88e1-43b7-b066-9c046b4fd47a",
            "Name": "config-items-eds"
        },
        {
            "EventDataStoreArn": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLEf-b314-4c85-964e-3e43b1e8c3b4",
            "Name": "s3-data-events"
        }
    ]
}
```

イベントデータストアを次のように更新します。 AWS CLI

次の例では、イベントデータストアを更新する方法を示します。

トピック

- 請求モードを次のように更新します。 AWS CLI
- リテンションモードを更新し、ターミネーション保護を有効にして、 AWS KMS key で a を指定します。 AWS CLI
- で終了保護を無効にします AWS CLI

請求モードを次のように更新します。 AWS CLI

イベントデータストアの --billing-mode によって、イベントの取り込みと保存にかかるコスト、および、イベントデータストアでの保持期間のデフォルトと最大が決まります。イベントデータストアの --billing-mode が FIXED_RETENTION_PRICING に設定されている場合は、値を EXTENDABLE_RETENTION_PRICING に変更できます。イベントデータストアで 1 か月あたりに

取り込まれるイベントデータが 25 TB 未満で、最大 3653 日の柔軟な保持期間を設定したい場合には、一般的に EXTENDABLE_RETENTION_PRICING をお勧めします。料金については、「AWS CloudTrail の料金」と「 CloudTrail Lake コストの管理」を参照してください。

> **Note**
>
> --billing-mode の値を EXTENDABLE_RETENTION_PRICING から FIXED_RETENTION_PRICING に変更することはできません。イベントデータストアの課金モードが EXTENDABLE_RETENTION_PRICING に設定されているが FIXED_RETENTION_PRICING を使用したい場合は、イベントデータストアで取り込みを停止して、FIXED_RETENTION_PRICING を使用する新しいイベントデータストアを作成できます。

AWS CLI update-event-data-store以下のコマンド例は、--billing-modeFIXED_RETENTION_PRICINGEXTENDABLE_RETENTION_PRICINGイベントデータストアのをからに変更します。--event-data-store パラメータ値は ARN (または ARN の ID サフィックス) で、必須です。その他のパラメータはオプションです。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--billing-mode EXTENDABLE_RETENTION_PRICING
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

リテンションモードを更新し、ターミネーション保護を有効にして、 AWS KMS key で a を指定します。 AWS CLI

AWS CLI update-event-data-store次のコマンド例は、イベントデータストアを更新して保持期間を 100 日に変更し、終了保護を有効にします。`--event-data-store` パラメータ値は ARN (または ARN の ID サフィックス) で、必須です。その他のパラメータはオプションです。この例では、保持期間を 100 日間に変更するために `--retention-period` パラメータが追加されています。オプションで、`--kms-key-id`コマンドに追加し、値として KMS キー ARN を指定することで、 AWS Key Management Service 暗号化を有効にしてを指定できます。 AWS KMS key `--termination-protection-enabled`終了保護が有効になっていないイベントデータストアで終了保護を有効にするために追加されました。

外部からのイベントを記録するイベントデータストアは、 AWS AWS イベントを記録するように更新することはできません。同様に、 AWS イベントを記録するイベントデータストアは、外部からのイベントを記録するように更新することはできません AWS。

> **Note**
>
> CloudTrail イベントデータストアの保持期間を短縮すると、`eventTime`新しい保存期間より古いイベントはすべて削除されます。たとえば、以前の保持期間が 365 日だったのに 100 日に短縮した場合、100 CloudTrail 日以上前のイベントは削除されます。`eventTime`

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE \
```

```
--retention-period 100 \
--kms-key-id "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias" \
--termination-protection-enabled
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Select all S3 data events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
                    "StartsWith": [
                        "arn:aws:s3"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 100,
    "KmsKeyId": "arn:aws:kms:us-east-1:0123456789:alias/KMS_key_alias",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
```

```
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

で終了保護を無効にします AWS CLI

デフォルトでは、イベントデータストアでは終了保護が有効になり、イベントデータストアが誤って削除されるのを防ぎます。終了保護が有効の場合、イベントデータストアを削除できません。イベントデータストアを削除するには、まず終了保護を無効にする必要があります。

AWS CLI update-event-data-store以下のコマンド例は、--no-termination-protection-enabledパラメータを渡すことで終了保護を無効にします。

```
aws cloudtrail update-event-data-store \
--region us-east-1 \
--no-termination-protection-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "management-events-eds",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
```

```
    "TerminationProtectionEnabled": false,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

を使用してイベントデータストアへの取り込みを停止します。 AWS CLI

AWS CLI stop-event-data-store-ingestion以下のコマンド例は、イベントデータストアによるイベントの取り込みを停止します。取り込みを停止するには、イベントデータストアの Status が ENABLED で、eventCategory が Management、Data、ConfigurationItem のいずれかでなければなりません。イベントデータストアは --event-data-store によって指定されます。これは、イベントデータストア ARN、または、この ARN の ID サフィックスを受け入れます。stop-event-data-store-ingestion を実行すると、イベントデータストアの状態が STOPPED_INGESTION に変化します。

イベントデータストアの状態が STOPPED_INGESTION である場合、そのストアはアカウントの最大数 (10 個) に計上されません。

```
aws cloudtrail stop-event-data-store-ingestion
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

コマンドが成功した場合、レスポンスはありません。

を使用してイベントデータストアへの取り込みを開始します。 AWS CLI

AWS CLI start-event-data-store-ingestion以下のコマンド例は、イベントデータストアへのイベントの取り込みを開始します。取り込みを開始するには、イベントデータストアの Status が STOPPED_INGESTION で、eventCategory が Management、Data、ConfigurationIte
いずれかでなければなりません。イベントデータストアは --event-data-store によって指定されます。これは、イベントデータストア ARN、または、この ARN の ID サフィックスを受け入れます。start-event-data-store-ingestion を実行すると、イベントデータストアの状態が ENABLED に変化します。

```
aws cloudtrail start-event-data-store-ingestion --event-data-store
 arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-
bcf6cEXAMPLE
```

コマンドが成功した場合、レスポンスはありません。

イベントデータストアでのフェデレーションを有効にする

フェデレーションを有効にするには、必須パラメータの `--event-data-store` と `--role` を指定して aws cloudtrail enable-federation コマンドを実行します。`--event-data-store` には、イベントデータストア ARN (または ARN の ID サフィックス) を指定します。`--role` には、フェデレーションロールの ARN を指定します。ロールはアカウントに存在し、必要最小限のアクセス許可が付与されている必要があります。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

この例は、管理アカウントのイベントデータストアの ARN と、委任された管理者アカウントのフェデレーションロールの ARN を指定することで、委任された管理者が組織のイベントデータストアのフェデレーションを有効にする方法を示しています。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

イベントデータストアでのフェデレーションを無効にする

イベントデータストアでのフェデレーションを無効にするには、aws cloudtrail disable-federation コマンドを実行します。イベントデータストアは、イベントデータストア ARN、または ARN の ID サフィックスを受け入れる `--event-data-store` によって指定されます。

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> これが組織のイベントデータストアである場合は、管理アカウントのアカウント ID を使用します。

を使用してイベントデータストアを削除します。 AWS CLI

以下のサンプル AWS CLI delete-event-data-store コマンドは、イベントデータストア ARN、または ARN の ID サフィックスを受け入れる `--event-data-store` によって指定されたイベントデータストアを無効にします。delete-event-data-store の実行後、イベントデータストアの最終状態が `PENDING_DELETION` になり、イベントデータストアは 7 日間の待機期間後に自動的に削除されます。

イベントデータストアでの delete-event-data-store の実行後、無効化されたデータストアを使用しているクエリで list-queries、describe-query、または get-query-results を実行することはできません。イベントデータストアが削除保留中になっている場合、そのイベントデータストアはアカウントの最大数 (10 個) に計上されます。

> **Note**
>
> `--termination-protection-enabled` が設定されている場合、または `FederationStatus` が `ENABLED` に設定されている場合は、イベントデータストアを削除できません。

```
aws cloudtrail delete-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

コマンドが成功した場合、レスポンスはありません。

を使用してイベントデータストアを復元します。 AWS CLI

以下のサンプル AWS CLI restore-event-data-store コマンドは、削除保留中のイベントデータストアを復元します。イベントデータストアは、イベントデータストア ARN、または ARN の ID サフィックスを受け入れる `--event-data-store` によって指定されます。削除されたイベントデータストアを復元できるのは、削除後 7 日間の待機期間内のみです。

```
aws cloudtrail restore-event-data-store
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

レスポンスには、ARN、高度なイベントセレクタ、および復元のステータスなどのイベントデータストアに関する情報が含まれています。

イベントデータストアのライフサイクルを管理する

以下は、イベントデータストアのライフサイクルの各ステージです。

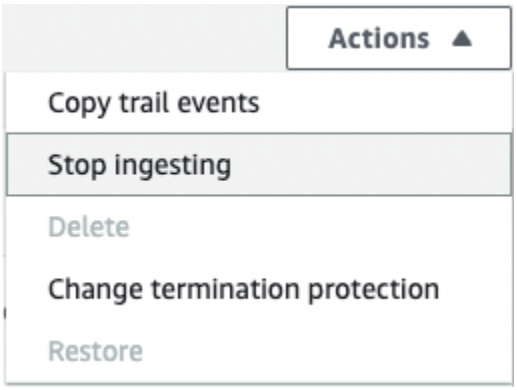
- CREATED – イベントデータストアが作成されたことを示す短期的な状態です。
- ENABLED — イベントデータストアはアクティブで、イベントを取り込んでいます。クエリを実行し、証跡イベントをイベントデータストアにコピーすることができます。
- STARTING_INGESTION — イベントデータストアがライブイベントの取り込みを開始することを示す、短期的な状態です。
- STOPPING_INGESTION — イベントデータストアがライブイベントの取り込みを停止することを示す、短期的な状態です。
- STOPPED_INGESTION — イベントデータストアは、ライブイベントを取り込んでいません。イベントデータストアにすでに存在するイベントに対してクエリを実行したり、証跡イベントをイベントデータストアにコピーしたりすることはできます。
- PENDING_DELETION – イベントデータストアは ENABLED または STOPPED_INGESTION の状態になり、削除されましたが、現在は 7 日間の待機期間中で、これが終わると永久に削除されます。このイベントデータストアではクエリは実行できず、復元以外の操作を実行することはできません。

イベントデータストアを削除できるのは、フェデレーションと終了保護の両方が無効になっている場合のみです。終了保護は、イベントデータストアが誤って削除されることを防ぎます。デフォルトで、イベントデータストアでは終了保護が有効になっています。フェデレーションで Athena のイベントデータストアデータをクエリできますが、デフォルトでは無効になっています。

イベントデータストアを削除すると、イベントデータストアは 7 日間 PENDING_DELETION 状態を保持した後で、恒久的に削除されます。7 日間の待機期間中は、イベントデータストアを復元できます。PENDING_DELETION 状態の間、イベントデータストアをクエリに使用することはできず、復元操作以外の操作をイベントデータストアで実行することはできません。削除保留中のイベントデータストアはイベントの取り込みを行わないため、料金は発生しません。ただし、削除保留中のイベントデータストアは、1 つの に存在する可能性のあるイベントデータストアのクォータにカウントされます AWS リージョン。

イベントデータストアで実行可能なアクション

イベントデータストアの削除または復元、証跡イベントのコピー、イベント取り込みの開始または停止、イベントストアの終了保護の有効化または無効化の操作には、イベントデータストアの詳細ページの [アクション] メニューにあるコマンドを使用します。



証跡イベントをコピーするオプションは、 CloudTrail 管理イベントとデータイベントを含むイベントデータストアでのみ使用できます。取り込みを開始および停止するオプションは、イベント (管理イベントとデータ CloudTrail イベント) または AWS Config 設定項目を含むイベントデータストアでのみ使用できます。

イベントデータストアへ証跡イベントをコピーします

トレイルイベントを CloudTrail Lake イベントデータストアにコピーして、 point-in-time トレイルに記録されたイベントのスナップショットを作成できます。証跡イベントをコピーしても、イベントをログに記録する証跡の機能が損なわれることはなく、証跡が変更されることもありません。

CloudTrail トレイルイベントをイベント用に構成された既存のイベントデータストアにコピーすることも、 CloudTrail 新しいイベントデータストアを作成して、イベントデータストアの作成の一部として [トレイルイベントのコピー] オプションを選択することもできます。証跡イベントを既存のイベントデータストアにコピーする方法の詳細については、「既存のイベントデータストアに証跡イベントをコピーします」を参照してください。新しいイベントデータストアの作成方法に関する詳細は、「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。

証跡イベントを組織のイベントデータストアにコピーするには、組織の管理アカウントを使用する必要があります。組織の委任された管理者アカウントを使用して、証跡イベントをコピーすることはできません。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail コストの価格設定と管理について詳しくは、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

トレイルイベントを CloudTrail Lake イベントデータストアにコピーすると、イベントデータストアが取り込む非圧縮データの量に基づいて料金が発生します。

トレイルイベントを CloudTrail Lake にコピーすると、gzip（圧縮）CloudTrail 形式で保存されているログを解凍し、ログに含まれるイベントをイベントデータストアにコピーします。非圧縮データのサイズは、実際の S3 ストレージサイズよりも大きくなる可能性があります。圧縮されていないデータのサイズを概算するには、S3 バケット内のログのサイズに 10 を掛けます。

コピーするイベントの時間範囲を短くすることで、コストを削減できます。コピーしたイベントのクエリにイベントデータストアのみを使用する予定の場合は、イベントの取り込みを無効にして、今後のイベントで料金が発生しないようにすることができます。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

シナリオ

次の表は、証跡イベントのコピーに関する一般的なシナリオと、コンソールを使用して各シナリオを実行する方法について示したものです。

シナリオ	どうすればコンソールでこれを実行できますか?
新しいイベントを取り込むことなく、 CloudTrail Lake の過去のトレイルイベントの分析とクエリを行います。	新しいイベントデータストアを作成し、イベントデータストアを作成する一環として [証跡イベントをコピー] を選択します。イベントデータストアを作成する際には、[イベントを取り込む] (手順のステップ 15) の選択を解除し、イベントデータストアが確実に証跡の過去のイベントのみを含み、未来のイベントは含まれないようにします。
既存のトレイルを CloudTrail Lake イベントデータストアに置き換えます。	証跡と同じイベントセレクターを持つイベントデータストアを作成し、イベントデータストアの対象範囲が証跡と同じであることを確認します。 ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成より前の、コピーされたイベントの日付範囲を選択します。 イベントデータストアを作成したら、証跡の ログ記録をオフにします。そうすれば、追加料金の発生を防げます。

トピック

- 証跡イベントのコピーに関する留意事項
- 証跡イベントのコピーに必要な許可
- 既存のイベントデータストアに証跡イベントをコピーします
- イベントコピーの詳細
- 例:トレイルイベントを新しいイベントデータストアにコピーします。

証跡イベントのコピーに関する留意事項

証跡イベントをコピーする場合は、以下の要素を考慮してください。

- トレイルイベントをコピーする場合、S3 `GetObject`API CloudTrail オペレーションを使用してソース S3 バケットのトレイルイベントを取得します。S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Outposts、S3 Intelligent-Tiering Deep Archive 階層など、一部の S3 でアーカイブされたストレージクラスには、`GetObject` を使用してアクセスできません。これらのアーカイブ済みストレージ クラスに保存されている証跡イベントをコピーするには、まず S3 `RestoreObject` オペレーションでコピーを復元する必要があります。アーカイブされたオブジェクトの復元の詳細については、「Amazon S3 ユーザーガイド」の「アーカイブされたオブジェクトの復元」を参照してください。
- トレイルイベントをイベントデータストアにコピーすると、 CloudTrail コピー先のイベントデータストアのイベントタイプ、高度なイベントセレクター、 AWS リージョンまたはの設定に関係なく、すべてのトレイルイベントがコピーされます。
- 証跡イベントを既存のイベントデータストアにコピーする前に、そのイベントデータストアの料金設定オプションと保持期間が、ご自身のユースケースについて適切に設定されていることを確認してください。
  - 料金オプション: 料金オプションによって、イベントの取り込みと保存にかかるコストが決まります。料金オプションの詳細については、「AWS CloudTrail 料金表」および「イベントデータストアの料金オプション」を参照してください。
  - 保存期間:保持期間によって、イベントデータがイベントデータストアに保持される期間が決まります。 CloudTrail `eventTime`イベントデータストアの保持期間内であるトレイルイベントのみをコピーします。適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数 (保持期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

- 調査のため証跡イベントをイベントデータストアにコピーしており、それ以上のイベントを取り込む必要がない場合は、イベントデータストアへの取り込みを停止できます。イベントデータストアを作成する際に、[イベントを取り込む] オプション (手順のステップ 15) の選択を解除し、イベントデータストアは確実に証跡の過去のイベントのみを含み、未来のイベントは含まれないようにします。
- 証跡イベントをコピーする前に、ソース S3 バケットにアタッチされているアクセスコントロールリスト (ACL) をすべて無効にして、送信先イベントデータストアの S3 バケットポリシーを更新します。S3 バケットとポリシーの更新の詳細については、「証跡イベントのコピー用の Amazon S3 バケットポリシー」を参照してください。ACL の無効化の詳細については、「Amazon S3 ユーザーガイド」の「オブジェクトの所有権のコントロールとバケットに対する ACL の無効化」を参照してください。
- CloudTrail ソース S3 バケットにある Gzip 圧縮ログファイルからのトレイルイベントのみをコピーします。 CloudTrail 圧縮されていないログファイルや Gzip 以外の形式で圧縮されたログファイルからはトレイルイベントをコピーしません。
- ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の、コピーされたイベントの時間範囲を選択します。
- デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、`CloudTrail`他のサービスのプレフィックスをチェックしません。 AWS CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、トレイルイベントをコピーするときにプレフィックスを選択する必要があります。
- 証跡イベントを組織のイベントデータストアにコピーするには、組織の管理アカウントを使用する必要があります。委任された管理者アカウントは、証跡イベントを組織のイベントデータストアにコピーできません。

証跡イベントのコピーに必要な許可

トレイルイベントをコピーする前に、IAM ロールに必要な権限がすべて揃っていることを確認してください。IAM ロールの許可を更新する必要があるのは、既存の IAM ロールを選択して証跡イベントをコピーする場合だけです。新しい IAM ロールを作成する場合は、 CloudTrail そのロールに必要なすべての権限が付与されます。

ソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでバケット内のデータの復号化が許可されていることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、 CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。

トピック

証跡イベントをコピーするための IAM 許可

証跡イベントをコピーする場合は、新しい IAM ロールを作成するか、既存の IAM ロールを使用するか選択できます。新しい IAM ロールを選択すると、必要な権限を持つ IAM CloudTrail ロールが作成されます。ユーザー側でこれ以上アクションを行う必要はありません。

既存のロールを選択する場合は、IAM ロールのポリシーでソース S3 CloudTrail バケットからトレイルイベントをコピーできることを確認してください。このセクションでは、必要な IAM ロールのアクセス許可と信頼ポリシーの例を示します。

次の例は、ソース S3 CloudTrail バケットからトレイルイベントをコピーすることを許可するアクセス権限ポリシーを示しています。*myAccountId*、*#####*、*#######*、*eventDataStoreId* を、設定に適した値に置き換えます*myBucketName*。*MyAccountId* は CloudTrail Lake AWS に使用されるアカウント ID であり、S3 AWS バケットのアカウント ID とは異なる場合があります。

key-region、*keyAccountID*、*keyID* を、ソース S3 バケットの暗号化に使用する KMS キーの値に置き換えます。送信元 S3 バケットが暗号化に KMS キーを使用しない場合は、AWSCloudTrailImportKeyAccess ステートメントを省略できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
```

```
        }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
         }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

次の例は IAM 信頼ポリシーを示しています。これにより、IAM CloudTrail ロールを引き受け、ソース S3 バケットからトレイルイベントをコピーできます。*myAccountId*、*#####*、および *eventDataStoreArn* を、設定に適した値に置き換えてください。*MyAccountID* は CloudTrail Lake に使用される AWS アカウント ID であり、S3 バケットのアカウント ID と同じではない場合があります。 AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
```

```
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

証跡イベントのコピー用の Amazon S3 バケットポリシー

デフォルトでは、Amazon S3 バケットとオブジェクトはプライベートです。リソース所有者 (バケットを作成した AWS アカウント) のみが、バケットとそれに含まれるオブジェクトにアクセスできます。リソース所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

トレイルイベントをコピーする前に、S3 バケットポリシーを更新して、ソース S3 CloudTrail バケットからトレイルイベントをコピーできるようにする必要があります。

S3 バケットポリシーに次のステートメントを追加して、これらの権限を付与できます。*roleArn* *myBucketName*とを実際の構成に適した値に置き換えてください。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
```

```
    ]
},
```

ソース S3 バケット内のデータを復号化するための KMS キーポリシー

ソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、SSE-KMS 暗号化が有効になっている S3 `kms:Decrypt` `kms:GenerateDataKey` バケットからトレイルイベントをコピーするのに必要なおよび権限が KMS キーポリシーに含まれていることを確認してください。 CloudTrail ソース S3 バケットが複数の KMS キーを使用している場合は、各キーポリシーを更新する必要があります。KMS キーポリシーを更新すると CloudTrail 、ソース S3 バケットのデータを復号化し、CloudTrail検証チェックを実行してイベントが標準に準拠していることを確認し、イベントを Lake イベントデータストアにコピーできるようになります。 CloudTrail

次の例は、ソース S3 バケットのデータを復号化できる CloudTrail KMS キーポリシーを示しています。*roleArn myBucketName*、*MyAccountId*、*#####*、*eventDataStoreID* は、構成に適した値に置き換えてください。*MyAccountID* は CloudTrail Lake AWS に使用されるアカウント ID であり、S3 バケットのアカウント ID とは異なる場合があります。 AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

既存のイベントデータストアに証跡イベントをコピーします

以下の手順を実行し、証跡イベントを既存のイベントデータストアにコピーします。新しいイベントデータストアの作成方法に関する詳細は、「コンソールを使用してイベントのイベントデータストアCloudTrailを作成する」を参照してください。

> **Note**
>
> 証跡イベントを既存のイベントデータストアにコピーする前に、そのイベントデータストアの料金設定オプションと保持期間が、ご自身のユースケースについて適切に設定されていることを確認してください。
>
> - 料金オプション: 料金オプションによって、イベントの取り込みと保存にかかるコストが決まります。料金オプションの詳細については、「AWS CloudTrail 料金表」および「イベントデータストアの料金オプション」を参照してください。
> - 保存期間:保持期間によって、イベントデータがイベントデータストアに保持される期間が決まります。 CloudTrail `eventTime`イベントデータストアの保持期間内であるトレイルイベントのみをコピーします。適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数 (保持期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

イベントデータストアに証跡イベントをコピーするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [Copy trail events] (トレイルイベントをコピー) を選択します。
4. [Copy trail events] (証跡イベントのコピー) ページの [Event source] (イベント ソース) で、コピーする証跡を選択します。デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、 AWS 他のサービスのプレフィックスを確認しません。 CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、[Enter S3 URI] を選択し、[Browse S3] を選択してプレフィックスを参照します。トレイルのソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでデータの復号化が許可されて

いることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。KMS キーポリシーの更新の詳細については、「ソース S3 バケット内のデータを復号化するための KMS キーポリシー」を参照してください。

S3 バケットポリシーは、S3 CloudTrail バケットからトレイルイベントをコピーするためのアクセス権を付与する必要があります。S3 バケットとポリシーの更新の詳細については、「証跡イベントのコピー用の Amazon S3 バケットポリシー」を参照してください。

5. [イベントの時間範囲を指定] で、イベントをコピーする時間範囲を選択します。 CloudTrail トレイルイベントをコピーする前に、プレフィックスとログファイル名をチェックして、選択した開始日と終了日の間の日付が名前に含まれていることを確認します。[Relative range] (相対範囲) または[Absolute range] (絶対範囲) を選択することができます。ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の時間範囲を選択します。

   > **Note**
   >
   > CloudTrail `eventTime`イベントデータストアの保存期間内のトレイルイベントのみをコピーします。たとえば、イベントデータストアの保持期間が 90 日の場合、90 CloudTrail `eventTime` 日以上前のトレイルイベントはコピーされません。

   - [相対範囲] を選択すると、過去 6 か月、1 年、2 年、7 年間に記録されたイベントをコピーするか、またはカスタム範囲をコピーするかを選択できます。 CloudTrail 選択した期間内に記録されたイベントをコピーします。
   - [絶対範囲] を選択すると、特定の開始日と終了日を選択できます。 CloudTrail 選択した開始日と終了日の間に発生したイベントをコピーします。
6. [Delivery location] (配信場所) で、ドロップダウンリストから配信先イベントデータストアを選択します。
7. [Permissions] (アクセス許可) については、以下の IAM ロールのオプションから選択します。既存の IAM ロールを選択する場合は、IAM ロールポリシーが必要なアクセス許可を提供していることを確認してください。IAM ロールの許可の更新の詳細については、「証跡イベントをコピーするための IAM 許可」を参照してください。

   - [Create a new role (recommended)] (新しいロールの作成 (推奨)) を選択して、新しい IAM ロールを作成します。[Enter IAM role name] (IAM ロール名を入力してください) に、ロールの名前を入力します。 CloudTrail この新しいロールに必要な権限が自動的に作成されます。

- リストにないカスタム IAM ロールを使用するには、[カスタム IAM ロール ARN を使用] を選択します。[Enter IAM role ARN] (IAM ロールの ARN を入力) で、IAM ARN を入力します。
- ドロップダウンリストから既存の IAM ロールを選択します。

8. [Copy events] (イベントをコピー) を選択します。
9. 確認を求められます。確認する準備ができたら、[Copy trail events to Lake] (証跡イベントを Lake にコピー) を選択してから[Copy events] (イベントをコピー) を選択します。
10. [Copy details] (コピーの詳細) ページで、コピーの状態を確認し、エラーを確認できます。証跡イベントのコピーが完了すると、その[Copy status] (コピー ステータス) は、エラーがない場合は[Completed] (完了) に設定され、エラーが発生した場合は[Failed] (失敗) に設定されます。

> **Note**
>
> イベントコピーの詳細ページに表示される詳細は、リアルタイムではありません。[Prefixes copied] (コピーされたプレフィックス) などの詳細の実際の値は、ページに表示される値よりも高くなる場合があります。 CloudTrail イベントコピーの過程で、詳細を段階的に更新します。

11. [Copy status] (コピーのステータス) が[Failed] (失敗) の場合は、[Copy failures] (コピーの失敗) に示されているエラーを修正し、[Retry copy] (コピーの再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。

証跡イベントコピーの詳細を表示する方法については、「イベントコピーの詳細」を参照してください。

イベントコピーの詳細

証跡イベントのコピーが開始されると、コピーの状態やコピーの失敗に関する情報など、イベントコピーの詳細を表示できます。

> **Note**
>
> イベントコピーの詳細ページに表示される詳細は、リアルタイムではありません。[Prefixes copied] (コピーされたプレフィックス) などの詳細の実際の値は、ページに表示される値よりも高くなる場合があります。CloudTrail イベントコピーの過程で詳細を段階的に更新します。

イベントコピーの詳細ページにアクセスするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. 左側のナビゲーション ペインの [Lake] で、[イベントデータストア] を選択します。
3. イベントデータストアを選択します。
4. [Event copy status] (イベントコピーステータス) セクションでイベントコピーを選択します。

詳細をコピーします

[Copy details] (コピーの詳細) から、証跡イベントのコピーに関する次の詳細を表示できます。

- [Event log S3 location] (イベントログ S3 の場所) - 証跡イベントログファイルを含むソース S3 バケットの場所。
- [Copy ID] (コピーの ID) - コピーの ID 。
- [Prefixes copied] (コピーされたプレフィックス) - コピーされた S3 プレフィックスの数を表します。トレイルイベントのコピー中に、 CloudTrail プレフィックスに保存されているトレイルログファイル内のイベントをコピーします。
- [Copy status] (コピーのステータス) - コピーのステータス。
  - [Initialize] (初期化中) - 証跡イベントのコピーが開始されたときに表示される初期状態。
  - [In progress] (進行中) - 証跡イベントのコピーが進行中であることを示します。

    > **Note**
    >
    > 別の証跡イベントのコピーが[In progress] (進行中) の場合、証跡イベントはコピーできません。証跡イベントのコピーを停止するには、[Stop copy] (コピーの停止) を選択します。

  - [Stopped] (停止中) - [Stop copy] (コピーを停止) アクションが発生したことを示します。証跡イベントのコピーを再試行するには、[Retry copy] (コピーの再試行) を選択します。
  - [Failed] (失敗) - コピーは完了しましたが、一部の証跡イベントはコピーに失敗しました。[Copy failures] (コピーの失敗) でエラーメッセージを確認します。証跡イベントのコピーを再試行するには、[Retry copy] (コピーの再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。
  - [Completed] (完了) - コピーはエラーなしで完了しました。イベントデータストア内のコピーされた証跡イベントをクエリできます。

- [Created time] (作成時刻) - 証跡イベントのコピーがいつ開始されたかを示します。
- [Finish time] (終了時刻) - 証跡イベントのコピーがいつ完了または停止したかを示します。

コピーの失敗

[Copy failures] (コピーの失敗) から、コピーの失敗ごとにエラーの場所、エラー メッセージ、およびエラーの種類を確認できます。失敗の一般的な理由としては、S3 プレフィックスに圧縮されていないファイルが含まれていたり、以外のサービスによって配信されたファイルが含まれていたことが挙げられます。CloudTrail失敗のもう 1 つ考えられ原因としては、アクセスの問題です。たとえば、イベントデータストアの S3 CloudTrail バケットがイベントをインポートするためのアクセス権を付与しなかった場合、`AccessDenied`エラーが発生します。

コピーの失敗ごとに、次のエラー情報を確認します。

- [Error location] (エラーの場所) - S3 バケット内の、エラーが発生した場所を示します。ソース S3 バケットに圧縮されていないファイルが含まれていたためにエラーが発生した場合、[Error location] (エラーの場所) に、そのファイルが見つかるプレフィックスがを含まれます。
- [Error message] (エラーメッセージ) - エラーが発生した理由について説明します。
- [Error type] (エラータイプ) - エラータイプを示します。たとえば、`AccessDenied` の [Error type] (エラータイプ)の場合、許可の問題が原因でエラーが発生したことを示します。証跡イベントのコピーに必要なアクセス許可の詳細については、「証跡イベントのコピーに必要な許可」を参照してください。

失敗を解決したら、[Retry copy] (再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。

例:トレイルイベントを新しいイベントデータストアにコピーします。

このチュートリアルでは、トレイルイベントを新しい CloudTrail Lake イベントデータストアにコピーして履歴分析を行う方法を説明します。証跡イベントのコピーに関する詳細については、「イベントデータストアへ証跡イベントをコピーします」を参照してください。

新規イベントデータストアへ証跡イベントをコピーする

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。

3. [Create event data store] (イベントデータストアの作成) をクリックします。
4. [イベントデータストアの設定] ページの [一般的な詳細] で、イベントデータストアに名前 (など) を入力します*my-management-events-eds*。イベントデートストアの意図をすぐに識別できる名前を使用するのがベストプラクティスです。 CloudTrail 命名要件については、を参照してください命名の要件。
5. イベントデータストアで使用したい [料金オプション] を選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、ご使用のイベントデータストアでのデフォルトと最長の保持期間が決まります。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

   以下のオプションが利用できます。

   - [1 年間の延長可能な保持料金] – 1 か月あたり取り込むイベントデータが 25 TB 未満で、最大 10 年間の柔軟な保存期間を希望する場合、一般的に推奨されます。最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加料金はありません。366 日が経過すると、 pay-as-you-go 価格設定で保存期間の延長が可能になります。これがデフォルトのオプションです。
     - デフォルトの保持期間: 366 日間
     - 最長保持期間: 3,653 日間
   - [7 年間の保持料金] – 1 か月あたり 25 TB を超えるイベントデータを取り込む予定で、最長 7 年間の保存期間が必要な場合に推奨されます。データの保持は取り込み料金に含まれており、追加料金は発生しません。
     - デフォルトの保持期間: 2,557 日間
     - 最長保持期間: 2,557 日間
6. イベントデータストアの保存期間を日数単位で指定します。保持期間は、1 年間の延長可能な保持料金オプションの場合で 7 日から 3,653 日 (約 10 年)、7 年間の保持料金オプションでは 7 日から 2,557 日 (約 7 年) に設定できます。

   CloudTrail Lake は、イベントが指定された保存期間内かどうかをチェックして、イベントを保持するかどうかを決定します。`eventTime`例えば、保存期間を 90 日に指定した場合、90 CloudTrail `eventTime` 日以上経過したイベントは削除されます。

   > **Note**
   >
   > CloudTrail `eventTime`指定した保存期間より古いイベントはコピーされません。

適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントをイベントデータストアに保持したい日数 (保持期間 = *oldest-event-in-days*+ *number-days-to-retain*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

7. (オプション) [暗号化] で、独自の KMS キーを使用してイベントデータストアを暗号化するかどうかを選択します。デフォルトでは、イベントデータストア内のすべてのイベントは、 AWS ユーザーが所有および管理する KMS CloudTrail キーを使用して暗号化されます。

   独自の KMS キーを使用して暗号化を有効にするには、[独自の AWS KMS key を使用する] を選択します。[新規] AWS KMS key を選択して自動的に作成するか、[既存] を選択して既存の KMS キーを使用します。「KMS エイリアスの入力」 で、エイリアスを次の形式で指定します。`alias/` *MyAliasName*独自の KMS キーを使用するには、KMS キーポリシーを編集して、CloudTrail口グの暗号化と復号化を許可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。AWS KMS の主要ポリシーの設定 CloudTrail CloudTrail AWS KMS マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   独自の KMS キーを使用すると、 AWS KMS 暗号化と復号化にコストがかかります。イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。

   > **Note**
   >
   > AWS Key Management Service 組織のイベントデータストアの暗号化を有効にするには、管理アカウント用の既存の KMS キーを使用する必要があります。

8. (オプション) Amazon Athena を使用してイベントデータに対しクエリを実行する場合は、[Lake クエリフェデレーション] で [有効] を選択します。フェデレーションを使用すると、 AWS Glue データカタログ内のイベントデータストアに関連するメタデータを表示したり、Athena のイベントデータに対して SQL クエリを実行したりできます。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンは、クエリするデータを検索、読み

取り、処理する方法を知ることができます。詳細については、「イベントデータストアのフェデレーション」を参照してください。

Lake クエリフェデレーションを有効にするするには、[有効] を選択した後に、以下の操作を実行します。

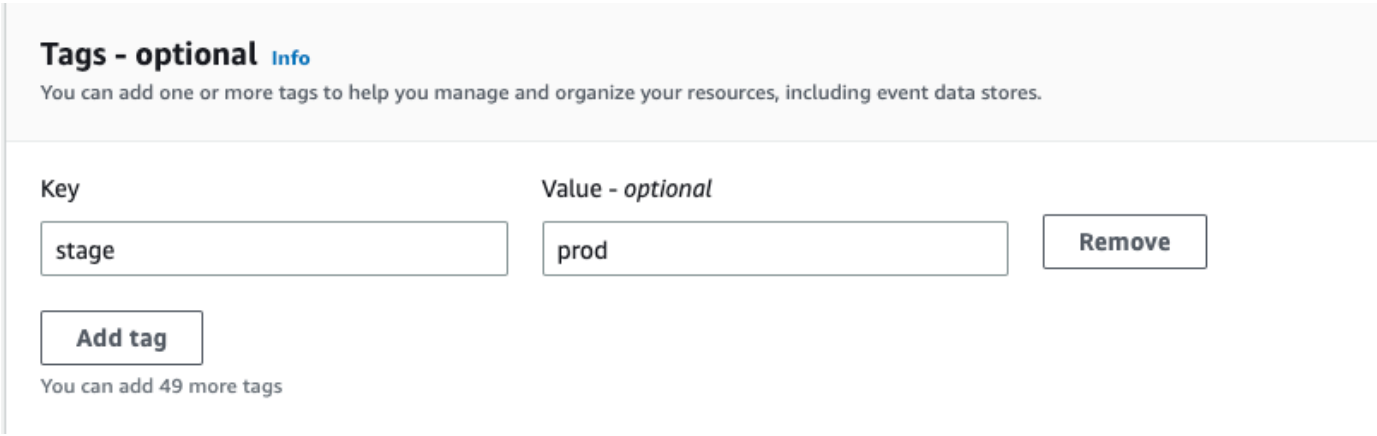
a. 新しいロールを作成するか、既存の IAM ロールを使用するかを選択します。 AWS Lake Formation は、このロールを使用してフェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 CloudTrail 必要な権限を持つロールが自動的に作成されます。既存のロールを選択する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。

b. 新しいロールを作成する場合は、そのロールを識別する名前を指定します。

c. 既存のロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。

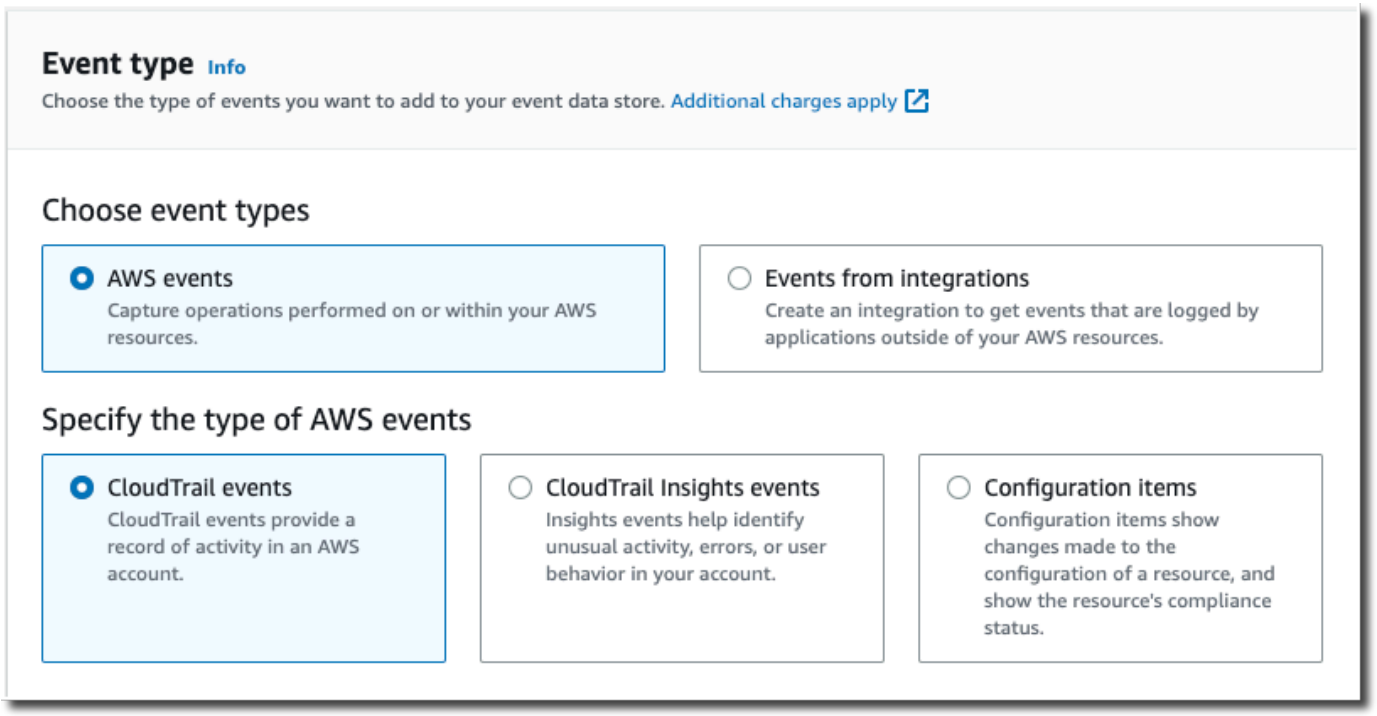
9. (オプション) [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) をデータセットに追加します。 CloudTrail タグはイベントデータストアを識別するのに役立ちます。例えば、**stage** という名前の **prod** という値のタグをアタッチできます。タグを使用して、イベントデータストアへのアクセスを制限できます。タグを使用して、イベントデータストアのクエリコストと取り込みコストを追跡することもできます。

   タグを使用してコストを追跡する方法については、「 CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でタグを使用する方法については AWS、『リソースへのタグ付け』ユーザーガイドの「 AWS AWS リソースのタグ付け」を参照してください。



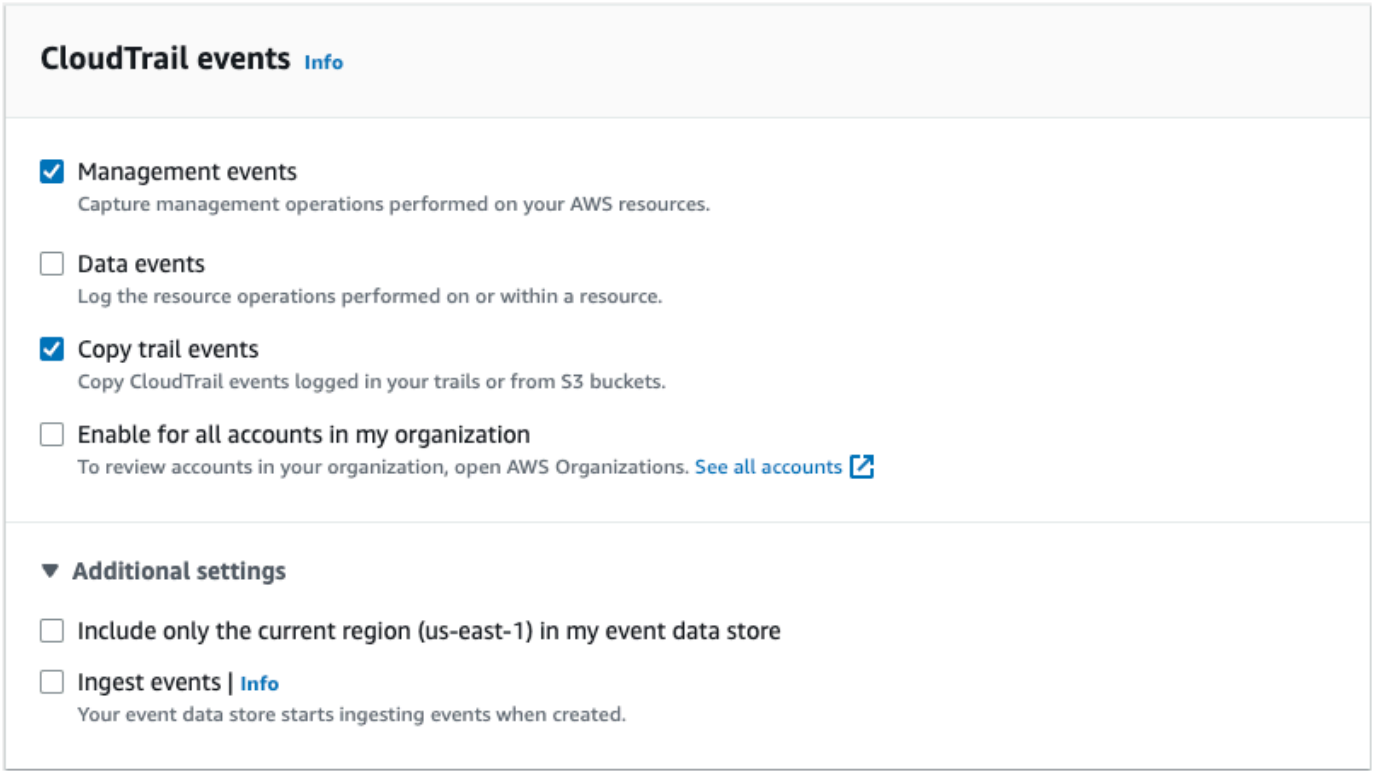
10. [次へ] を選択して、イベントデータストアを設定します。

11. [イベントの選択]ページで、[イベントタイプ] はデフォルトの選択のままにします。



12. CloudTrail イベントについては、[管理イベント] を選択したままにし、[トレイルイベントのコピー] を選択します。この例では、イベントデータストアは過去のイベントの分析にのみ使用し、将来のイベントは取り込まないため、イベントタイプを考慮する必要はありません。

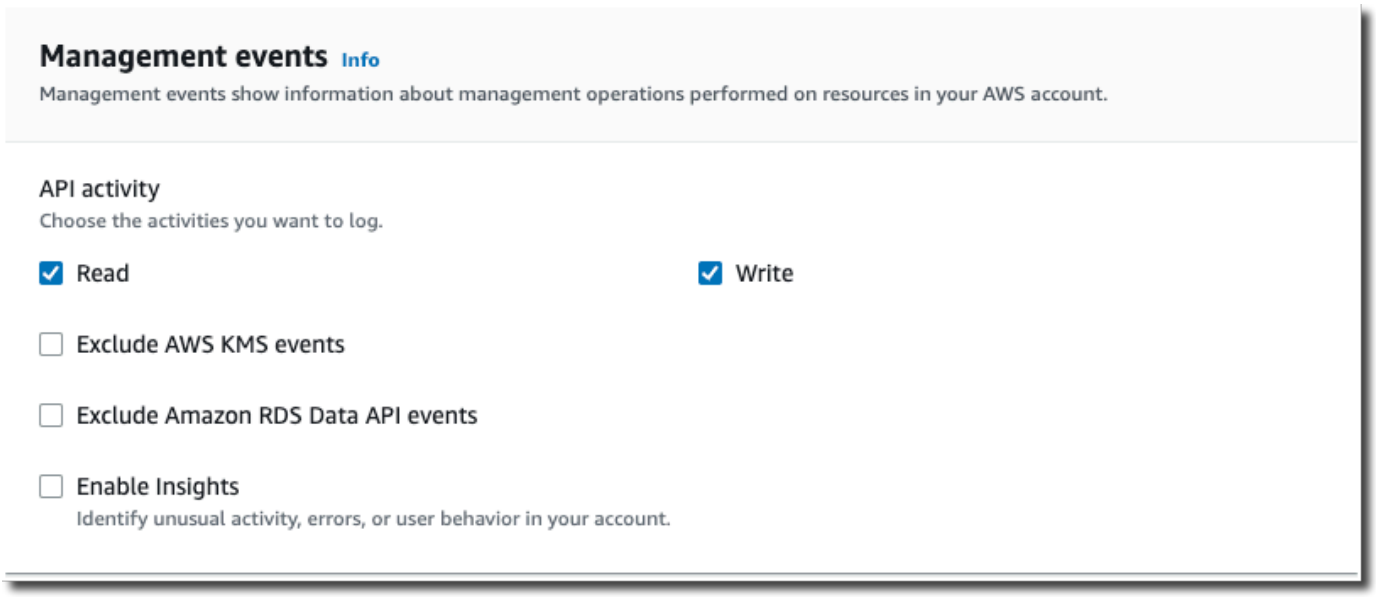
    既存の証跡を置き換えるためにイベントデータストアを作成する場合は、証跡と同じイベントセレクターを選択して、イベントデータストアが同じイベント範囲であることを確認してください。



13. 組織のイベントデータストアの場合は、[組織内の全アカウントで有効にする] を選択します。このオプションは、 AWS Organizations でアカウントを設定していない場合は変更できません。

> **Note**
>
> 組織のイベントデータストアを作成する場合、組織イベントデータストアに証跡イベントをコピーできるのは管理アカウントだけなので、組織の管理アカウントでサインインする必要があります。

14. [追加設定] で、[イベントの取り込み] を選択解除します。この例では、コピーされたイベントのクエリのみを扱い、イベントデータストアでは未来のイベントを取り込まないためです。デフォルトでは、 AWS リージョン イベントデータストアはすべてのイベントを収集し、作成時にイベントの取り込みを開始します。
15. [管理イベント] は、デフォルト設定のままにします。



16. [証跡イベントのコピー] 領域で、以下の手順を完了してください。

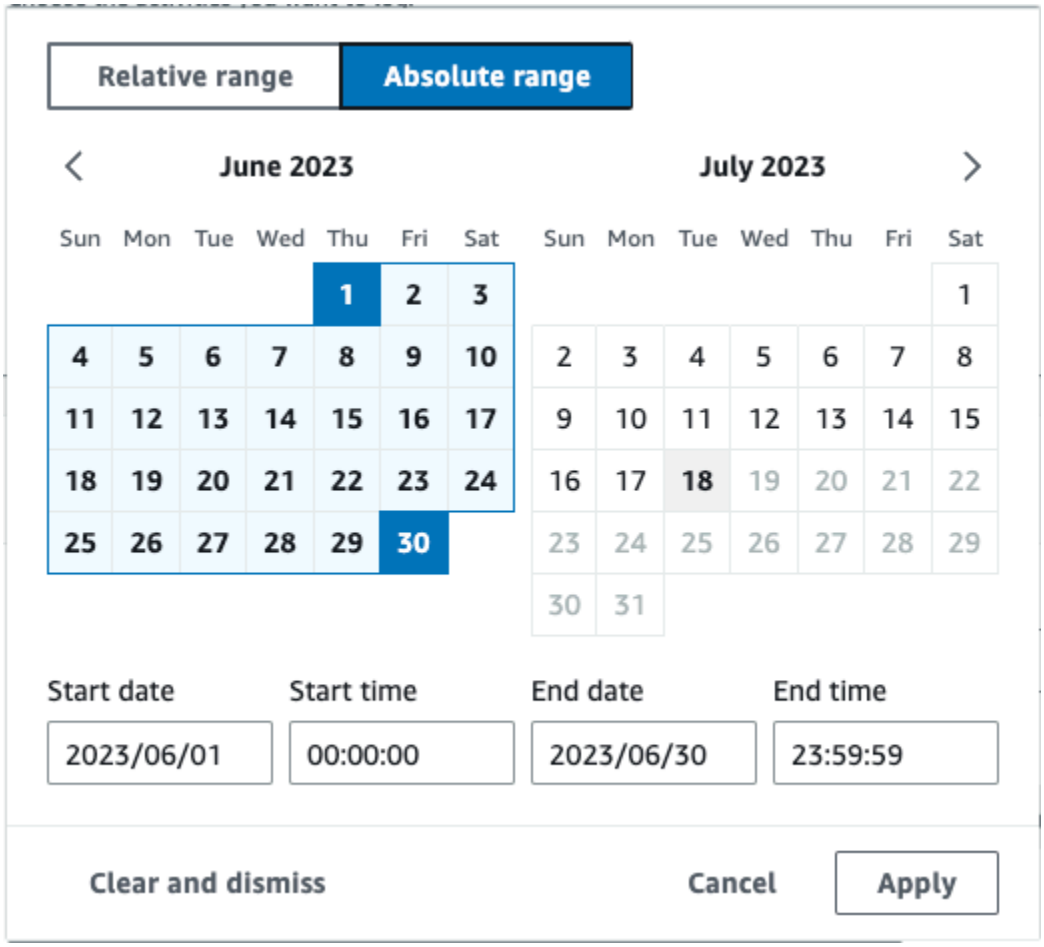
    a. コピーするトレイルを選択します。この例では、*management-events* という名前の証跡を扱います。

       デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、`CloudTrail`他のサービスのプレフィックスをチェックしません。 AWS CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、[Enter S3 URI] を選択し、[Browse S3] を選択してプレフィックスを参照します。トレイルのソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでデータの復号化が許可されていることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。KMS キーポリシーの更新の詳細については、「ソース S3 バケット内のデータを復号化するための KMS キーポリシー」を参照してください。

    b. イベントをコピーする時間範囲を選択してください。 CloudTrail トレイルイベントをコピーする前に、プレフィックスとログファイル名をチェックして、選択した開始日と終了日の間の日付が名前に含まれていることを確認します。[Relative range] (相対範囲) または[Absolute range] (絶対範囲) を選択することができます。ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の時間範囲を選択します。

- [相対範囲] を選択すると、過去 6 か月、1 年、2 年、7 年間に記録されたイベントをコピーするか、またはカスタム範囲をコピーするかを選択できます。 CloudTrail 選択した期間内に記録されたイベントをコピーします。
- [絶対範囲] を選択すると、特定の開始日と終了日を選択できます。 CloudTrail 選択した開始日と終了日の間に発生したイベントをコピーします。

この例では、[絶対範囲] を選択し、6 月全体を選択します。

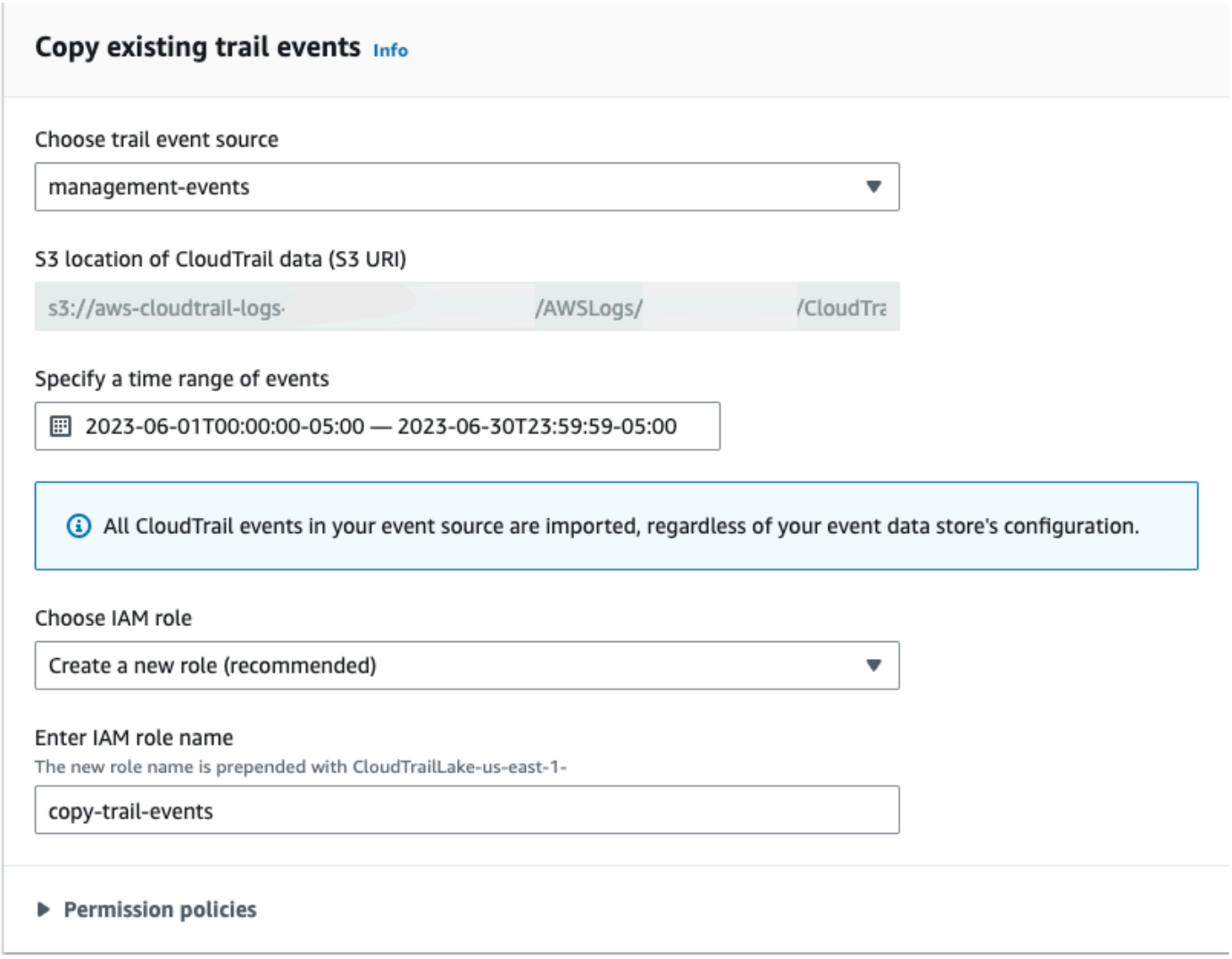


c. [Permissions] (アクセス許可) については、以下の IAM ロールのオプションから選択します。既存の IAM ロールを選択する場合は、IAM ロールポリシーが必要なアクセス許可を提供していることを確認してください。IAM ロールの許可の更新の詳細については、「証跡イベントをコピーするための IAM 許可」を参照してください。

- [Create a new role (recommended)] (新しいロールの作成 (推奨)) を選択して、新しい IAM ロールを作成します。[IAM ロール名を入力] には、ロールの名前を入力します。CloudTrail この新しいロールに必要な権限が自動的に作成されます。

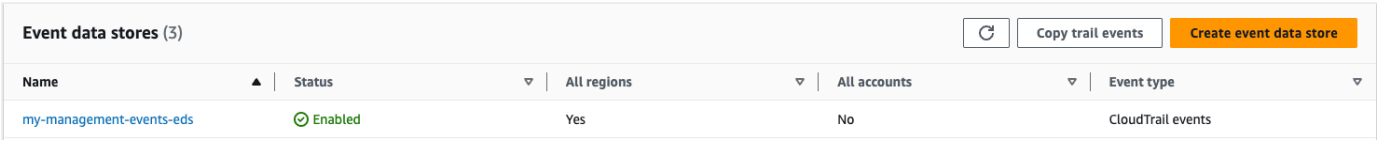
- リストにないカスタム IAM ロールを使用するには、[カスタム IAM ロール ARN を使用] を選択します。[Enter IAM role ARN] (IAM ロールの ARN を入力) で、IAM ARN を入力します。
- ドロップダウンリストから既存の IAM ロールを選択します。

この例では、[新しいロールを作成し (推奨)] を選択し、**copy-trail-events** と名前をつけます。



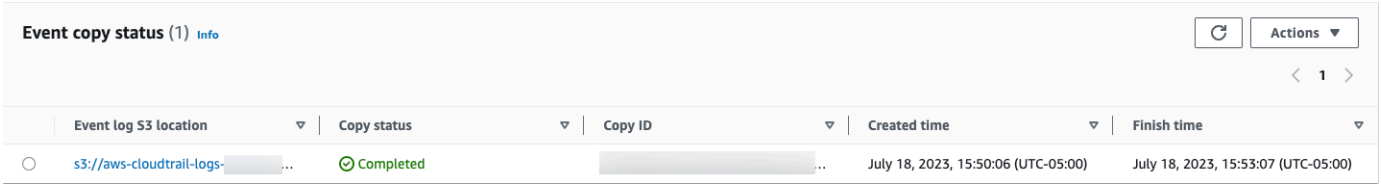
17. [Next] (次へ) を選択して、選択内容を確認します。
18. [Review and create] (確認と作成) ページで、選択内容を確認します。セクションを変更するには、[Edit] (編集) をクリックします。イベントデータストアを作成する準備が整ったら、[Create event data store] (イベントデータストアの作成) をクリックします。

19. 新しいイベントデータストアが、[イベントデータストア] ページの [イベントデータストア] テーブルに表示されます。

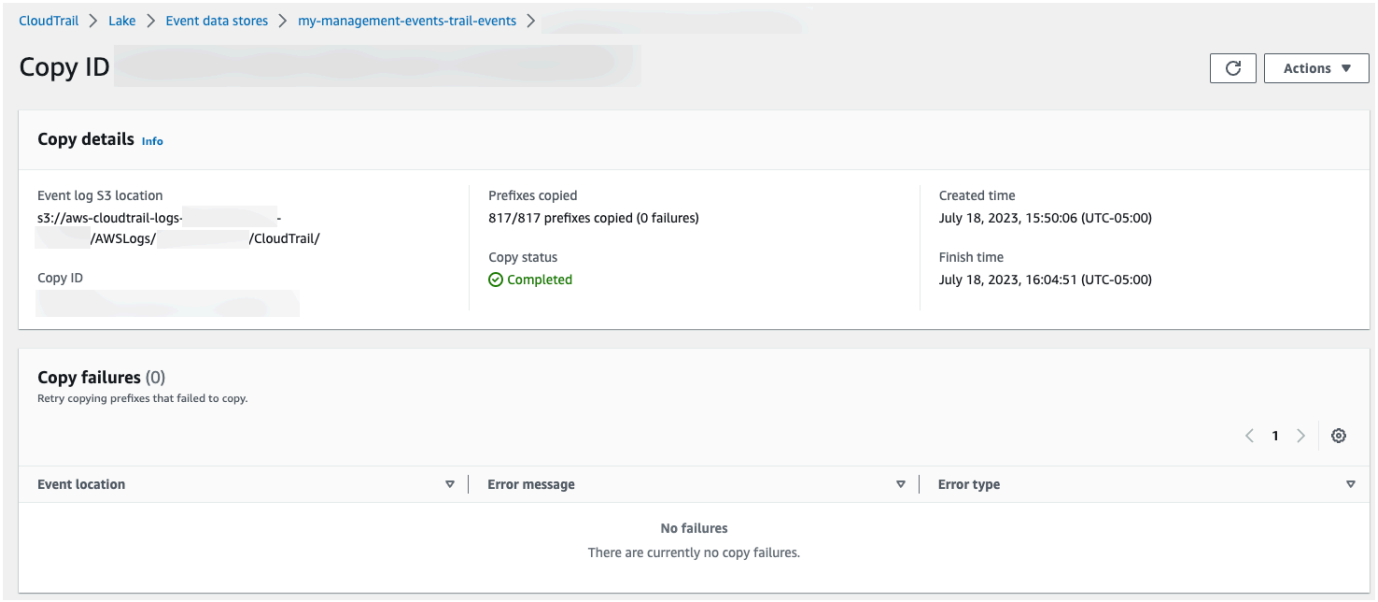


20. イベントデータストア名を選択すると、詳細ページが表示されます。詳細ページには、イベントデータストアの詳細とコピーのステータスが表示されます。イベントのコピーステータスは、[イベントコピーのステータス] 領域に表示されます。

    証跡イベントのコピーが完了すると、その[Copy status] (コピー ステータス) は、エラーがない場合は[Completed] (完了) に設定され、エラーが発生した場合は[Failed] (失敗) に設定されます。



21. コピーの詳細を表示するには、[イベントログ S3 の場所] 列を選択するか、[アクション] メニューで [詳細を表示] を 選択します。証跡イベントコピーの詳細を表示する方法については、「イベントコピーの詳細」を参照してください。



22. [コピー失敗] 領域には、証跡イベントのコピー時に発生したすべてのエラーが表示されます。[Copy status] (コピーのステータス) が[Failed] (失敗) の場合は、[Copy failures] (コピーの失敗) に示されているエラーを修正し、[Retry copy] (コピーの再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。

イベントデータストアのフェデレーション

イベントデータストアをフェデレーションすると、データカタログ 内の AWS Glue イベントデータストアに関連付けられたメタデータを表示したり、 にデータカタログを登録したり AWS Lake Formation、Amazon Athena を使用してイベントデータに対して SQL クエリを実行したりできます。 AWS Glue Data Catalog に保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。

CloudTrail コンソール、 AWS CLI、または EnableFederation API オペレーションを使用してフェデレーションを有効にできます。Lake クエリフェデレーションを有効にすると、 CloudTrail は という名前のマネージドデータベース `aws:cloudtrail` (データベースがまだ存在しない場合) と、AWS Glue Data Catalog にマネージドフェデレーションテーブルを作成します。イベントデータストア ID はテーブル名に使用されます。 は、フェデレーションロール ARN とイベントデータストアを CloudTrail に登録します。これはAWS Lake Formation、 AWS Glue Data Catalog 内のフェデレーションリソースのきめ細かなアクセス制御を許可するサービスです。

Lake クエリフェデレーションを有効にするには、新しい IAM ロールを作成するか、既存のロールを選択する必要があります。Lake Formation はこのロールを使用して、フェデレーションイベントデータストアのアクセス許可を管理します。 CloudTrail コンソールを使用して新しいロールを作成すると、 はロールに必要なアクセス許可 CloudTrail を自動的に作成します。既存のロールを選択する場合は、ロールが最小限のアクセス許可を提供していることを確認してください。

CloudTrail コンソール、、または DisableFederation API オペレーションを使用して AWS CLIフェデレーションを無効にすることができます。フェデレーションを無効にすると、 CloudTrail は AWS Glue、 AWS Lake Formation、および Amazon Athena との統合を無効にします。Lake クエリフェデレーションを無効にした後は、Athena でイベントデータをクエリできなくなります。フェデレーションを無効にすると CloudTrail Lake データは削除されず、引き続き CloudTrail Lake でクエリを実行できます。

CloudTrail Lake イベントデータストアのフェデレーションには CloudTrail 料金はかかりません。Amazon Athena でクエリを実行するにはコストがかかります。Athena の料金の詳細については、「Amazon Athena の料金」を参照してください。

AWS CloudTrail Lake と Amazon Athena を使用してアクティビティログを分析する

トピック

- 考慮事項
- フェデレーションに必要なアクセス許可

- Lake クエリフェデレーションを有効にする
- Lake クエリフェデレーションを無効にする
- を使用した CloudTrail Lake フェデレーションリソースの管理 AWS Lake Formation

考慮事項

イベントデータストアのフェデレーションを行う場合は、以下の要素を考慮してください。

- CloudTrail Lake イベントデータストアのフェデレーションには CloudTrail 料金はかかりません。Amazon Athena でクエリを実行するにはコストがかかります。Athena の料金の詳細については、「Amazon Athena の料金」を参照してください。
- Lake Formation は、フェデレーションリソースのアクセス許可を管理するために使用されます。フェデレーションロールを削除するか、Lake Formation または からリソースへのアクセス許可を取り消す場合 AWS Glue、Athena からクエリを実行することはできません。Lake Formation 操作の詳細については、を使用した CloudTrail Lake フェデレーションリソースの管理 AWS Lake Formation を参照してください。
- Lake Formation に登録されたデータのクエリに Amazon Athena を使用するユーザーには、`lakeformation:GetDataAccess` アクションを許可する IAM アクセス許可ポリシーが必要です。 AWS マネージドポリシー: はこのアクションAmazonAthenaFullAccessを許可します。インラインポリシーを使用する場合は、このアクションを許可するように許可ポリシーを更新してください。詳細については、「Lake Formation と Athena ユーザー許可の管理」を参照してください。
- Athena のフェデレーションテーブルにビューを作成するには、`aws:cloudtrail` 以外の送信先データベースが必要です。これは、`aws:cloudtrail`データベースが によって管理されているためです CloudTrail。
- Amazon でデータセットを作成するには QuickSight、カスタム SQL を使用する オプションを選択する必要があります。詳細については、「Amazon Athena データを使用したデータセットの作成」を参照してください。
- フェデレーションが有効になっている場合、イベントデータストアを削除することはできません。フェデレーションイベントデータストアを削除するには、まず、フェデレーションを無効化し、終了保護が有効になっている場合はこれも無効にする必要があります。
- 組織のイベントデータストアには、次の考慮事項が適用されます。
  - 組織のイベントデータストアでフェデレーションを有効にできるのは、委任された管理者アカウントの 1 つ、または管理アカウントだけです。他の委任された管理者アカウントも、Lake Formation データ共有機能を使用して情報をクエリおよび共有することはできます。

- すべての委任された管理者アカウントも組織の管理アカウントもフェデレーションを無効にできます。

フェデレーションに必要なアクセス許可

イベントデータストアのフェデレーションを行う前に、フェデレーションロールとフェデレーションの有効化と無効化に必要なすべてのアクセス許可があることを確認してください。フェデレーションロールのアクセス許可を更新する必要があるのは、既存の IAM ロールを選択してフェデレーションを有効にする場合だけです。 CloudTrail コンソールを使用して新しい IAM ロールを作成することを選択した場合、 はロールに必要なすべてのアクセス許可 CloudTrail を提供します。

トピック

イベントデータストアのフェデレーションのための IAM アクセス許可

フェデレーションを有効にする際に、新しい IAM ロールを作成するか、既存の IAM ロールを使用するか選択できます。新しい IAM ロールを選択すると、 は必要なアクセス許可を持つ IAM ロール CloudTrail を作成し、ユーザー側でそれ以上のアクションは必要ありません。

既存のロールを選択する場合は、IAM ロールのポリシーがフェデレーションを有効にするために必要なアクセス許可を付与していることを確認してください。このセクションでは、必要な IAM ロールのアクセス許可と信頼ポリシーの例を示します。

次の例は、フェデレーションロールのアクセス許可ポリシーを示しています。最初のステートメントには、`Resource` のイベントデータストアの完全な ARN を指定します。

このポリシーの 2 番目のステートメントにより、Lake Formation は KMS キーで暗号化されたイベントデータストアのデータを復号できます。*`key-region`*、*`account-id`*、*`key-id`* は KMS キーの値に置き換えてください。イベントデータストアが暗号化に KMS キーを使用しない場合は、このステートメントを省略できます。

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

```
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:eds-region:account-id:eventdatastore/eds-
id"
        },
        {
          "Sid": "LakeFederationKMSDecryptAccess",
          "Effect": "Allow",
          "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:key-region:account-id:key/key-id"
      }
    ]
}
```

次の例は IAM 信頼ポリシーを示しています。これにより、 AWS Lake Formation は、フェデレーションイベントデータストアのアクセス許可を管理する IAM ロールを引き受けることができます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

フェデレーションの有効化に必要なアクセス許可

次のポリシーの例は、イベントデータストアでフェデレーションを有効にするために最低限必要なアクセス許可を提供します。このポリシーにより CloudTrail 、 はイベントデータストアでフェデレーションを有効に AWS Glue し、 AWS Glue Data Catalog でフェデレーションリソースを作成し、リソース登録 AWS Lake Formation を管理できます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to enable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow access to the federation role",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::region:role/federation-role-name"
        },
        {
            "Sid": "Allow AWS Glue to create the federated resources in the Data
 Catalog",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id",
                "arn:aws:glue:region:account-id:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "Allow Lake Formation to manage resource registration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
```

```
}
```

フェデレーションの無効化に必要なアクセス許可

次のポリシーの例は、イベントデータストアでフェデレーションを無効にするために最低限必要なリソースを提供します。このポリシーにより、 CloudTrail はイベントデータストアでのフェデレーションを無効に AWS Glue し、 AWS Glue Data Catalog 内のマネージドフェデレーションテーブルを削除し、Lake Formation はフェデレーションリソースの登録を解除できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow CloudTrail to disable federation on the event data store",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id"
        },
        {
            "Sid": "Allow AWS Glue to delete the managed federated table from the AWS
 Glue Data Catalog",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/aws:cloudtrail",
                "arn:aws:glue:region:account-id:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "Allow Lake Formation to deregister the resource",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:region:account-id:catalog:account-id"
        }
    ]
}
```

Lake クエリフェデレーションを有効にする

Lake クエリフェデレーションを有効にするには、 CloudTrail コンソール AWS CLI、、または EnableFederation API オペレーションを使用します。Lake クエリフェデレーションを有効にする

と、 は という名前のマネージドデータベース aws:cloudtrail (データベースがまだ存在しない場合) と、 AWS Glue Data Catalog にマネージドフェデレーションテーブル CloudTrail を作成します。イベントデータストア ID はテーブル名に使用されます。 は、フェデレーションロール ARN とイベントデータストアを CloudTrail に登録します。これはAWS Lake Formation、 AWS Glue Data Catalog 内のフェデレーションリソースのきめ細かなアクセス制御を許可するサービスです。

このセクションでは、 CloudTrail コンソールと を使用してフェデレーションを有効にする方法について説明します AWS CLI。

CloudTrail console

以下の手順では、既存のイベントデータストアで Lake クエリフェデレーションを有効にする方法を示します。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. 更新するイベントデータストアを選択します。データストアの [詳細] ページが開きます。
4. [Lake クエリフェデレーション] で、[編集] を選択し、[有効化] を選択します。
5. 新しい IAM ロールを作成するか、既存のロールを使用するか選択します。新しいロールを作成すると、 は必要なアクセス許可を持つロール CloudTrail を自動的に作成します。既存のロールを使用する場合は、そのロールのポリシーが必要最小限のアクセス許可を提供していることを確認してください。
6. 新しい IAM ロールを作成する場合は、ロールの名前を入力します。
7. 既存の IAM ロールを使用している場合は、使用したいロールを選択します。ロールは、ご自身のアカウント内に存在する必要があります。
8. [変更を保存] を選択します。[フェデレーションステータス] は Enabled に変わります。

AWS CLI

フェデレーションを有効にするには、必須パラメータの --event-data-store と --role を指定して aws cloudtrail enable-federation コマンドを実行します。--event-data-store には、イベントデータストア ARN (または ARN の ID サフィックス) を指定します。--role には、フェデレーションロールの ARN を指定します。ロールはアカウントに存在し、必要最小限のアクセス許可が付与されている必要があります。

```
aws cloudtrail enable-federation
```

```
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
--role arn:aws:iam::account-id:role/federation-role-name
```

この例は、管理アカウントのイベントデータストアの ARN と、委任された管理者アカウントのフェデレーションロールの ARN を指定することで、委任された管理者が組織のイベントデータストアのフェデレーションを有効にする方法を示しています。

```
aws cloudtrail enable-federation
--event-data-store arn:aws:cloudtrail:region:management-account-
id:eventdatastore/eds-id
--role arn:aws:iam::delegated-administrator-account-id:role/federation-role-name
```

Lake クエリフェデレーションを無効にする

CloudTrail コンソール、、または DisableFederation API オペレーションを使用して AWS CLIフェデレーションを無効にすることができます。フェデレーションを無効にすると、 は AWS Glue、 AWS Lake Formation、および Amazon Athena との統合を CloudTrail 無効にします。Lake クエリフェデレーションを無効にした後は、Athena でイベントデータをクエリできなくなります。フェデレーションを無効にすると CloudTrail Lake データは削除されず、引き続き CloudTrail Lake でクエリを実行できます。

このセクションでは、 CloudTrail コンソールと を使用してフェデレーションを無効にする方法について説明します AWS CLI。

CloudTrail console

以下の手順では、既存のイベントデータストアで Lake クエリフェデレーションを無効にする方法を示します。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. 更新するイベントデータストアを選択します。データストアの [詳細] ページが開きます。
4. [Lake クエリフェデレーション] で、[編集] を選択し、[無効化] を選択します。
5. [変更を保存] を選択します。[フェデレーションステータス] は `Disabled` に変わります。

AWS CLI

イベントデータストアでのフェデレーションを無効にするには、aws cloudtrail disable-federation コマンドを実行します。イベントデータストアは、イベントデータストア ARN、または ARN の ID サフィックスを受け入れる `--event-data-store` によって指定されます。

```
aws cloudtrail disable-federation
--event-data-store arn:aws:cloudtrail:region:account-id:eventdatastore/eds-id
```

> **Note**
>
> これが組織のイベントデータストアである場合は、管理アカウントのアカウント ID を使用します。

を使用した CloudTrail Lake フェデレーションリソースの管理 AWS Lake Formation

イベントデータストアをフェデレーションすると、 はフェデレーションロール ARN とイベントデータストアを CloudTrail に登録します。このサービスは AWS Lake Formation、 AWS Glue Data Catalog 内のフェデレーションリソースのきめ細かなアクセス制御を許可するサービスです。このセクションでは、Lake Formation を使用して CloudTrail Lake フェデレーションリソースを管理する方法について説明します。

フェデレーションを有効にすると、 は AWS Glue Data Catalog に次のリソース CloudTrail を作成します。

- マネージドデータベース – account. CloudTrail manages データベース`aws:cloudtrail`ごとに 1 つの名前のデータベース CloudTrail を作成します。でデータベースを削除または変更することはできません AWS Glue。
- マネージドフェデレーティッドテーブル – フェデレーティッドイベントデータストアごとに 1 つのテーブル CloudTrail を作成し、テーブル名にイベントデータストア ID を使用します。CloudTrail はテーブルを管理します。のテーブルを削除または変更することはできません AWS Glue。テーブルを削除するには、イベントデータストアのフェデレーションを無効化する必要があります。

フェデレーションリソースへのアクセスの制御

2 つのアクセス許可方式のいずれかを使用して、マネージドデータベースとテーブルへのアクセスを制御できます。

- IAM のみのアクセス制御 – IAM のみのアクセス制御では、必要な IAM アクセス許可が付与されたアカウントのすべてのユーザーに、すべての Data Catalog リソースへのアクセス権が付与されます。が IAM と AWS Glue どのように連携するかについては、「 が IAM と AWS Glue どのように連携するか」を参照してください。

  Lake Formation コンソールでは、この方式が [Use only IAM access control] (IAM アクセスコントロールのみを使用する) として表示されます。

  > **Note**
  >
  > データフィルターを作成して他の Lake Formation 機能を使用する場合は、Lake Formation アクセス制御を使用する必要があります。

- Lake Formation のアクセス制御 – この方式には以下の利点があります。
  - データフィルターを作成することで、列レベル、行レベル、およびセルレベルのセキュリティを実装することができます。
  - データベースとテーブルは、Lake Formation の管理者と、データベースとリソースの作成者にのみ表示されます。別のユーザーがこれらのリソースにアクセスする必要がある場合は、明示的に Lake Formation アクセス許可を使用してアクセス権を付与する必要があります。

アクセス制御の詳細については、「細粒度のアクセスコントロールのための方式」を参照してください。

フェデレーションリソースのアクセス許可方式の決定

初めてフェデレーションを有効にすると、 は Lake Formation データレイク設定を使用してマネージドデータベースとマネージドフェデレーションテーブル CloudTrail を作成します。

フェデレーション CloudTrail を有効にすると、マネージドデータベースとマネージドフェデレーションテーブルに使用しているアクセス許可メソッドを、それらのリソースのアクセス許可をチェックすることで確認できます。リソースに対して `IAM_ALLOWED_PRINCIPALS` に `ALL` (Super) の設定がある場合、リソースは IAM アクセス許可によってのみ管理されます。設定がない場合、リソースは Lake Formation アクセス許可によって管理されます。Lake Formation のアクセス許可の詳細については、「Lake Formation の許可リファレンス」を参照してください。

マネージドデータベースとマネージドフェデレーションテーブルのアクセス許可方式は異なる場合があります。例えば、データベースとテーブルの値を確認すると、次のようになっている場合があります。

- データベースでは、ALL (Super) を IAM_ALLOWED_PRINCIPALS に割り当てた値がアクセス許可に存在し、データベースに対して IAM のみのアクセス制御を使用していることを示しています。
- テーブルでは、ALL (Super) を IAM_ALLOWED_PRINCIPALS に割り当てた値が存在せず、Lake Formation アクセス許可によるアクセス制御を示しています。

Lake Formation のフェデレーションリソースの IAM_ALLOWED_PRINCIPALS アクセス許可に ALL (Super) を追加または削除することで、いつでもアクセス方式を切り替えることができます。

Lake Formation を使用したクロスアカウント共有

このセクションでは、Lake Formation を使用してマネージドデータベースとマネージドフェデレーションテーブルをアカウント間で共有する方法について説明します。

次の手順を実行すると、マネージドデータベースをアカウント間で共有できます。

1. クロスアカウントデータ共有のバージョンをバージョン 4 に更新します。
2. データベースに IAM_ALLOWED_PRINCIPALS への Super アクセス許可がある場合は削除して、Lake Formation アクセス制御に切り替えます。
3. データベースで、外部のアカウントに Describe アクセス許可を付与します。
4. Data Catalog リソースが と共有 AWS アカウント されており、アカウントが共有アカウントと同じ AWS 組織内にない場合は、 AWS Resource Access Manager （ AWS RAM) からのリソース共有の招待を受け入れます。詳細については、AWS 「RAM からのリソース共有の招待を受け入れる」を参照してください。

これらの手順を完了すると、データベースは外部アカウントに表示されるはずです。デフォルトでは、データベースを共有しても、データベース内のどのテーブルへのアクセス権も付与されません。

次の手順を実行すると、すべてまたは個別のマネージドフェデレーションテーブルを外部アカウントと共有できます。

1. クロスアカウントデータ共有のバージョンをバージョン 4 に更新します。
2. テーブルに IAM_ALLOWED_PRINCIPALS への Super アクセス許可がある場合は削除して、Lake Formation アクセス制御に切り替えます。

3. (オプション) 任意のデータフィルターを指定して列や行を制限します。
4. テーブルで、外部のアカウントに `Select` アクセス許可を付与します。
5. Data Catalog リソースが と共有 AWS アカウント されており、アカウントが共有アカウントと同じ AWS 組織内にない場合は、 AWS Resource Access Manager （ AWS RAM) からのリソース共有の招待を受け入れます。組織の場合、RAM 設定を使用して自動承諾できます。詳細については、AWS 「RAM からのリソース共有の招待を受け入れる」を参照してください。
6. これで、テーブルが表示されるはずです。このテーブルで Amazon Athena クエリを有効にするには、共有テーブルとのリソースリンクをこのアカウントで作成します。

所有アカウントは、Lake Formation から外部アカウントのアクセス許可を削除するか、 でフェデレーションを無効にすることで、いつでも共有を取り消すことができます CloudTrail。

組織のイベントデータストア

で組織を作成した場合は AWS Organizations、その組織内のすべてのイベントを記録する組織イベントデータストアを作成できます。 AWS アカウント 組織イベントデータストアは AWS リージョン、すべての地域に適用することも、現在の地域に適用することもできます。組織のイベントデータストアを使用して、 AWS外からイベントを収集することはできません。

組織イベントデータストアは、管理アカウントまたは委任管理者アカウントのいずれかを使用して作成できます。委任された管理者が組織のイベントデータストアを作成しても、組織のイベントデータストアは組織の管理アカウントに存在します。これは、管理アカウントがすべての組織リソースの所有権を保持するためです。

組織の管理アカウントは、アカウントレベルのイベントデータストアを更新して組織に適用できます。

組織のイベントデータストアが組織への適用として指定された場合は、組織内のすべてのメンバーアカウントに自動的に適用されます。メンバーアカウントは、組織のイベントデータストアを表示することも、これを変更または削除することもできません。デフォルトでは、メンバーアカウントは組織のイベントデータストアにアクセスできず、組織のイベントデータストアに対してクエリを実行することもできません。

次の表は、組織内の管理アカウントと委任管理者アカウントの機能を示しています。 AWS Organizations

機能	管理アカウント	委任された管理者アカウント
委任された管理者アカウントを登録または削除する。	はい	いいえ
AWS CloudTrail AWS Config イベントまたは構成項目用の組織イベントデータストアを作成します。	はい	はい
組織のイベントデータストアでの Insights の有効化。	はい	いいえ
組織のイベントデータストアの更新。	はい	あり [1]
組織のイベントデータストアで Lake クエリフェデレーションを有効にする。[2]	はい	はい
組織のイベントデータストアでの Lake クエリフェデレーションの無効化。	はい	はい
組織のイベントデータストアの削除。	はい	はい
イベントデータストアに証跡イベントをコピーする。	はい	いいえ
組織のイベントデータストアでのクエリ実行。	はい	はい
組織イベントデータストアの CloudTrail Lake ダッシュボードを表示します。	はい	はい

[1] 組織のイベントデータストアをアカウントレベルのイベントデータストアに変換したり、アカウントレベルのイベントデータストアを組織のイベントデータストアに変換したりできるのは管理アカウントだけです。組織のイベントデータストアは管理アカウントにのみ存在するため、委任された管理者はこれらのアクションを実行できません。組織イベントデータストアをアカウントレベルのイベントデータストアに変換すると、管理アカウントのみがイベントデータストアにアクセスできます。同様に、組織のイベントデータストアに変換できるのは、管理アカウントにあるアカウントレベルのイベントデータストアだけです。

[2]組織のイベントデータストアでフェデレーションを有効にできるのは、委任された管理者アカウントの 1 つ、または管理アカウントだけです。他の委任管理者アカウントは、Lake Formation のデータ共有機能を使用すると、情報をクエリし共有することが可能です。組織の管理アカウントだけでなく委任された管理者アカウントも、フェデレーションを無効化することができます。

組織イベントデータストアを作成します。

組織の管理アカウントまたは委任管理者アカウントは、イベント (管理イベント、 CloudTrail データイベント) AWS Config または構成項目のいずれかを収集する組織イベントデータストアを作成できます。

> **Note**
>
> 組織の管理アカウントのみがトレイルイベントをイベントデータストアにコピーできます。

CloudTrail console

コンソールを使用して組織のイベントデータストアを作成するには

1. 「イベント用イベントデータストアの作成」手順に従って、 CloudTrail CloudTrail 管理イベントまたはデータイベント用の組織イベントデータストアを作成します。

   または

   「構成項目用のイベントデータストアの作成」手順の手順に従って、 AWS ConfigAWS Config 構成項目用の組織イベントデータストアを作成します。
2. [イベントの選択] ページで、組織内のすべてのアカウントで [有効にする] を選択します。

AWS CLI

組織イベントデータストアを作成するには、create-event-data-store`--organization-enabled`コマンドを実行してオプションを含めます。

AWS CLI `create-event-data-store`以下のコマンド例は、すべての管理イベントを収集する組織イベントデータストアを作成します。 CloudTrail 管理イベントはデフォルトで記録されるため、イベントデータストアがすべての管理イベントをログに記録していて、データイベントをまったく収集していない場合は、高度なイベントセレクターを指定する必要はありません。

```
aws cloudtrail create-event-data-store --name org-management-eds --organization-
enabled
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE6-d493-4914-9182-e52a7934b207",
    "Name": "org-management-eds",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": true,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-16T15:30:50.689000+00:00",
    "UpdatedTimestamp": "2023-11-16T15:30:50.851000+00:00"
}
```

AWS CLI `create-event-data-store`次のコマンド例では、`config-items-org-eds` AWS Config 構成項目を収集するという名前の組織イベントデータストアを作成します。構成項目を収集するには、`eventCategoryConfigurationItem`詳細イベントセレクターでフィールドが等しくなるように指定します。

```
aws cloudtrail create-event-data-store --name config-items-org-eds \
--organization-enabled \
--advanced-event-selectors '[
    {
        "Name": "Select AWS Config configuration items",
```

```
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["ConfigurationItem"] }
        ]
    }
]'
```

アカウントレベルのイベントデータストアを組織に適用します。

組織の管理アカウントは、アカウントレベルのイベントデータストアを変換して組織に適用できます。

CloudTrail console

コンソールを使用してアカウントレベルのイベントデータストアを更新するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. 更新するイベントデータストアを選択します。このアクションで、イベントデータストアの詳細ページが開きます。
4. [General details] で、[Edit] を選択します。
5. 組織内のすべてのアカウントで [有効にする] を選択します。
6. [変更を保存] を選択します。

イベントデータストアの更新に関する追加情報については、を参照してくださいコンソールでイベントデータストアを更新する。

AWS CLI

アカウントレベルのイベントデータストアを更新して組織に適用するには、update-event-data-storeコマンドを実行してオプションを含めます`--organization-enabled`。

```
aws cloudtrail update-event-data-store --region us-east-1 \
--organization-enabled \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下も参照してください。

- 組織の委任された管理者
- CloudTrail 委任された管理者を追加する
- CloudTrail 委任された管理者を削除する

外部のイベントソースとの統合を作成 AWS

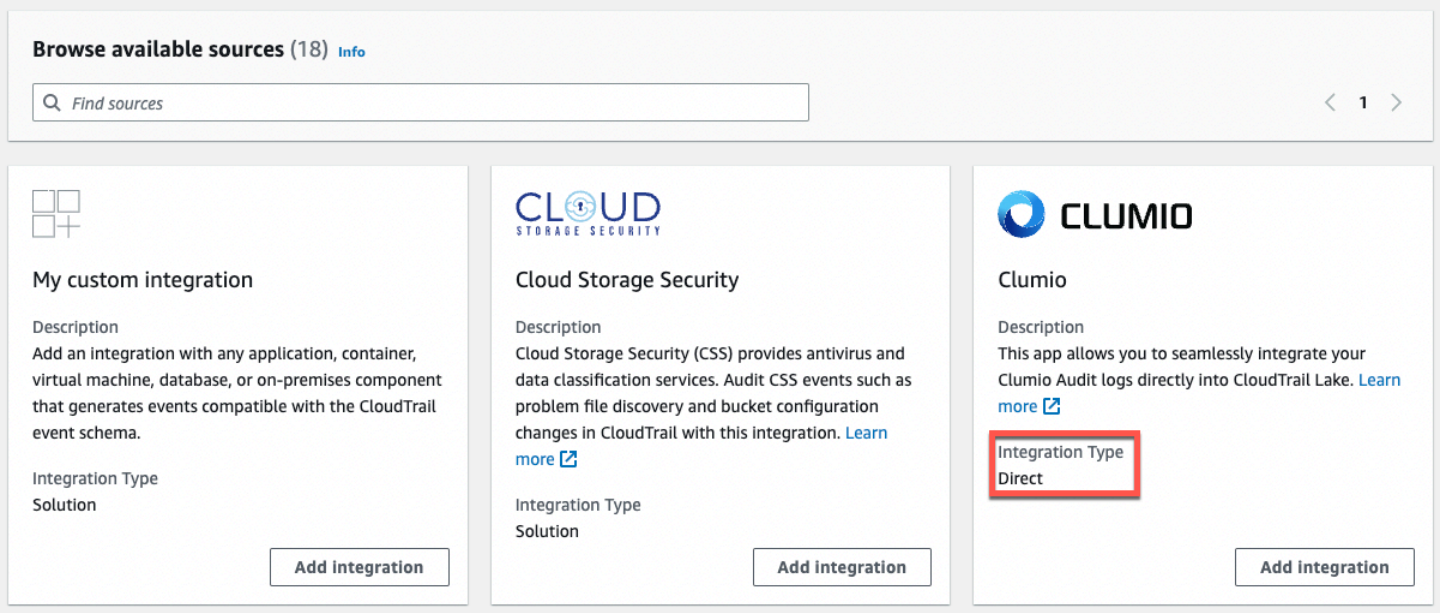
を使用すると CloudTrail 、オンプレミスやクラウド、仮想マシン、コンテナでホストされている社内アプリケーションやSaaSアプリケーションなど、ハイブリッド環境のあらゆるソースからのユーザーアクティビティデータを記録して保存できます。ログ集計やレポート用のツールを複数使用しなくても、このデータを保存、アクセス、分析、トラブルシューティングし、必要なアクションを実行できます。

ソース以外からのアクティビティイベントは、チャネルを使用して CloudTrail、AWS CloudTrail 連携する外部パートナーや独自のソースからLakeにイベントを持ち込むことで機能します。チャネルを作成するときは、チャネルソースから着信するイベントを保存するイベントデータストアを 1 つまたは複数選択します。eventCategory="ActivityAuditLog" イベントを口グ記録するように送信先イベントデータストアが設定されているのであれば、必要に応じて、チャネルの送信先をそれらのストアに変更することが可能です。外部パートナーからのイベント用のチャネルを作成するときは、パートナーまたはソースアプリケーションにチャネル ARN を提供します。チャネルにアタッチされたリソースポリシーにより、ソースはチャネルを介してイベントを送信できます。チャネルにリソースポリシーがない場合、チャネルの PutAuditEvents API を呼び出せるのは、そのチャネルの所有者のみです。

CloudTrail Okta やなど、多くのイベントソースプロバイダーと提携しています。 LaunchDarkly外部のイベントソースとのインテグレーションを作成する場合 AWS、これらのパートナーのいずれかをイベントソースとして選択するか、[マイカスタムインテグレーション] を選択して独自のソースからのイベントをに統合できます。 CloudTrailソースごとに最大 1 つのチャネルが許可されます。

統合には、直接とソリューションの 2 種類が存在します。ダイレクトインテグレーションでは、パートナーが PutAuditEvents API を呼び出して、 AWS アカウントのイベントデータストアにイベントを配信します。ソリューション統合では、 AWS アプリケーションがアカウント内で実行され、アプリケーションが PutAuditEvents API を呼び出して、アカウントのイベントデータストアにイベントを配信します AWS 。

[Integrations] (統合) ページで、[Available sources] (利用可能なソース) タブを開くと、パートナーの [Integration type] (統合タイプ) を表示できます。



はじめに、 CloudTrail パートナーや他のアプリケーションソースからのイベントをコンソールを使って記録するインテグレーションを作成します。

トピック

- CloudTrail コンソールを使用してパートナーとのインテグレーションを作成します。
- コンソールとのカスタムインテグレーションを作成します。
- CloudTrail とのLakeインテグレーションの作成、更新、管理 AWS CLI
- 統合パートナーに関する追加情報
- CloudTrail Lake インテグレーションのイベントスキーマ

CloudTrail コンソールを使用してパートナーとのインテグレーションを作成します。

外部のイベントソースとのインテグレーションを作成する場合 AWS、これらのパートナーのいずれかをイベントソースとして選択できます。パートナーアプリケーションとのインテグレーションを作成する場合、パートナーは、イベントを送信するためにこのワークフローで作成したチャネルの Amazon リソースネーム (ARN) を必要とします。 CloudTrail CloudTrail統合を作成した後は、パートナーからの指示に従い必要なチャネル ARN を提供することで、その統合の設定を完了します。 CloudTrail `PutAuditEvents`パートナーがインテグレーションのチャネルを呼び出した後、インテグレーションはパートナーイベントの取り込みを開始します。

1. AWS Management Console にログインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[統合] を選択します。
3. [Add integration] (統合を追加) ページで、チャネルの名前を入力します。名前には 3～128 の文字数が使用できます。使用できるのは文字、数字、ピリオド、アンダースコア、ダッシュのみです。
4. イベントの取得元である、パートナーアプリケーションソースを選択します。オンプレミスまたはクラウドでホストされている、独自のアプリケーションからのイベントと統合する場合は、[My custom integration] (カスタム統合) を選択します。
5. [Event delivery location] (イベントの配信場所) で、既存のイベントデータストアで以前と同じアクティビティイベントのログ記録を行うか、新しいイベントデータストアを作成するかを選択します。

   イベントデータストアを新しく作成する場合には、イベントデータストアの名前を入力し、料金オプションを選択し、保持期間を日単位で指定します。イベントデータストアは指定された日数分、イベントデータを保存します。

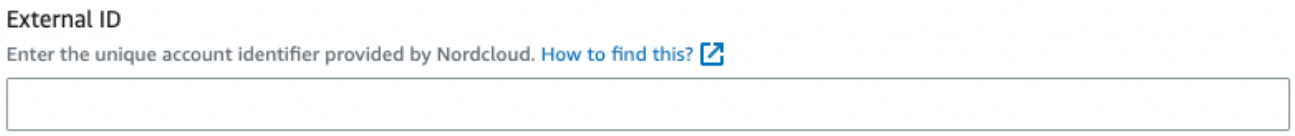
   アクティビティイベントを、既存の (1 つ以上の) イベントデータストアにログ記録する場合は、対象となるイベントデータストアをリストから選択します。イベントデータストアに保存できるのは、アクティビティイベントのみです。コンソール内のイベントタイプは、[Events from integrations] (統合からのイベント) にする必要があります。API 内での `eventCategory` 値は `ActivityAuditLog` にする必要があります。
6. [Resource policy] (リソースポリシー) では、統合のチャネル用にリソースポリシーを設定します。リソースポリシーとは、JSON によるポリシードキュメントです。このドキュメントでは、指定したプリンシパルが対象のリソースにおいて実行できるアクションの種類と、その際の条件を指定します。リソースポリシーでプリンシパルとして定義されているアカウントは、`PutAuditEvents` API を呼び出してイベントをチャネルに配信することができます。IAM ポリシーで `cloudtrail-data:PutAuditEvents` アクションが許可されている場合、リソース所有者はリソースに暗黙的にアクセスできます。

   ポリシーに必要な情報は、統合タイプによって決まります。Direction インテグレーションでは、 AWS パートナーのアカウント ID CloudTrail が自動的に追加され、パートナーから提供された固有の外部 ID を入力するよう求められます。ソリューション統合では、プリンシパルとして少なくとも 1 AWS つのアカウント ID を指定する必要があります。また、代理人の混乱を防ぐために任意で外部 ID を入力することもできます。

> **Note**
>
> チャネルのリソースポリシーを作成しない場合は、そのチャネルの所有者だけが、チャネル内で PutAuditEvents API を呼び出すことができます。

a. 直接統合の場合には、パートナーから提供された外部 ID を入力します。統合パートナーは、一意の外部 ID (アカウント ID やランダムに生成された文字列など) を統合のために提供し、混乱した代理問題を防ぎます。パートナーが一意の外部 ID の作成と提供を責任もって行います。

   [How to find this?] (これを見つけるには?) を選択すると、外部 ID を検索する方法が記載された、パートナー提供のドキュメントを表示できます。



> **Note**
>
> リソースポリシーに外部 ID が含まれているのであれば、PutAuditEvents API に対するすべての呼び出しに、この外部 ID を含める必要があります。ただし、ポリシーで外部 ID が定義されていない場合でも、パートナーは、PutAuditEvents API を呼び出して externalId パラメータを指定することができます。

b. ソリューション統合では、「 AWS アカウントを追加」を選択して、 AWS ポリシーにプリンシパルとして追加するアカウント ID を指定します。

7. (オプション) [Tag] (タグ) エリアでは、イベントデータストアおよびチャネルへのアクセスを特定、ソート、および制御できるようにするタグのキーと値のペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でのタグの使用方法の詳細については AWS、の「AWS リソースのタグ付け」を参照してください。AWS 全般のリファレンス
8. 新しい統合を作成する準備ができたら、[Add integration] (統合を追加) を選択します。レビューページはありません。 CloudTrail 統合を作成しますが、チャネルの Amazon リソースネーム (ARN) をパートナーアプリケーションに提供する必要があります。チャネル ARN をパートナーアプリケーションに対し指定するための手順は、パートナードキュメントのウェブサイトで確認

できます。詳細を参照するには、[Integrations] (統合) ページの [Available sources] (利用可能なソース) タブで、パートナーの [Learn more] (詳細はこちら) リンクを選択し AWS Marketplace 内のパートナーページを開きます。

統合のセットアップを完了するために、パートナーまたはソースアプリケーションに対し、チャネルの ARN を指定します。統合のタイプに応じて、お客様、パートナー、またはアプリケーションが PutAuditEvents API を実行し、お客様の AWS アカウントにあるイベントデータストアに対し、アクティビティイベントを配信します。アクティビティイベントが配信されたら、 CloudTrail Lake を使用してアプリケーションから記録されたデータを検索、クエリ、分析できます。イベントデータには、、、などeventVersioneventSource、 CloudTrailイベントペイロードと一致するフィールドが含まれます。userIdentity

コンソールとのカスタムインテグレーションを作成します。

を使用すると CloudTrail 、オンプレミスやクラウド、仮想マシン、コンテナでホストされている社内アプリケーションやSaaSアプリケーションなど、ハイブリッド環境のあらゆるソースからのユーザーアクティビティデータを記録して保存できます。この手順の前半を CloudTrail Lake コンソールで実行し、PutAuditEventsAPI を呼び出してイベントを取り込み、チャネル ARN とイベントペイロードを指定します。PutAuditEventsAPI を使用してアプリケーションのアクティビティをに取り込んだら CloudTrail、 CloudTrail Lake を使用してアプリケーションから記録されたデータを検索、クエリ、分析できます。

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[統合] を選択します。
3. [Add integration] (統合を追加) ページで、チャネルの名前を入力します。名前には 3～128 の文字数が使用できます。使用できるのは文字、数字、ピリオド、アンダースコア、ダッシュのみです。
4. [My custom integration] (カスタム統合) を選択します。
5. [Event delivery location] (イベントの配信場所) で、既存のイベントデータストアで以前と同じアクティビティイベントのログ記録を行うか、新しいイベントデータストアを作成するかを選択します。

   イベントデータストアを新規で作成する場合には、そのデータストアの名前を入力すると同時に、保持期間を日単位で指定します。イベントデータをイベントデータストアに保存できる期間は、[1 年間の延長可能な保存料金] オプションを選択した場合は最大 3,653 日 (約 10 年)、[7 年間の保存料金] オプションを選択した場合は最大 2,557 日 (約 7 年間) です。

アクティビティイベントを、既存の (1 つ以上の) イベントデータストアに口グ記録する場合は、対象となるイベントデータストアをリストから選択します。イベントデータストアに保存できるのは、アクティビティイベントのみです。コンソール内のイベントタイプは、[Events from integrations] (統合からのイベント) にする必要があります。API 内での `eventCategory` 値は `ActivityAuditLog` にする必要があります。

6. [Resource policy] (リソースポリシー) では、統合のチャネル用にリソースポリシーを設定します。リソースポリシーとは、JSON によるポリシードキュメントです。このドキュメントでは、指定したプリンシパルが対象のリソースにおいて実行できるアクションの種類と、その際の条件を指定します。リソースポリシーでプリンシパルとして定義されているアカウントは、`PutAuditEvents` API を呼び出してイベントをチャネルに配信することができます。

   > **Note**
   >
   > チャネルのリソースポリシーを作成しない場合は、そのチャネルの所有者だけが、チャネル内で `PutAuditEvents` API を呼び出すことができます。

   a. (オプション) さらに保護を強化するために、一意の外部 ID を入力します。混乱した代理問題を避けるため、外部 ID には、アカウント ID またはランダムに生成された値などによる、固有の文字列を使用します。

      > **Note**
      >
      > リソースポリシーに外部 ID が含まれているのであれば、`PutAuditEvents` API に対するすべての呼び出しに、この外部 ID を含める必要があります。ただし、ポリシーで外部 ID が定義されていない場合でも、`PutAuditEvents` API を呼び出して `externalId` パラメータを指定することが可能です。

   b. 「 AWS アカウントを追加」を選択し、 AWS チャンネルのリソースポリシーにプリンシパルとして追加する各アカウント ID を指定します。

7. (オプション) [Tag] (タグ) エリアでは、イベントデータストアおよびチャネルへのアクセスを特定、ソート、および制御できるようにするタグのキーと値のペアを最大 50 個追加することができます。タグに基づいてイベントデータストアへのアクセスを認可するために IAM ポリシーを使用する方法の詳細については、「例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否」を参照してください。でのタグの使用方法の詳細については AWS、の「AWS リソースにタグを付ける」を参照してください。AWS 全般のリファレンス

8. 新しい統合を作成する準備ができたら、[Add integration] (統合を追加) を選択します。レビューページはありません。 CloudTrail 統合を作成しますが、カスタムイベントを統合するには、PutAuditEventsリクエストでチャネル ARN を指定する必要があります。

9. PutAuditEventsAPI を呼び出して、アクティビティイベントをに取り込みます。CloudTrailPutAuditEvents リクエストごとに最大 100 のアクティビティイベント (または最大 1 MB) を追加することが可能です。前のステップで作成したチャネル ARN、 CloudTrail 追加するイベントのペイロード、および外部 ID (リソースポリシーで指定されている場合) が必要になります。イベントペイロードに取り込む前に、機密情報や個人を特定できる情報がイベントペイロードに含まれていないことを確認してください。 CloudTrailインジェストするイベントは、に従う必要があります。 CloudTrail CloudTrail Lake インテグレーションのイベントスキーマ

> **Tip**
>
> AWS CloudShellを使用して、 AWS 最新の API を実行していることを確認してください。

次に、put-audit-events CLI コマンドの使用例を示します。--audit-events および --channel-arn パラメータが必要です。前述の手順で作成したチャネルの ARN が必要です。これは、統合の詳細ページからコピーできます。--audit-eventsの値はイベントオブジェクトの JSON 配列です。 --audit-eventsイベントの必須 ID、の値として必要なイベントのペイロードEventData、およびへの取り込み後のイベントの整合性の検証に役立つオプションのチェックサムが含まれます。 CloudTrail

```
aws cloudtrail-data put-audit-events \
--region region \
--channel-arn $ChannelArn \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

次に、2 つのイベントを処理するコマンドの例を示します。

```
aws cloudtrail-data put-audit-events \
--region us-east-1 \
--channel-arn arn:aws:cloudtrail:us-east-1:01234567890:channel/EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE \
--audit-events \
```

```
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

次のコマンドの例では、イベントペイロードの JSON ファイル (custom-events.json) を指定するための --cli-input-json パラメーターを追加しています。

```
aws cloudtrail-data put-audit-events \
--channel-arn $channelArn \
--cli-input-json file://custom-events.json \
--region us-east-1
```

次は、JSON ファイル (custom-events.json) の内容の例です。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",\"recipientAccountId\":
\"recipient_account_ID\"}",
        "id": "1"
      }
   ]
}
```

(オプション) チェックサム値を計算する

PutAuditEventsリクエストの値として指定するチェックサムは、 CloudTrail チェックサムと一致するイベントを受信したかどうかを確認するのに役立ち、イベントの整合性を検証するのにも役立ち

ます。EventDataChecksumチェックサム値は、次のコマンドを実行することで、Base64-SHA256アルゴリズムによって計算されます。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

このコマンドは、 チェックサムを返します。次に例を示します。

```
EXAMPLEHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

このチェックサム値が、PutAuditEvents リクエストの EventDataChecksum 値になります。チェックサムが提供されたイベントのチェックサムと一致しない場合、 CloudTrail エラーでイベントを拒否します。InvalidChecksum

CloudTrail とのLakeインテグレーションの作成、更新、管理 AWS CLI

を使用して CloudTrail Lake インテグレーションを作成、更新、管理できます。 AWS CLI を使用するときは AWS CLI、 AWS リージョン コマンドがプロファイルに設定されたで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

CloudTrail Lake インテグレーションで使用できるコマンド

CloudTrail Lake でインテグレーションを作成、更新、管理するためのコマンドには以下が含まれます。

- create-event-data-store外部のイベント用のイベントデータストアを作成するには。 AWS
- delete-channelインテグレーションに使用したチャンネルを削除する。

- delete-resource-policy CloudTrail Lake インテグレーションのチャンネルにアタッチされているリソースポリシーを削除します。
- get-channel CloudTrail チャンネルに関する情報を返す。
- get-resource-policyチャネルに添付されているリソースベースのポリシードキュメントの JSON テキストを取得します。 CloudTrail
- list-channels現在のアカウントのチャンネルとそのソース名を一覧表示します。
- put-audit-eventsアプリケーションイベントを CloudTrail Lake に取り込みます。必須パラメータはauditEvents、 CloudTrail 取り込みたいイベントの JSON レコード (ペイロードとも呼ばれる) を受け入れます。これらのイベントは、1 PutAuditEvents 回のリクエストあたり最大 100 個 (または 1 MB まで) 追加できます。
- put-resource-policy CloudTrail 外部のイベントソースとの統合に使用されるチャネルに、リソースベースのアクセス権限ポリシーをアタッチすること。 AWSリソースベースのポリシーについて詳しくは、「リソースベースのポリシーの例」を参照してくださいAWS CloudTrail 。
- update-channel必要なチャネル ARN または UUID で指定されたチャネルを更新します。

CloudTrail Lake イベントデータストアで使用できるコマンドのリストについては、を参照してください。イベントデータストアで使用できるコマンド

CloudTrail Lake クエリで使用できるコマンドのリストについては、を参照してください CloudTrail Lake クエリで使用できるコマンド。

とのインテグレーションを作成して、 AWS 外部からのイベントを口グに記録してください。 AWS CLI

では AWS CLI、外部からのイベントを 4 つのコマンド (条件を満たすイベントデータストアがすでにある場合は 3 つ) AWS で記録するインテグレーションを作成します。インテグレーションの宛先として使用するイベントデータストアは、1 つのリージョンと 1 つのアカウント用である必要があります。マルチリージョンにすることはできず、組織のイベントを口グに記録することもできず AWS Organizations、アクティビティイベントのみを含めることができます。コンソール内のイベントタイプは、[Events from integrations] (統合からのイベント) にする必要があります。API 内での eventCategory 値は ActivityAuditLog にする必要があります。統合の詳細については、「外部のイベントソースとの統合を作成 AWS」を参照してください。

1. 統合に使用可能なイベントデータストアをまだ 1 つも作成していない場合は、create-event-data-store を実行してそれを作成します。

AWS CLI 以下のコマンド例は、 AWS外部からのイベントを記録するイベントデータストアを作成します。アクティビティイベントの場合、eventCategory フィールドのセレクタ値は ActivityAuditLog です。このイベントデータストアでは、保持期間は 90 日に設定されています。デフォルトでは、イベントデータストアはすべてのリージョンからイベントを収集しますが、AWS 収集するのはイベントではないため、--no-multi-region-enabledオプションを追加して 1 つのリージョンに設定します。終了保護はデフォルトで有効化されます。また、このイベントデータストアでは、組織内のアカウントのためのイベント収集は行いません。

```
aws cloudtrail create-event-data-store \
--name my-event-data-store \
--no-multi-region-enabled \
--retention-period 90 \
--advanced-event-selectors '[
    {
      "Name": "Select all external events",
      "FieldSelectors": [
          { "Field": "eventCategory", "Equals": ["ActivityAuditLog"] }
        ]
    }
  ]'
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "AdvancedEventSelectors": [
        {
           "Name": "Select all external events",
           "FieldSelectors": [
              {
                  "Field": "eventCategory",
                  "Equals": [
                      "ActivityAuditLog"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
```

```
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-10-27T10:55:55.384000-04:00",
    "UpdatedTimestamp": "2023-10-27T10:57:05.549000-04:00"
}
```

次のステップに進みチャネルの作成を行うには、イベントデータストアの ID (ARN のサフィックス、または前出の応答例にある EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE) が必要になります。

2. create-channelコマンドを実行して、 CloudTrailパートナーまたはソースアプリケーションが内のイベントデータストアにイベントを送信できるようにするチャネルを作成します。

   チャネルは、以下のコンポーネントを含みます。

   ソース

   CloudTrail この情報を使用して、 CloudTrail お客様に代わってイベントデータを送信するパートナーを特定します。ソースは必須で、AWS 以外のすべての有効なイベント用に Custom とするか、パートナーイベントソースの名前を使用するか、どちらかを選びます。ソースごとに最大 1 つのチャネルが許可されます。

   利用可能なパートナーの Source 値については、「統合パートナーに関する追加情報」を参照してください。

   取り込みステータス

   チャネルステータスでは、チャネルソースからの最後のイベントが、いつ受信されたかを知ることができます。

   送信先

   送信先は、チャネルからイベントを受信している CloudTrail Lake イベントデータストアです。チャネルのための送信先イベントデータストアは、変更することが可能です。

   ソースからのイベントの受信を停止するには、対象のチャネルを削除します。

   このコマンドを実行するには、送信先イベントデータストアの ID が少なくとも 1 つ必要です。送信先として有効な型は EVENT_DATA_STORE です。取り込んだイベントは、複数のイベントデータストアに送信することができます。次のコマンドの例では、--destinations パラメー

ターの Location 属性内にある ID で表される、2 つのイベントデータストアに対しイベントを送信するチャネルを作成します。--destinations、--name、および --source パラメータが必要です。パートナーからイベントを取り込むには、 CloudTrail パートナーの名前をの値として指定します。--source外部にある独自のアプリケーションからイベントを取り込むにはAWS、Customの値としてを指定します。--source

```
aws cloudtrail create-channel \
    --region us-east-1 \
    --destinations '[{"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location":
 "EXAMPLEg922-5n2l-3vz1- apqw8EXAMPLE"}]'
    --name my-partner-channel \
    --source $partnerSourceName \
```

create-channel コマンドに対する応答の中から、新しいチャネルの ARN をコピーします。以降の手順で put-resource-policy および put-audit-events コマンドを実行する際には、この ARN が必要になります。

3. put-resource-policyコマンドを実行してリソースポリシーをチャネルにアタッチします。リソースポリシーとは、JSON によるポリシードキュメントです。このドキュメントでは、指定したプリンシパルが対象のリソースにおいて実行できるアクションの種類と、その際の条件を指定します。チャネルのリソースポリシーでプリンシパルとして定義されているアカウントは、PutAuditEvents API を呼び出してイベントを配信することができます。

> **Note**
>
> チャネルのリソースポリシーを作成しない場合は、そのチャネルの所有者だけが、チャネル内で PutAuditEvents API を呼び出すことができます。

ポリシーに必要な情報は、統合タイプによって決まります。

- CloudTrail ディレクション統合では、 AWS ポリシーにパートナーのアカウント ID を含める必要があり、パートナーから提供された固有の外部 ID を入力する必要があります。CloudTrail CloudTrail コンソールを使用してインテグレーションを作成すると、 AWS パートナーのアカウント ID がリソースポリシーに自動的に追加されます。AWS ポリシーに必要なアカウント番号の取得方法については、パートナーのドキュメントを参照してください。

- ソリューション統合では、プリンシパルとして少なくとも 1 AWS つのアカウント ID を指定する必要があります。また、代理人の混乱を防ぐために任意で外部 ID を入力することもできます。

リソースポリシーには、以下の要件があります。

- ポリシーで定義されているリソース ARN は、ポリシーがアタッチされているチャネル ARN と一致する必要があります。
- このポリシーには、cloudtrail-data という 1 つのアクションしか含まれていません。PutAuditEvents
- ポリシーには、少なくとも 1 つのステートメントを含めます。ポリシーには、最大 20 個のステートメントを記述できます。
- 各ステートメントには、少なくとも 1 つのプリンシパルを含めます。1 つのステートメントには、最大 50 個のプリンシパルを記述できます。

```
aws cloudtrail put-resource-policy \
    --resource-arn "channelARN" \
    --policy "{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
```

```
                {
                    "cloudtrail:ExternalId": "UniqueExternalIDFromPartner"
                }
            }
        }
    ]
}"
```

リソースポリシーの詳細については、「AWS CloudTrail リソースベースのポリシーの例」を参照してください。

4. PutAuditEventsAPI を実行してアクティビティイベントを取り込みます。 CloudTrail追加するイベントのペイロードが必要です。 CloudTrail イベントペイロードに取り込む前に、機密情報や個人を特定できる情報がイベントペイロードに含まれていないことを確認してください。 CloudTrailPutAuditEvents API では、cloudtrail エンドポイントではなく cloudtrail-data CLI エンドポイントが使用されることに注意してください。

   次に、put-audit-events CLI コマンドの使用例を示します。--audit-events および --channel-arn パラメータが必要です。--external-id パラメータは、リソースポリシーで外部 ID が定義されている場合に必要です。前述のステップで作成したチャネルの ARN が必要です。の値はイベントオブジェクトの --audit-events JSON 配列です。 --audit-eventsイベントの必須 ID、の値として必要なイベントのペイロードEventData、およびへの取り込み後のイベントの整合性の検証に役立つオプションのチェックサムが含まれます。 CloudTrail

```
aws cloudtrail-data put-audit-events \
--channel-arn $ChannelArn \
--external-id $UniqueExternalIDFromPartner \
--audit-events \
id="event_ID",eventData='"{event_payload}"' \
id="event_ID",eventData='"{event_payload}"',eventDataChecksum="optional_checksum"
```

   次に、2 つのイベントを処理するコマンドの例を示します。

```
aws cloudtrail-data put-audit-events \
--channel-arn arn:aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--external-id UniqueExternalIDFromPartner \
--audit-events \
id="EXAMPLE3-0f1f-4a85-9664-d50a3EXAMPLE",eventData='"{\"eventVersion\":\0.01\",
\"eventSource\":\"custom1.domain.com\", ...
```

```
\}"' \
id="EXAMPLE7-a999-486d-b241-b33a1EXAMPLE",eventData='"{\"eventVersion\":\0.02\",
\"eventSource\":\"custom2.domain.com\", ...
\}"',eventDataChecksum="EXAMPLE6e7dd61f3ead...93a691d8EXAMPLE"
```

次のコマンドの例では、イベントペイロードの JSON ファイル (custom-events.json) を指定するための --cli-input-json パラメーターを追加しています。

```
aws cloudtrail-data put-audit-events --channel-arn $channelArn --external-id
 $UniqueExternalIDFromPartner --cli-input-json file://custom-events.json --region
 us-east-1
```

次は、JSON ファイル (custom-events.json) の内容の例です。

```
{
    "auditEvents": [
      {
        "eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":
\"principalId\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":
\"value\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"12.34.56.78\",\"recipientAccountId\":
\"152089810396\"}",
        "id": "1"
      }
   ]
}
```

コマンドを実行すると、統合が機能していて、 CloudTrail ソースからイベントが正しく取り込まれていることを確認できます。get-channelの出力には、get-channel CloudTrailイベントを受信した最新のタイムスタンプが表示されます。

```
aws cloudtrail get-channel --channel arn:aws:cloudtrail:us-east-1:01234567890:channel/
EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

(オプション) チェックサム値を計算する

PutAuditEventsリクエストの値として指定するチェックサムは、 CloudTrail チェックサムと一致するイベントを受信したかどうかを確認するのに役立ち、イベントの整合性を検証するのにも役立ちます。EventDataChecksumチェックサム値は、次のコマンドを実行することで、Base64-SHA256アルゴリズムによって計算されます。

```
printf %s "{"eventData": "{\"version\":\"eventData.version\",\"UID\":\"UID\",
        \"userIdentity\":{\"type\":\"CustomUserIdentity\",\"principalId\":\"principalId
\",
        \"details\":{\"key\":\"value\"}},\"eventTime\":\"2021-10-27T12:13:14Z\",
\"eventName\":\"eventName\",
        \"userAgent\":\"userAgent\",\"eventSource\":\"eventSource\",
        \"requestParameters\":{\"key\":\"value\"},\"responseElements\":{\"key\":\"value
\"},
        \"additionalEventData\":{\"key\":\"value\"},
        \"sourceIPAddress\":\"source_IP_address\",
        \"recipientAccountId\":\"recipient_account_ID\"}",
        "id": "1"}" \
 | openssl dgst -binary -sha256 | base64
```

このコマンドは、 チェックサムを返します。次に例を示します。

```
EXAMPLEDHjkI8iehvCUCWTIAbNYkOgO/t0YNw+7rrQE=
```

このチェックサム値が、PutAuditEvents リクエストの EventDataChecksum 値になります。チェックサムが提供されたイベントのチェックサムと一致しない場合、 CloudTrail エラーでそのイベントを拒否します。InvalidChecksum

チャンネルを以下のように更新します。 AWS CLI

チャネルの名前、または送信先のイベントデータストアを更新するには、update-channel コマンドを実行します。--channel パラメータが必須です。チャネルのソースを更新することはできません。次に例を示します。

```
aws cloudtrail update-channel \
--channel aws:cloudtrail:us-east-1:123456789012:channel/EXAMPLE8-0558-4f7e-
a06a-43969EXAMPLE \
--name "new-channel-name" \
```

```
--destinations '[{"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEf852-4e8f-8bd1-
bcf6cEXAMPLE"}, {"Type": "EVENT_DATA_STORE", "Location": "EXAMPLEg922-5n2l-3vz1-
 apqw8EXAMPLE"}]'
```

チャンネルを削除すると、とのインテグレーションが削除されます。 AWS CLI

外部でのパートナーイベントやその他のアクティビティイベントの取り込みを停止するには AWS、コマンドを実行してチャンネルを削除します。delete-channel削除するチャネルの ARN、またはチャネル ID (ARN のサフィックス) が必要です。次に例を示します。

```
aws cloudtrail delete-channel \
--channel EXAMPLE8-0558-4f7e-a06a-43969EXAMPLE
```

統合パートナーに関する追加情報

このセクションの表は、各統合パートナーのソース名と、それぞれの統合タイプ (直接またはソリューション) を示しています。

[Source name] (ソース名) 列の情報は、`CreateChannel` API を呼び出す際に必要となります。ソース名は、`Source` パラメータの値として指定します。

パートナー名 (コンソール)	ソース名 (API)	統合タイプ
My custom integration	`Custom`	solution
Cloud Storage Security	`CloudStorageSecurityConsole`	solution
Clumio	`Clumio`	direct
CrowdStrike	`CrowdStrike`	solution
CyberArk	`CyberArk`	solution
GitHub	`GitHub`	solution
Kong Inc	`KongGatewayEnterprise`	solution
LaunchDarkly	`LaunchDarkly`	direct

パートナー名 (コンソール)	ソース名 (API)	統合タイプ
Netskope	NetskopeCloudExchange	solution
Nordcloud (IBM 傘下)	IBMMulticloud	direct
MontyCloud	MontyCloud	direct
Okta	OktaSystemLogEvents	solution
One Identity	OneLogin	solution
Shoreline.io	Shoreline	solution
Snyk.io	Snyk	direct
Wiz	WizAuditLogs	solution

パートナードキュメントの表示

パートナーと CloudTrail Lake の統合について詳しくは、パートナーのドキュメントをご覧ください。

パートナードキュメントを表示するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail にあるコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[統合] を選択します。
3. [Integrations] (統合) ページで [Available sources] (利用可能なソース) を選択した後で、ドキュメントを表示したいパートナーの [Learn more] (詳細はこちら) を選択します。

CloudTrail Lake インテグレーションのイベントスキーマ

以下の表では、 CloudTrail イベントレコード内のスキーマ要素と一致する必須およびオプションのスキーマ要素について説明しています。eventDataの内容はイベントによって提供され、CloudTrail 他のフィールドは取り込み後に提供されます。

CloudTrail イベントレコードの内容については、で詳しく説明しています。CloudTrail レコードの内容

- CloudTrail 取り込み後にによって提供されるフィールド。
- イベントによって提供されるフィールド

CloudTrail 取り込み後にによって提供されるフィールド。

フィールド名	入力タイプ	要件	説明
eventVersion	string	必須	イベントのバージョン。
eventCategory	string	必須	イベントカテゴリ。AWS イベント以外の場合、値はですActivityAuditLog 。
eventType	string	必須	イベントタイプです。AWS 非イベントの場合、有効値はですActivityLog 。
eventID	string	必須	イベントの一意の ID。
eventTime	string	必須	yyyy-MM-DDTHH:mm:ss 形式および協定世界時 (UTC) で表示した、イベントのタイムスタンプ)。
awsRegion	string	必須	AWS リージョン PutAuditEvents 呼び出しが行われた場所。

フィールド名	入力タイプ	要件	説明
recipientAccountId	string	必須	このイベントを受信したアカウント ID を表します。 CloudTrail イベントペイロードから計算してこのフィールドに値を入力します。
補遺	-	オプションです。	イベントの処理が遅延した理由に関する情報が表示されます。既存のイベントから情報が欠落している場合、補遺ブロックには、不足している情報と、不足している理由が表示されます。
• 理由	string	オプションです。	イベントまたはその内容の一部が欠落していた理由。
• updatedFields	string	オプションです。	付則によって更新されているイベントレコードフィールド。これは、理由が UPDATED_DATA の場合にのみ提供されます。

フィールド名	入力タイプ	要件	説明
• originalUID	string	オプションです。	ソースからのイベントの元の UID。これは、理由が UPDATED_DATA の場合にのみ提供されます。
• originalEventID	string	オプションです。	元のイベント ID。これは、理由が UPDATED_DATA の場合にのみ提供されます。
metadata	-	必須	イベントが使用したチャネルに関する情報。
• ingestionTime	string	必須	イベントが処理された時刻を yyyy-MM-DDTHH:mm:ss 形式の協定世界時 (UTC) で表示したタイムスタンプ。
• channelARN	string	必須	イベントが使用したチャネルの ARN。

カスタマーイベントによって提供されるフィールド

フィールド名	入力タイプ	要件	説明
eventData	-	必須	CloudTrail コールで送信される監査データ。PutAuditEvents

フィールド名	入力タイプ	要件	説明
• version	string	必須	ソースから送られたイベントのバージョン。 長さの制限: 最大長は 256 文字です。
• userIdentity	-	必須	リクエストを作成したユーザーに関する情報。
• • type	string	必須	ユーザー ID のタイプ。 長さの制限: 最大長は 128 文字です。
• • principalId	string	必須	イベントのアクター用の一意の識別子。 長さの制限: 最大長は 1024 文字です。
• • details	JSON オブジェクト	オプションです。	ID に関する追加情報。
• userAgent	string	オプションです。	リクエストが行われたエージェント。 長さの制限: 最大長は 1024 文字です。

フィールド名	入力タイプ	要件	説明
• eventSource	string	必須	これはパートナーイベントソース、またはイベントがログ記録されるカスタムアプリケーションです。 長さの制限: 最大長は 1024 文字です。
• eventName	string	必須	リクエストされたアクションで、ソースサービスまたはアプリケーション用の API のアクションの 1 つ。 長さの制限: 最大長は 1024 文字です。
• eventTime	string	必須	yyyy-MM-DDTHH:mm:ss 形式および協定世界時 (UTC) で表示した、イベントのタイムスタンプ)。
• UID	string	必須	リクエストを識別するための UID 値。この値は、呼び出されたサービスまたはアプリケーションで生成されます。 長さの制限: 最大長は 1024 文字です。

フィールド名	入力タイプ	要件	説明
• requestParameters	JSON オブジェクト	オプションです。	リクエストとともに送信されたパラメータ (ある場合)。このフィールドの最大サイズは 100 kB です。この上限を超えるコンテンツは拒否されます。
• responseElements	JSON オブジェクト	オプションです。	変更を行うアクションのレスポンスの要素 (アクションの作成、更新、削除)。このフィールドの最大サイズは 100 kB です。この上限を超えるコンテンツは拒否されます。
• errorCode	string	オプションです。	イベントでのエラーを表す文字列。 長さの制限: 最大長は 256 文字です。
• errorMessage	string	オプションです。	エラーに関する説明。 長さの制限: 最大長は 256 文字です。
• sourceIPAddress	string	オプションです。	リクエストが行われた IP アドレス。アドレスには IPv4 と IPv6 の両方を使用できます。

フィールド名	入力タイプ	要件	説明
• recipientAccountId	string	必須	このイベントを受信したアカウント ID を表します。アカウント ID は、 AWS チャンネルを所有するアカウント ID と同じでなければなりません。
• additionalEventData	JSON オブジェクト	オプションです。	リクエストまたはレスポンスの一部ではないイベントに関する追加のデータ。このフィールドの最大サイズは 28 kB です。この制限を超えるコンテンツは拒否されます。

次の例は、 CloudTrail イベントレコード内のものと一致するスキーマ要素の階層を示しています。

```
{
    "eventVersion": String,
    "eventCategory": String,
    "eventType": String,
    "eventID": String,
    "eventTime": String,
    "awsRegion": String,
    "recipientAccountId": String,
    "addendum": {
       "reason": String,
       "updatedFields": String,
       "originalUID": String,
       "originalEventID": String
    },
    "metadata" : {
       "ingestionTime": String,
```

```
        "channelARN": String
    },
    "eventData": {
        "version": String,
        "userIdentity": {
          "type": String,
          "principalId": String,
          "details": {
             JSON
          }
        },
        "userAgent": String,
        "eventSource": String,
        "eventName": String,
        "eventTime": String,
        "UID": String,
        "requestParameters": {
           JSON
        },
        "responseElements": {
           JSON
        },
        "errorCode": String,
        "errorMessage": String,
        "sourceIPAddress": String,
        "recipientAccountId": String,
        "additionalEventData": {
           JSON
        }
    }
}
```

CloudTrail Lake ダッシュボードを表示する

CloudTrail Lake ダッシュボードを使用して、イベントデータストア内のイベントを視覚化できます。複数の異なるダッシュボードタイプから選択できます。イベントデータストアで使用できるダッシュボードタイプは、イベントデータストアのアドバンスイベントセレクタの設定に応じて異なります。たとえば、 CloudTrail 管理イベントに関する情報が表示されるダッシュボードでは、 CloudTrail 現在選択されているイベントデータストアが管理イベントを収集している場合にのみダッシュボードを選択できます。

各ダッシュボードタイプは複数のウィジェットで構成され、各ウィジェットは SQL クエリを表します。ウィジェットのクエリを表示するには、[クエリエディターで表示して分析] を選択してクエリエディターを開きます。ウィジェットへの入力に使用されるシステム生成クエリを変更することはできませんが、クエリエディタでクエリを編集してクエリを実行して詳細な分析を行うことができます。

ダッシュボードにデータを入力して更新するには、[クエリを実行] を選択します。[クエリを実行] を選択すると、 CloudTrail システムによって生成されたクエリがユーザーに代わって実行されます。クエリの実行にはコストがかかるため、 CloudTrail クエリの実行に関連するコストを確認するように求められます。これは 1 回限りの確認です。料金について詳しくは、「 CloudTrail 価格設定」を参照してくださいCloudTrail 。

トピック

制限事項

現在のリリースには次の制限が適用されます。

- 現在のリリースでは、カスタマイズされたダッシュボード、ウィジェット、およびクエリはサポートされていません。
- 現在のリリースでは、イベント (データイベント、管理イベント) と Insights CloudTrail イベントを収集するイベントデータストア用のダッシュボードのみが提供されています。
- 現在のリリースでは、ダッシュボードへの入力に使用されるシステム生成クエリの編集はサポートされていません。[クエリエディター]タブでは、ウィジェットの基盤となるクエリを表示および編集できますが、クエリに加えた変更はダッシュボード外での補足分析を目的としています。

前提条件

Lake ダッシュボードには次の前提条件が適用されます。

- Lake ダッシュボードを表示して使用するには、少なくとも 1 つの CloudTrail Lake イベントデータストアを作成する必要があります。イベントデータストアは、コンソール AWS CLI、または

SDK を使用して作成できます。コンソールを使用してイベントデータストアを作成する方法の詳細については、「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。を使用してイベントデータストアを作成する方法については AWS CLI、を参照してくださいを使用して、イベントデータストアを作成、更新、管理します AWS CLI。

- ダッシュボードに入力するには、 CloudTrail ユーザーに代わってクエリを実行します。ダッシュボードページを初めて表示すると、 CloudTrail クエリの実行に関連するコストを確認するように求められます。クエリの実行コストを確認するには、[同意する] を選択します。

ダッシュボードを選択する

次の手順を使用して、表示するイベントデータストアとダッシュボードタイプを選択します。

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. 左のナビゲーションペインの [Lake] の下にある [ダッシュボード] を選択します。
3. データを視覚化するイベントデータストアを選択します。
4. 表示するダッシュボードの種類を選択します。ダッシュボードリストは、選択したイベントデータストアのアドバンスイベントセレクタの設定に基づいて入力されます。

   ダッシュボードのタイプを以下に示します。

   - 概要ダッシュボード-最もアクティブなユーザーと AWS リージョン、 AWS のサービス イベント数別に表示されます。また、`read` と `write` の管理イベントのアクティビティ、最もスロットリングされているイベント、上位のエラーに関する情報も表示できます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。
   - [管理イベント] ダッシュボード - ユーザーごとのコンソールのログインイベント、アクセス拒否イベント、破壊的なアクション、上位エラーが表示されます。ユーザーごとに TLS バージョンと古い TLS 呼び出しに関する情報を表示することもできます。このダッシュボードは、管理イベントを収集するイベントデータストアで使用できます。
   - [S3 データイベント] ダッシュボード - S3 アカウントのアクティビティ、最もアクセスされた S3 オブジェクト、上位の S3 ユーザー、上位の S3 アクションが表示されます。このダッシュボードは、Amazon S3 データイベントを収集するイベントデータストアで使用できます。
   - [Insights イベント]ダッシュボード – 全体的な Insights タイプ別の Insights イベントの比率、上位ユーザーとサービスに関する Insights タイプ別の Insights イベントの比率、および 1 日あたりの Insights イベント数が表示されます。ダッシュボードには、最大 30 日間の Insights

イベントを一覧表示するウィジェットも含まれます。このダッシュボードは、Insights イベントを収集するイベントデータストアでのみ利用可能です。

> **Note**
>
> - CloudTrail ソースイベントデータストアで初めてインサイトを有効にした後、異常なアクティビティが検出された場合は、最初の CloudTrail Insights イベントの配信までに最大 7 日かかることがあります。詳細については、「Insights イベントの配信を理解する」を参照してください。
> - [Insights イベント] ダッシュボードには、ソースイベントデータストアの設定によって決定される、選択したイベントデータストアによって収集された Insights イベントに関する情報のみが表示されます。例えば、ソースイベントデータストアで、`ApiErrorRateInsight` ではなく `ApiCallRateInsight` の Insights イベントを有効にしている場合には、`ApiErrorRateInsight` の Insights イベントに関する情報は表示されません。

5. [絶対範囲] または [相対範囲] でダッシュボードデータをフィルターします。特定の日付と時刻の範囲を選択するには、[絶対範囲] を選択します。事前定義済みの時間範囲またはカスタム範囲を選択するには、[相対範囲] を選択します。デフォルトでは、ダッシュボードには過去 24 時間のイベントデータが表示されます。

> **Note**
>
> CloudTrail Lake クエリでは、スキャンされるデータ量に応じてコストがかかります。コストを抑えるには、より狭い時間範囲にフィルタリングします。料金について詳しくは、「 CloudTrail 料金表」を参照してくださいAWS CloudTrail 。

6. [クエリを実行] を選択して、ダッシュボードのウィジェットに対してクエリを実行します。

日付または時間範囲でダッシュボードをフィルターする

デフォルトでは、ダッシュボードには過去 24 時間のデータが表示されます。ダッシュボードは [絶対範囲] または [相対範囲] でフィルターできます。

特定の日付と時刻の範囲を選択するには、[絶対範囲] を選択します。

事前定義済みの時間範囲またはカスタム範囲を選択するには、[相対範囲] を選択します。

時間範囲を選択したら、[クエリを実行] を選択してダッシュボードを更新します。

> **Note**
>
> CloudTrail Lake クエリでは、スキャンされるデータ量に基づいてコストがかかります。コストを抑えるには、より狭い時間範囲にフィルタリングします。料金について詳しくは、「CloudTrail 料金表」を参照してくださいAWS CloudTrail 。

ダッシュボードウィジェットのクエリを表示する

各ウィジェットは 1 つの SQL クエリを表します。ウィジェットのクエリを表示するには、[クエリエディターで表示して分析] を選択してクエリエディターを開きます。クエリエディターを使用すると、ダッシュボード外でクエリをさらに絞り込み、クエリを実行して更新されたクエリの結果を確認できます。クエリの操作の詳細については、「クエリを作成または編集する」を参照してください。

> **Note**
>
> ダッシュボードウィジェットのシステム生成クエリを変更することはできません。[クエリエディター] タブでクエリに加えた変更は、ダッシュボード外での詳細な分析のみを目的としています。

CloudTrail レイククエリ

CloudTrail Lake のクエリは SQL で作成されています。 CloudTrail Lake Editor タブでクエリを作成するには、SQL でクエリを一から記述するか、保存済みまたはサンプルクエリを開いて編集します。包含されているサンプルクエリを独自の変更で上書きすることはできませんが、新しいクエリとして保存することが可能です。許可される SQL クエリ言語の詳細については、「CloudTrail レイク SQL 制約」を参照してください。

無制限のクエリ (`SELECT * FROM edsID` など) は、イベントデータストア内のすべてのデータをスキャンします。コストを抑えるため、クエリに開始および終了 `eventTime` タイムスタンプを追加することで、クエリを制限することをお勧めします。以下は、指定されたイベントデータストア内で、イベント時刻が 2023 年 1 月 5 日午後 1 時 51 分より後 (>) で、2023 年 1 月 19 日午後 1 時 51 分より前 (<) のすべてのイベントを検索する例です。イベントデータストアの最小保存期間は 7 日間であるため、開始および終了 `eventTime` 値の間の最小間隔も 7 日間です。

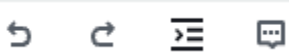
```
SELECT *
FROM eds-ID
WHERE
     eventtime >='2023-01-05 13:51:00' and eventtime < ='2023-01-19 13:51:00'
```

トピック

- クエリエディタツール
- CloudTrail コンソールにサンプルクエリが表示されます。
- クエリを作成または編集する
- クエリを実行し、クエリ結果を保存する
- クエリ結果を表示する
- 保存されたクエリ結果のダウンロード
- 保存されたクエリ結果の検証
- を使用して CloudTrail Lake クエリの実行と管理を行います。 AWS CLI

クエリエディタツール

クエリエディタの右上にあるツールバーは、SQL クエリの作成とフォーマットに役立つコマンドを提供します。



以下のリストは、ツールバーのコマンドの説明です。

- [Undo] (元に戻す) – クエリエディタで最後に行ったコンテンツの変更を元に戻します。
- [Redo] (再実行) – クエリエディタで行った最後のコンテンツ変更を繰り返します。
- [Format selected] (選択部分のフォーマット) – クエリエディタの内容を SQL のフォーマット規則とスペース規則に従って配列します。
- 選択部分にコメント/コメントを解除 - クエリの選択した部分にコメントがない場合、コメントを追加します。選択した部分に既にコメントがある場合、このオプションを選択するとコメントが削除されます。

CloudTrail コンソールにサンプルクエリが表示されます。

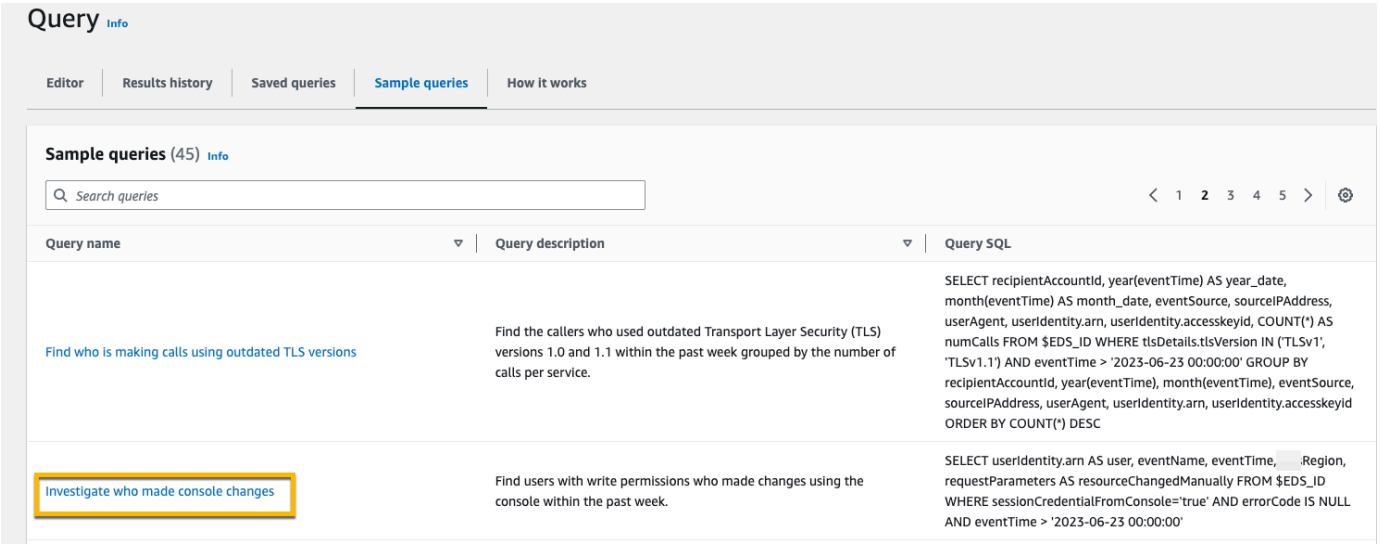
CloudTrail コンソールには、独自のクエリの作成を始めるのに役立つサンプルクエリが多数用意されています。

CloudTrail クエリでは、スキャンされたデータ量に基づいて料金が発生します。コストを抑えるため、クエリに開始および終了 `eventTime` タイムスタンプを追加することで、クエリを制限することをお勧めします。料金について詳しくは、「 CloudTrail 料金表」を参照してくださいAWS CloudTrail 。

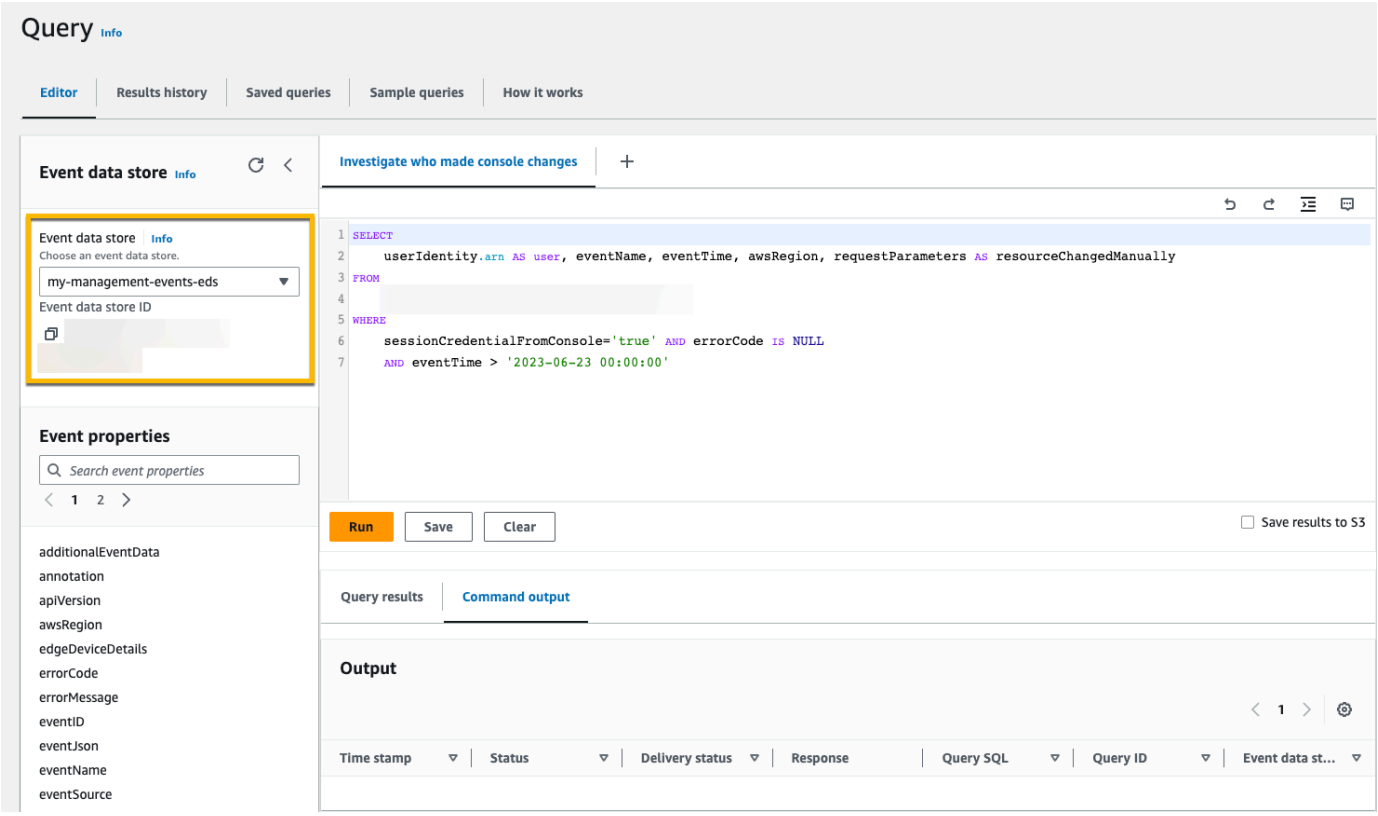
> **Note**
>
> GitHub コミュニティが作成したクエリも表示できます。詳細およびこれらのサンプルクエリを確認するには、 GitHub Web サイトの「CloudTrailLake サンプルクエリ」を参照してください。 AWS CloudTrail のクエリは評価されていません GitHub。

サンプルクエリを表示、実行する

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。
3. [Query] (クエリ) ページで、[Sample queries] (サンプルクエリ) タブを開きます。
4. リストからサンプルクエリを選択するか、クエリを検索してリストをフィルタリングします。この例では、[クエリ名] を選択し、[コンソール変更者の調査] クエリを開きます。そうすると、[Editor] (エディタ) タブでこのクエリが開きます。

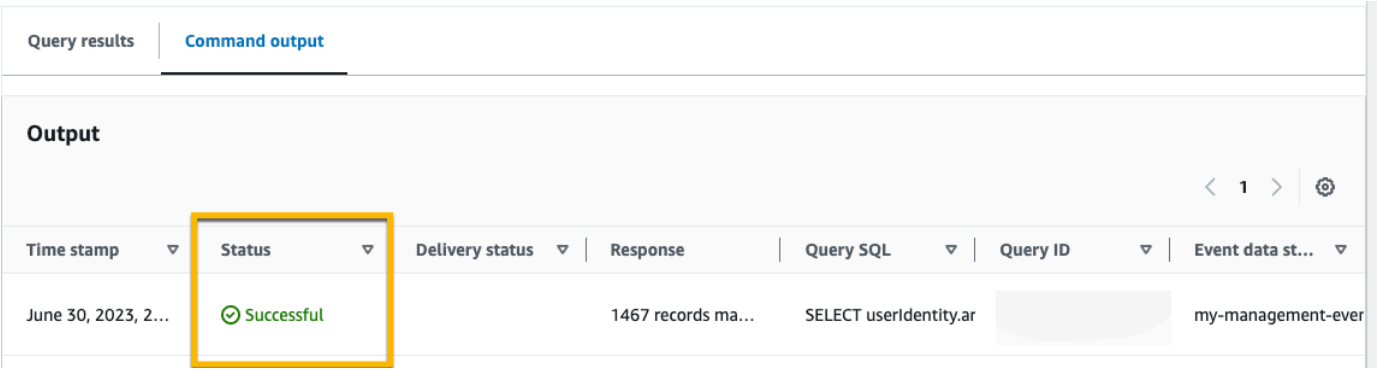


5. [エディター] タブで、クエリを実行するイベントデータストアを選択します。リストからイベントデータストアを選択すると、FROMクエリエディターの行にイベントデータストア ID CloudTrail が自動的に入力されます。

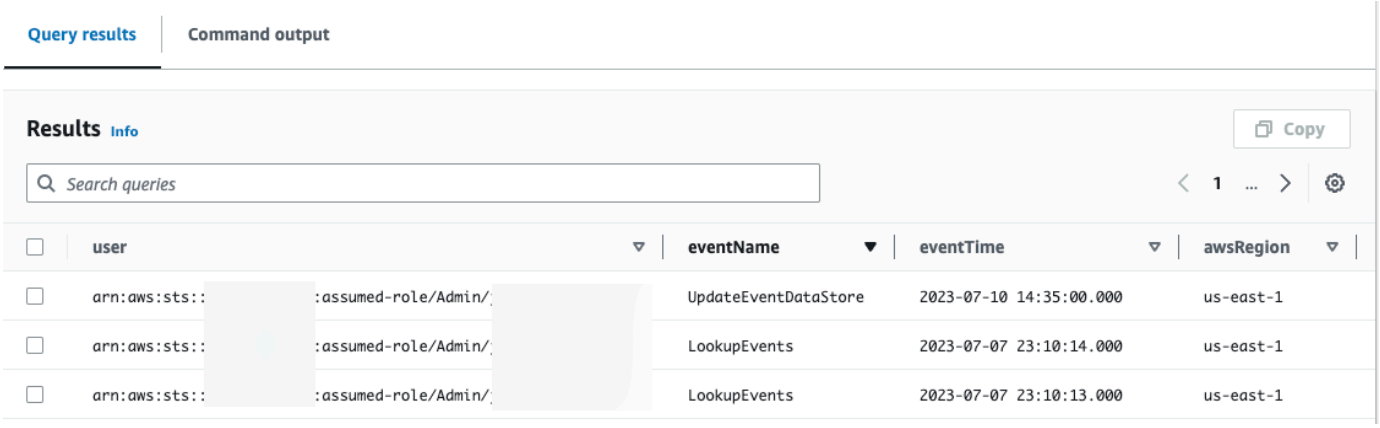


6. クエリを実行するには、[実行] を選択します。

[コマンド出力] タブには、クエリが成功したかどうか、一致したレコードの数、クエリの実行時間など、クエリに関するメタデータが表示されます。



[クエリ結果] タブには、選択したイベントデータストア内のクエリと一致したイベントデータが表示されます。



クエリ編集の詳細については、「クエリを作成または編集する」を参照してください。クエリの実行およびクエリ結果の保存に関する詳細については、「クエリを実行し、クエリ結果を保存する」を参照してください。

クエリを作成または編集する

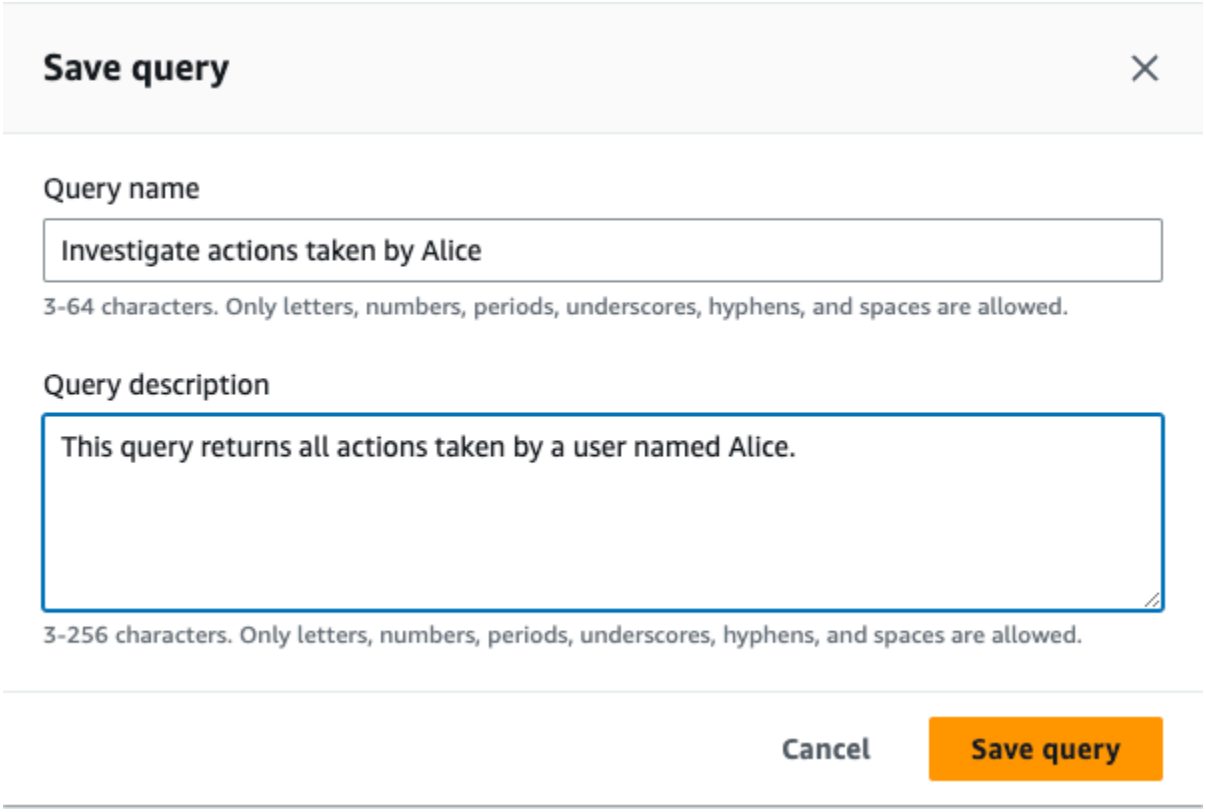
このチュートリアルでは、サンプルクエリを開いて編集し、Alice という名前のユーザーが実行したアクションを見つけて、新しいクエリとして保存します。クエリを保存している場合は、[Saved queries] (保存されたクエリ) タブで保存されたクエリを編集することもできます。コストを抑えるため、クエリに開始および終了 eventTime タイムスタンプを追加することで、クエリを制限することをお勧めします。

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。
3. [Query] (クエリ) ページで、[Sample queries] (サンプルクエリ) タブを開きます。
4. クエリ名を選択してサンプルクエリを開きます。そうすると、[Editor] (エディタ) タブでこのクエリが開きます。この例では、「Investigate user actions」という名前のクエリを選択し、クエリを編集して Alice という名前のユーザーのアクションを検索します。
5. [エディター] タブで、WHERE 行を編集して調査するユーザーを指定し、必要に応じて eventTime の値を更新します。FROMの値はイベントデータストアの ARN の ID 部分で、CloudTrail イベントデータストアを選択すると自動的に入力されます。

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
```

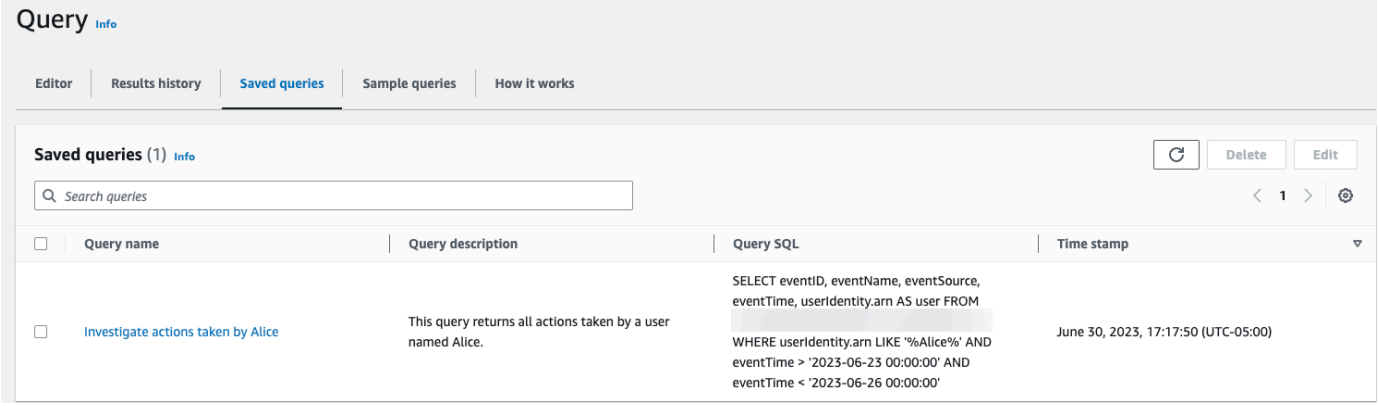
```
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

6. クエリは、保存する前に実行して、機能することを確認できます。クエリを実行するには、[Event data store] (イベントデータストア) ドロップダウンリストからイベントデータストアを選択して、[Run] (実行)をクリックします。[Command output] (コマンド出力) タブの [Status] (ステータス) 列でアクティブなクエリを確認して、クエリが正常に実行されたことを確認します。
7. サンプルクエリを更新したら、[保存] を選択します。
8. [Save query] (クエリを保存) で、クエリの名前と説明を入力します。[Save query] (クエリを保存) をクリックして、変更を新しいクエリとして保存します。クエリに対する変更を破棄するには、[Cancel] (キャンセル) をクリックするか、[Save query] (クエリを保存) ウィンドウを閉じます。



> **Note**
>
> 保存されたクエリはブラウザに関連付けられます。 CloudTrail 別のブラウザまたは別のデバイスを使用してコンソールにアクセスすると、保存されたクエリは使用できません。

9. [Saved queries] (保存されたクエリ) タブを開くと、表に新しいクエリが表示されます。



クエリを実行し、クエリ結果を保存する

クエリを選択または保存したら、イベントデータストアでクエリを実行できます。

クエリを実行すると、オプションとしてクエリ結果を Amazon S3 バケットに保存できます。CloudTrail Lake でクエリを実行すると、クエリによってスキャンされたデータ量に基づいて料金が発生します。クエリ結果を S3 バケットに保存する場合、追加の CloudTrail Lake 料金は発生しませんが、S3 ストレージには料金がかかります。S3 の価格設定に関する詳細については、「Amazon S3 pricing」(Amazon S3 価格設定) を参照してください。

CloudTrail クエリスキャンの完了後にクエリ結果が配信されるため、クエリ結果を保存すると、S3 CloudTrail バケットに表示される前にクエリ結果がコンソールに表示される場合があります。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。 CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。クエリスキャンの完了後、S3 バケットに配信されるデータは、1 GB あたり平均 60～90 秒の遅延が見込まれます。

Lake CloudTrail を使用してクエリを実行するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。

2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。
3. [保存されたクエリ] または [サンプルクエリ] タブ で、クエリ名を選択して実行するクエリを選択します。
4. [Event data store] (イベントデータストア) の [Editor] (エディタ) タブで、ドロップダウンリストからイベントデータストアを選択します。
5. (オプション) [Editor] (エディタ) タブで [Save results to S3] (結果を S3 に保存) を選択し、クエリ結果を S3 バケットに保存します。デフォルトの S3 バケットを選択すると、 CloudTrail 必要なバケットポリシーが作成され、適用されます。デフォルトの S3 バケットを選択した場合、IAM `s3:PutEncryptionConfiguration` ポリシーにはアクションのアクセス権限を含める必要があります。デフォルトではバケットのサーバー側の暗号化が有効になっているためです。クエリ結果保存の詳細については、「保存されたクエリ結果に関する追加情報」を参照してください。

   > **Note**
   >
   > 別のバケットを使用するには、バケット名を指定するか、[Browse S3] (S3 を閲覧) を選択してバケットを選択します。バケットポリシーは、 CloudTrail クエリ結果をバケットに配信するアクセス権限を付与する必要があります。バケットポリシーを手動で編集する方法については、 CloudTrail レイククエリ結果の Amazon S3 バケットポリシー を参照してください。

6. [Editor] (エディタ) タブで、[Run] (実行) をクリックします。

   イベントデータストアのサイズと、それに含まれるデータの日数によっては、クエリの実行に数分かかる場合があります。[Command output] (コマンド出力) タブには、クエリのステータスと、クエリの実行が終了したかどうかが表示されます。クエリの実行が終了したら、[Query results] (クエリ結果) タブを開いて、アクティブなクエリ (現在エディタに表示されているクエリ) の結果の表を表示します。

> **Note**
>
> 1 時間以上実行するクエリは、タイムアウトすることがあります。クエリがタイムアウトになる前に処理された結果の一部は引き続き取得できます。 CloudTrail クエリ結果の一部は S3 バケットには配信されません。タイムアウトを回避するには、クエリを絞り込んでスキャンされるデータ量を制限する時間範囲を狭くすることができます。

保存されたクエリ結果に関する追加情報

クエリ結果の保存後、保存したクエリ結果を S3 バケットからダウンロードできるようになります。保存したクエリ結果の検索とダウンロードの詳細については、「保存されたクエリ結果のダウンロード」を参照してください。

保存したクエリ結果を検証して、 CloudTrail クエリ結果の配信後にクエリ結果が変更されたか、削除されたか、変更されていないかを判断することもできます。保存したクエリ結果の検証の詳細については、「保存されたクエリ結果の検証」を参照してください。

例:クエリ結果を Amazon S3 バケットに保存する

このウォークスルーでは、クエリ結果を S3 バケットに保存し、そのクエリ結果をダウンロードする方法を示します。

CloudTrail Lake のクエリ結果を Amazon S3 バケットに保存する

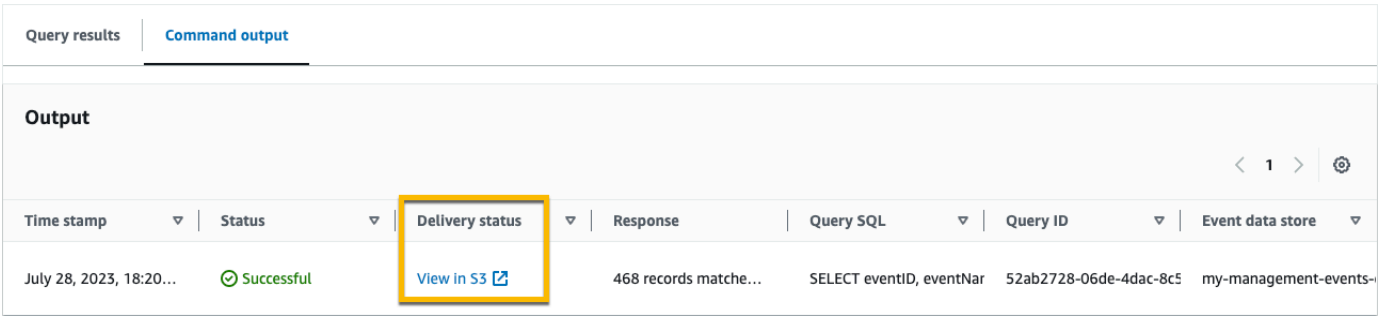
1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインの [Lake] で、[クエリ] を選択します。
3. [サンプルクエリ] または [保存したクエリ] タブ で、[クエリ名] を選択して実行するクエリを選択します。この例では、[ユーザーアクションの調査] という名前のサンプルクエリを選択します。
4. [Event data store] (イベントデータストア) の [Editor] (エディタ) タブで、ドロップダウンリストからイベントデータストアを選択します。リストからイベントデータストアを選択すると、`From`行にイベントデータストア ID CloudTrail が自動的に入力されます。
5. このサンプルクエリでは、`userIdentity.ARN` 値を編集し、`Admin` という名前のユーザーを指定し、`eventTime` の値はデフォルトのままとします。クエリを実行すると、スキャンされたデータ量に応じて料金が発生します。コストを抑えるため、クエリに開始および終了 `eventTime` タイムスタンプを追加することで、クエリを制限することをお勧めします。

6. [結果を S3 に保存] を選択し、クエリ結果を S3 バケットに保存します。デフォルトの S3 バケットを選択すると、 CloudTrail 必要なバケットポリシーが作成され、適用されます。デフォルトの S3 バケットを選択した場合、IAM `s3:PutEncryptionConfiguration` ポリシーにはアクションのアクセス権限を含める必要があります。デフォルトではバケットのサーバー側の暗号化が有効になっているためです。この例では、デフォルトの S3 バケットを使用します。

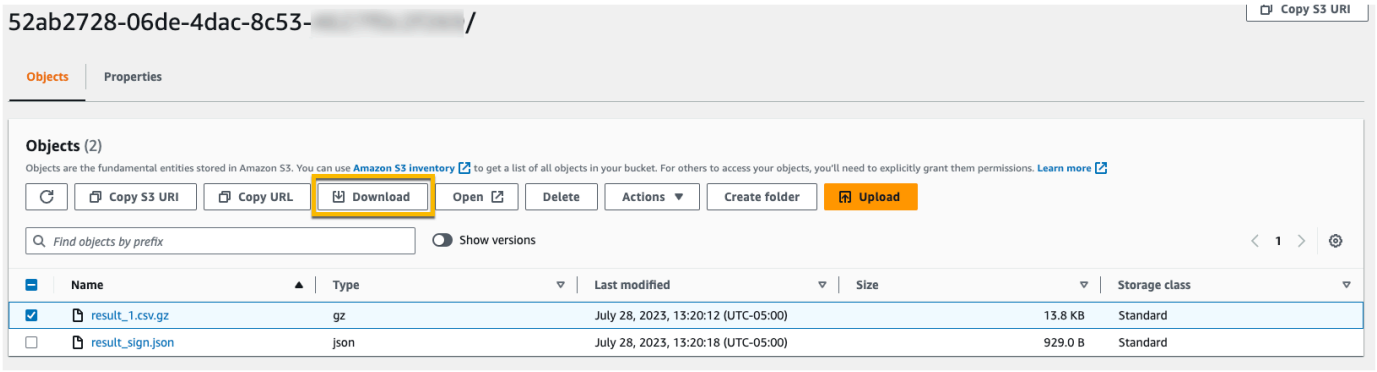
> **Note**
>
> 別のバケットを使用するには、バケット名を指定するか、[Browse S3] (S3 を閲覧) を選択してバケットを選択します。バケットポリシーは、 CloudTrail クエリ結果をバケットに配信するアクセス権限を付与する必要があります。バケットポリシーを手動で編集する方法については、CloudTrail レイククエリ結果の Amazon S3 バケットポリシー を参照してください。

7. [実行] を選択します。イベントデータストアのサイズと、それに含まれるデータの日数によっては、クエリの実行に数分かかる場合があります。[Command output] (コマンド出力) タブには、クエリのステータスと、クエリの実行が終了したかどうかが表示されます。クエリの実行が終了したら、[Query results] (クエリ結果) タブを開いて、アクティブなクエリ (現在エディタに表示されているクエリ) の結果の表を表示します。
8. 保存したクエリ結果を S3 バケットに配信すると CloudTrail 、Delivery status 列には、保存したクエリ結果ファイルと、保存したクエリ結果の検証に使用できる署名ファイルが含まれる S3 バケットへのリンクが表示されます。[S3 で表示] を選択すると、S3 バケット内のクエリ結果ファイルと署名ファイルが表示されます。

> **Note**
>
> クエリ結果を保存すると、S3 CloudTrail バケットに表示される前にクエリ結果がコンソールに表示される場合があります。これは、 CloudTrail クエリスキャンの完了後にクエリ結果が配信されるためです。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。 CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。クエリスキャンの完了後、S3 バケットに配信されるデータは、1 GB あたり平均 60～90 秒の遅延が見込まれます。



9. クエリ結果をダウンロードするには、クエリ結果ファイル (この例では、`result_1.csv.gz`) を選択し、[ダウンロード] を選択します。



保存したクエリ結果の検証の詳細については、「保存されたクエリ結果の検証」を参照してください。

クエリ結果を表示する

クエリが終了したら、その結果を表示できます。クエリの結果は、クエリの終了後 7 日間使用できます。アクティブなクエリの結果は、[Query results] (クエリ結果) タブで表示できます。または、[Lake] ホームページの [Results history] (結果履歴) タブで、最近のクエリすべての結果にアクセスすることができます。

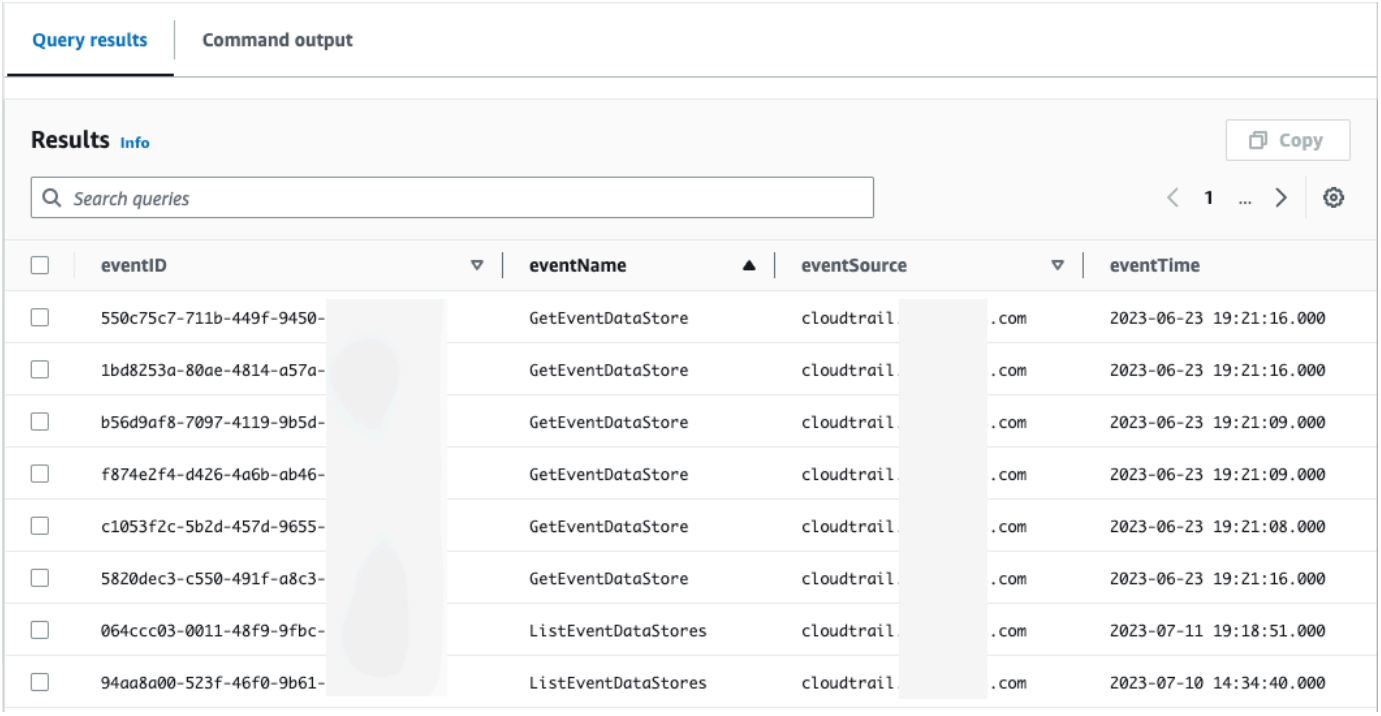
クエリとクエリの間にクエリ期間内の後続イベントがログに記録される場合があるため、クエリの結果は古いクエリ実行と新しいクエリ実行で変化する場合があります。

クエリ結果を保存すると、クエリ結果が S3 CloudTrail バケットに表示される前にコンソールに表示される場合があります。これは、 CloudTrail クエリスキャンの完了後にクエリ結果が配信されるためです。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。 クエリースキャンが完

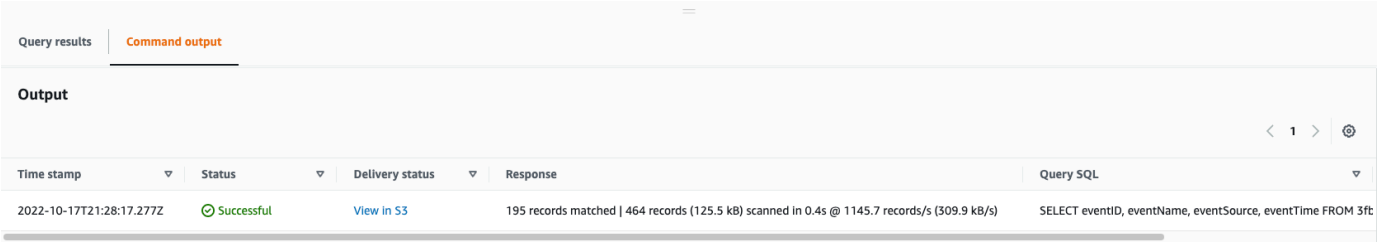
了すると、S3 バケットにデータが配信されるたびに、平均 60 ~ 90 秒のレイテンシーが発生することが予想されます。保存したクエリ結果の検索とダウンロードの詳細については、「保存されたクエリ結果のダウンロード」を参照してください。

> **Note**
>
> 1 時間以上実行するクエリは、タイムアウトすることがあります。クエリがタイムアウトする前に処理された部分的な結果を引き続き取得できます。 CloudTrail クエリ結果の一部は S3 バケットには配信されません。タイムアウトを回避するには、クエリを絞り込んでスキャンされるデータ量を制限する時間範囲を狭くすることができます。

1. アクティブなクエリの [Query results] (クエリ結果) タブでは、各行がクエリに一致したイベント結果を表しています。検索バーにイベントフィールドの値を全部または一部入力して、結果をフィルタリングします。イベントをコピーするには、コピーするイベントを選択し、[コピー] をクリックします。



2. [Command output] (コマンド出力) タブで、イベントデータストア ID、実行時間、スキャンされた結果の数、およびクエリが成功したかどうかなど、実行されたクエリに関するメタデータを表示します。クエリ結果を Amazon S3 バケットに保存した場合、メタデータには保存されたクエリ結果を含む S3 バケットへのリンクも含まれます。



保存されたクエリ結果のダウンロード

クエリ結果を保存したら、クエリ結果を含むファイルを見つけられる必要があります。 CloudTrail クエリ結果を保存するときに指定した Amazon S3 バケットにクエリ結果を配信します。

> **Note**
>
> CloudTrail クエリスキャンの完了後にクエリ結果が配信されるため、クエリ結果を保存すると、S3 バケットに表示される前にクエリ結果がコンソールに表示される場合があります。ほとんどのクエリは数分で完了しますが、イベントデータストアのサイズによっては、クエリ結果が S3 CloudTrail バケットに配信されるまでにかなり長い時間がかかる場合があります。 CloudTrail クエリ結果を圧縮された gzip 形式で S3 バケットに配信します。クエリスキャンの完了後、S3 バケットに配信されるデータは、1 GB あたり平均 60～90 秒の遅延が見込まれます。

トピック

- CloudTrail Lake に保存したクエリ結果を検索できます。
- CloudTrail Lake に保存したクエリ結果をダウンロードします。

CloudTrail Lake に保存したクエリ結果を検索できます。

CloudTrail クエリ結果と署名ファイルを S3 バケットに公開します。クエリ結果ファイルには保存されたクエリの出力が含まれ、署名ファイルはクエリ結果の署名とハッシュ値を提供します。署名ファイルを使用してクエリ結果を検証できます。クエリ結果検証の詳細については、「保存されたクエリ結果の検証」を参照してください。

クエリ結果ファイルまたは署名ファイルを取得するには、Amazon S3 コンソール、Amazon S3 コマンドラインインターフェイス (CLI)、または API を使用します。

Amazon S3 コンソールでクエリ結果ファイルと署名ファイルを見つけるには

1. Amazon S3 コンソールを開きます。
2. 指定したバケットを選択します。
3. 必要なクエリ結果ファイルおよび署名ファイルが見つかるまでオブジェクト階層内を移動します。クエリ結果ファイルの拡張子は.csv.gz、署名ファイルの拡張子は.json です。

次の例のように、オブジェクト階層を移動しますが、バケット名、アカウント ID、日付、およびクエリ ID は異なります。

```
All Buckets
    Bucket_Name
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

CloudTrail Lake に保存したクエリ結果をダウンロードします。

クエリ結果を保存すると、2 種類のファイルが Amazon S3 CloudTrail バケットに配信されます。

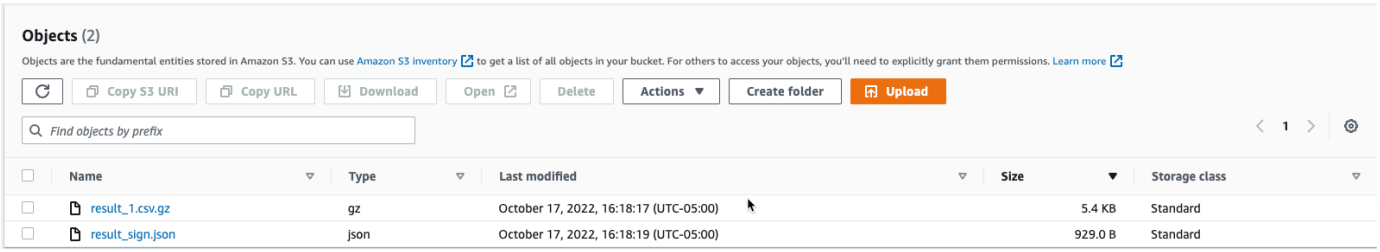
- クエリ結果ファイルの検証に使用できる JSON 形式の署名ファイル。署名ファイルは result_sign.json と名付けられています。署名ファイルの詳細については、「CloudTrail 署名ファイル構造」を参照してください。
- クエリからの結果を含む CSV 形式の 1 つ以上のクエリ結果ファイル。配信されるクエリ結果ファイルの数は、クエリ結果の合計サイズによって異なります。クエリ結果の最大ファイルサイズは 1 TB です。各クエリ結果ファイルには、result_*number*.csv.gz という名前が付けられています。たとえば、クエリ結果の合計サイズが 2 TB の場合、result_1.csv.gz と result_2.csv.gz という 2 つのクエリ結果ファイルを受信します。

CloudTrail クエリ結果と署名ファイルは Amazon S3 オブジェクトです。S3 コンソール、 AWS Command Line Interface (CLI)、または S3 API を使用して、クエリ結果を取得し、ファイルに署名できます。

以下の手順では、Amazon S3 コンソールを使用してクエリ結果をダウンロードし、ファイルに署名する方法について説明します。

Amazon S3 コンソールでクエリ結果ファイルまたは署名ファイルをダウンロードするには

1. Amazon S3 コンソールを開きます。
2. バケットを選択して、ダウンロードするファイルを選択します。



3. [Download] (ダウンロード) を選択し、プロンプトに従ってファイルを保存します。

> **Note**
>
> Chrome などの一部のブラウザでは、クエリ結果ファイルが自動的に抽出されます。その場合は、ステップ 5 に進みます。

4. 7-Zip のような製品を使用して、クエリ結果ファイルを抽出します。
5. クエリ結果ファイルまたは署名ファイルを開きます。

保存されたクエリ結果の検証

CloudTrail クエリ結果の配信後にクエリ結果が変更されたか、削除されたか、変更されていないかを判断するには、 CloudTrail クエリ結果の整合性検証を使用できます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、検出されない限り、クエリ結果ファイルを変更、削除、 CloudTrail または偽造することが計算上不可能になります。コマンドラインを使用してクエリ結果ファイルを検証できます。

使用する理由

検証されたクエリ結果ファイルは、セキュリティおよびフォレンシック調査で非常に重要です。たとえば、検証済みのクエリ結果ファイルを使用することで、クエリ結果ファイル自体が変更されていないことを明確に主張できます。 CloudTrail クエリ結果ファイルの整合性検証プロセスでは、クエリ結果ファイルが削除または変更されたかどうかもわかります。

トピック

保存したクエリ結果を、で検証します。 AWS CLI

aws cloudtrail verify-query-results コマンドを使用して、クエリ結果ファイルの整合性を検証してファイルに署名できます。

前提条件

コマンドラインを使用してクエリ結果の整合性を検証するには、次の条件を満たしている必要があります。

- へのオンライン接続が必要です AWS。
- AWS CLI バージョン 2 を使用する必要があります。
- ローカルでクエリ結果ファイルを検証してファイルに署名する場合、次の条件が適用されます。
  - 指定したファイルパスにクエリ結果ファイルと署名ファイルを配置する必要があります。--local-export-path パラメータの値としてファイルパスを指定します。
  - クエリ結果ファイルと署名ファイルの名前は変更しません。
- S3 バケットでクエリ結果ファイルを検証してファイルに署名する場合、次の条件が適用されます。
  - クエリ結果ファイルと署名ファイルの名前は変更しません。
  - クエリ結果ファイルの署名ファイルを含む Amazon S3 バケットへの読み取りアクセスが必要です。
  - 指定した S3 プレフィックスには、クエリ結果ファイルと署名ファイルが含まれている必要があります。--s3-prefix パラメータの値として S3 プレフィックスを指定します。

verify-query-results

verify-query-results コマンドは、各クエリ結果ファイルのハッシュ値を署名ファイル内の `fileHashValue` と比較し、署名ファイルの `hashSignature` を検証することによってクエリ結果ファイルのハッシュ値を検証します。

クエリ結果を検証する場合、--s3-bucket および --s3-prefix のいずれかのコマンドラインオプションを使用して S3 バケットに保存されているクエリ結果ファイルと署名ファイルを検証するか、--local-export-path コマンドラインオプションを使用して、ダウンロードしたクエリ結果ファイルと署名ファイルのローカル検証を実行することができます。

> **Note**
>
> verify-query-results コマンドはリージョン固有です。特定のクエリ結果を検証するには、--regionグローバルオプションを指定する必要があります AWS リージョン。

verify-query-results コマンドのオプションを以下に示します。

--s3-bucket *<###>*

クエリ結果ファイルと署名ファイルを保存する S3 バケット名を指定します。このパラメータは --local-export-path と共に使用できません。

--s3-prefix *<###>*

クエリ結果ファイルと署名ファイルを含む S3 フォルダーの S3 パスを指定します (`s3/path/` など)。このパラメータは --local-export-path と共に使用できません。ファイルが S3 バケットのルートディレクトリにある場合は、このパラメータを指定する必要はありません。

--local-export-path *<###>*

クエリ結果ファイルと署名ファイルを含むローカルディレクトリを指定します (`/local/path/to/export/file/` など)。このパラメータは --s3-bucket や --s3-prefix と共に使用できません。

例

次の例では、--s3-bucket および --s3-prefix コマンドラインオプションを使用してクエリ結果を検証し、クエリ結果ファイルと署名ファイルを含む S3 バケット名とプレフィックスを指定します。

```
aws cloudtrail verify-query-results --s3-bucket bucket_name --s3-prefix prefix --
region region
```

次の例では、--local-export-path コマンドラインオプションを使用して、ダウンロードしたクエリ結果を検証し、クエリ結果ファイルと署名ファイルのローカルパスを指定します。クエリ結果ファイ

ルのダウンロードの詳細については、「CloudTrail Lake に保存したクエリ結果をダウンロードします。」を参照してください。

```
aws cloudtrail verify-query-results --local-export-path local_file_path --region region
```

検証結果

次の表は、クエリ結果ファイルと書名ファイルの検証メッセージを示しています。

ファイルタイプ	検証メッセージ	説明
Sign file	Successfully validated sign and query result files	書名ファイルの署名は有効です。参照しているクエリ結果ファイルを確認できます。
Query result file	ValidationError: "File *file_name* has inconsistent hash value with hash value recorded in sign file, hash value in sign file is *expected_hash* , but get *computed_hash*	クエリ結果ファイルのハッシュ値が署名ファイルの fileHashValue と一致しなかったため、検証に失敗しました。
Sign file	ValidationError: Invalid signature in sign file	署名が無効なため、署名ファイルの検証に失敗しました。

CloudTrail 署名ファイル構造

署名ファイルには、クエリ結果を保存したときに Amazon S3 バケットに送られた各クエリ結果ファイルの名前、各クエリ結果ファイルのハッシュ値、ファイルのデジタル署名が含まれます。デジタル署名とハッシュ値は、クエリ結果ファイルおよび署名ファイル自体の整合性を検証するために使用されます。

署名ファイルの場所

署名ファイルは、次の構文で表される Amazon S3 バケットの場所に送られます。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-ID/CloudTrail-Lake/
Query/year/month/date/query-ID/result_sign.json
```

署名ファイルのコンテンツの例

以下のサンプルサインファイルには、 CloudTrail Lake のクエリ結果の情報が含まれています。

```
{
  "version": "1.0",
  "region": "us-east-1",
  "files": [
    {
      "fileHashValue" :
 "de85a48b8a363033c891abd723181243620a3af3b6505f0a44db77e147e9c188",
      "fileName" : "result_1.csv.gz"
    }
  ],
  "hashAlgorithm" : "SHA-256",
  "signatureAlgorithm" : "SHA256withRSA",
  "queryCompleteTime": "2022-05-10T22:06:30Z",
  "hashSignature" :
 "7664652aaf1d5a17a12ba50abe6aca77c0ec76264bdf7dce71ac6d1c7781117c2a412e5820bccf473b1361306dff6
  "publicKeyFingerprint" : "67b9fa73676d86966b449dd677850753"
}
```

署名ファイルのフィールドの説明

以下では、署名ファイルの各フィールドについて説明します。

`version`

署名ファイルのバージョン。

`region`

AWS クエリ結果の保存に使用されたアカウントのリージョン。

`files.fileHashValue`

圧縮されたクエリ結果ファイルの内容の 16 進エンコードされたハッシュ値です。

`files.fileName`

クエリ結果ファイルの名前。

`hashAlgorithm`

クエリ結果ファイルのハッシュ計算に使用されたハッシュアルゴリズムです。

`signatureAlgorithm`

ファイルの署名に使用されるアルゴリズムです。

`queryCompleteTime`

クエリ結果が S3 CloudTrail バケットに配信された日時を示します。この値を使用してパブリックキーを検索できます。

`hashSignature`

ファイルのハッシュ署名。

`publicKeyFingerprint`

このファイルの署名に使用されたパブリックキーの 16 進エンコードされたフィンガープリントです。

CloudTrail クエリ結果ファイルの整合性検証のカスタム実装

CloudTrail 業界標準の公開されている暗号アルゴリズムとハッシュ関数を使用しているため、独自のツールを作成してクエリ結果ファイルの整合性を検証できます。 CloudTrail クエリ結果を Amazon S3 バケットに保存すると、署名ファイルが S3 CloudTrail バケットに配信されます。独自の検証ソリューションを実装して、署名ファイルとクエリ結果ファイルを検証できます。署名ファイルの詳細については、「CloudTrail 署名ファイル構造」を参照してください。

このトピックでは、署名ファイルの署名方法について説明し、署名ファイルと、署名ファイルによって参照される署名ファイルを検証するソリューションの実装に必要な手順を詳しく示します。

CloudTrail 署名ファイルの署名方法を理解する

CloudTrail 署名ファイルは RSA デジタル署名で署名されます。各署名ファイルについて、CloudTrail次の処理を行います。

1. 各クエリ結果ファイルのハッシュ値を含むハッシュリストを作成します。
2. リージョンに固有のプライベートキーを取得します。
3. 文字列の SHA-256 ハッシュとプライベートキーを RSA 署名アルゴリズムに渡すと、そこでデジタル署名が作成されます。
4. 署名のバイトコードを 16 進形式にエンコードします。
5. デジタル署名を署名ファイルに入力します。

データ署名文字列の内容

データ署名文字列は、スペースで区切られた各クエリ結果ファイルのハッシュ値で構成されます。署名ファイルには、各クエリ結果ファイルの `fileHashValue` がリストされています。

カスタム検証を実装する手順

カスタム検証ソリューションを実装するときは、最初にダイジェストファイルを検証してから、署名ファイルと参照するクエリ結果ファイルを検証する必要があります。

署名ファイルを検証する

署名ファイルを検証するには、署名、対応するプライベートキーが署名に使用されたパブリックキー、計算したデータ署名文字列が必要です。

1. 署名ファイルを入手してください。
2. 本来の場所から署名ファイルが取得されたことを確認します。
3. 署名ファイルの 16 進エンコードされた署名を取得します。
4. パブリックキー (対応するプライベートキーが署名ファイルの署名に使用された) の 16 進エンコードされたフィンガープリントを取得します。
5. 署名ファイルで `queryCompleteTime` に対応する時間範囲のパブリックキーを取得します。時間範囲には、「`StartTime` より早い `queryCompleteTime`」および「`EndTime` より遅い `queryCompleteTime`」を選択します。

6. 取得したパブリックキーの中から、フィンガープリントが署名ファイルの publicKeyFingerprint の値と一致するパブリックキーを選択します。
7. 各クエリ結果ファイルのハッシュ値をスペースで区切ったハッシュリストを使用して、署名ファイルの署名を検証するために使用するデータ署名文字列を再作成します。署名ファイルには、各クエリ結果ファイルの fileHashValue がリストされています。

   たとえば、署名ファイルの files 配列に次の 3 つのクエリ結果ファイルが含まれている場合、ハッシュリストは「aaa bbb ccc」になります。

```
“files": [

   {

        "fileHashValue" : “aaa”,

        "fileName" : "result_1.csv.gz"

   },
   {

        "fileHashValue" : “bbb”,

        "fileName" : "result_2.csv.gz"

   },
   {

        "fileHashValue" : “ccc”,

        "fileName" : "result_3.csv.gz"

   }
],
```

8. 文字列の SHA-256 ハッシュ、パブリックキー、署名を、パラメータとしてRSA 署名検証アルゴリズムに渡して、署名を検証します。結果が true の場合、署名ファイルは有効です。

クエリ結果ファイルを検証する

署名ファイルが有効な場合は、署名ファイルが参照するクエリ結果ファイルを検証します。クエリ結果ファイルの整合性を検証するには、圧縮されたコンテンツの SHA-256 ハッシュ値を計算し、その

結果を署名ファイルに記録されているクエリ結果ファイルの fileHashValue と比較します。ハッシュが一致する場合、クエリ結果ファイルは有効です。

以下のセクションではこの検証を詳しく説明します。

A. 署名ファイルを取得する

最初の手順は、署名ファイルを取得し、パブリックキーのフィンガープリントを取得することです。

1. 検証するクエリ結果の署名ファイルを Amazon S3 バケットから取得します。
2. 次に、署名ファイルから hashSignature の値を取得します。
3. 署名ファイルで、署名ファイルの署名に使用されたプライベートキーに対応するパブリックキーのフィンガープリントを publicKeyFingerprint フィールドから取得します。

B. 署名ファイルの検証のためにパブリックキーを取得する

署名ファイルを検証するための公開鍵を取得するには、 AWS CLI または CloudTrail API を使用できます。どちらの場合も、検証しようとする署名ファイルの時間範囲 (開始時刻と終了時刻) を指定します。署名ファイル内の queryCompleteTime に対応する時間範囲を使用してください。指定した時間範囲について 1 つ以上のパブリックキーが返されることがあります。返されたキーの有効な時間範囲が重複する可能性があります。

> **Note**
>
> CloudTrail リージョンごとに異なる秘密鍵と公開鍵のペアを使用するため、各署名ファイルはそのリージョン固有の秘密鍵で署名されます。したがって、特定のリージョンの署名ファイルを検証するときは、同じリージョンからパブリックキーを取得する必要があります。

AWS CLI を使用して公開鍵を取得してください。

を使用して署名ファイルの公開鍵を取得するには AWS CLI、cloudtrail list-public-keysコマンドを使用します。このコマンドの形式は次のとおりです。

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

start-time および end-time パラメータには UTC タイムスタンプを使用します。これらはオプションです。指定しない場合、現在の時刻が使用され、現在アクティブなパブリックキー (1 つまたは複数) が返されます。

レスポンス例

レスポンスは、返されるキー (1 つまたは複数) を表す JSON オブジェクトのリストです。

CloudTrail API を使用してパブリックキーを取得します。

CloudTrail API を使用して署名ファイルの公開鍵を取得するには、開始時刻と終了時刻の値を ListPublicKeys API に渡します。この ListPublicKeys API は、指定された時間範囲内の、対応するプライベートキーが署名ファイルの署名に使用されたパブリックキーを返します。API は、各パブリックキーに対応するフィンガープリントも返します。

ListPublicKeys

このセクションでは、ListPublicKeys API のリクエストパラメータとレスポンス要素について説明します。

> **Note**
>
> ListPublicKeys のバイナリフィールドのエンコードは変更される可能性があります。

リクエストパラメータ

名前	説明
StartTime	オプションで、 CloudTrail 署名ファイルの公開鍵を検索する時間範囲の開始時間を UTC で指定します。 StartTime 指定されていない場合は、現在の時刻が使用され、現在の公開鍵が返されます。 タイプ: DateTime
EndTime	オプションで、 CloudTrail 署名ファイルの公開鍵を検索する時間範囲の終了時間を UTC で指定します。指定しない場合は EndTime 、現在の時刻が使用されます。 タイプ: DateTime

レスポンス要素

PublicKeyList は、次の要素を含む PublicKey オブジェクトの配列です。

名前	説明
Value	DER エンコードされたパブリックキー値 (PKCS #1 形式)。 型: Blob
ValidityStartTime	パブリックキーの有効期間の開始時刻。 タイプ: DateTime
ValidityEndTime	パブリックキーの有効期間の終了時刻。 タイプ: DateTime
Fingerprint	パブリックキーのフィンガープリント。フィンガープリントを使用して、署名ファイルの検証に使用する必要があるパブリックキーを特定できます。 型: 文字列

C. 検証に使用するパブリックキーを選択する

list-public-keys または ListPublicKeys によって取得されたパブリックキーの中から、そのフィンガープリントが署名ファイルの publicKeyFingerprint フィールドに記録されているフィンガープリントと一致するパブリックキーを選択します。これは署名ファイルの検証に使用するパブリックキーです。

D. データ署名文字列を再作成する

署名ファイルの署名と、関連付けられたパブリックキーを取得しました。次は、データ署名文字列を計算する必要があります。データ署名文字列の計算が完了すると、署名の検証に必要な入力を得られます。

データ署名文字列は、スペースで区切られた各クエリ結果ファイルのハッシュ値で構成されます。この文字列を再作成した後、署名ファイルを検証できます。

E. 署名ファイルを検証する

再作成したデータ署名文字列、デジタル署名、パブリックキーを、RSA 署名検証アルゴリズムに渡します。出力が true の場合、署名ファイルの署名が検証され、署名ファイルは有効です。

F. クエリ結果ファイルを検証する

署名ファイルの検証が完了したら、クエリ結果ファイルが参照するログファイルを検証することができます。署名ファイルにはクエリ結果ファイルの SHA-256 ハッシュが含まれています。 CloudTrail クエリ結果ファイルのいずれかが配信後に変更された場合、SHA-256 ハッシュが変更され、署名ファイルの署名が一致しなくなります。

以下の手順を使用して、署名ファイルの `files` 配列にリストされているクエリ結果ファイルを検証します。

1. 署名ファイル内で、`files.fileHashValue` フィールドからファイルの元のハッシュを取得します。
2. `hashAlgorithm` で指定されたハッシュアルゴリズムを使用して、クエリ結果ファイルの圧縮されたコンテンツをハッシュします。
3. クエリ結果ファイルごとに生成したハッシュ値を署名ファイルの `files.fileHashValue` と比較します。ハッシュが一致する場合、クエリ結果ファイルは有効です。

署名とクエリ結果ファイルのオフライン検証

署名ファイルとクエリ結果ファイルをオフラインで検証するとき、通常は前のセクションで説明した手順に従います。ただし、パブリックキーに関する次の情報を考慮する必要があります。

パブリックキー

オフラインで検証するには、所定の時間範囲のクエリ結果ファイルの検証に必要なパブリックキーを最初にオンラインで取得し (たとえば、`ListPublicKeys` を呼び出す)、オフラインで保存する必要があります。指定した最初の時間範囲外の他のファイルを検証するには、常にこの手順を繰り返す必要があります。

検証のサンプルスニペット

次のサンプルスニペットは、 CloudTrail 署名ファイルとクエリ結果ファイルを検証するためのスケルトンコードを示しています。このスケルトンコードはオンラインでもオフラインでも使用できます。つまり、実装する際に AWSとのオンライン接続を使用するかどうかはユーザーが決めることができます。推奨の実装では、Java Cryptography Extension (JCE) と Bouncy Castle をセキュリティプロバイダーとして使用しています。

サンプルスニペットには次の内容が含まれます。

- 署名ファイルの署名の検証に使用されるデータ署名文字列を作成する方法。

- 署名ファイルの署名を確認する方法。
- クエリ結果ファイルのハッシュ値を計算し、それを署名ファイルにリストされている fileHashValue と比較して、クエリ結果ファイルの信頼性を検証する方法。

```
import org.apache.commons.codec.binary.Hex;
import org.bouncycastle.asn1.pkcs.PKCSObjectIdentifiers;
import org.bouncycastle.asn1.pkcs.RSAPublicKey;
import org.bouncycastle.asn1.x509.AlgorithmIdentifier;
import org.bouncycastle.asn1.x509.SubjectPublicKeyInfo;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.json.JSONArray;
import org.json.JSONObject;

import java.security.KeyFactory;
import java.security.MessageDigest;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;
import java.util.stream.Collectors;


public class SignFileValidationSampleCode {

    public void validateSignFile(String s3Bucket, String s3PrefixPath) throws Exception
 {
        MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

        // Load the sign file from S3 (using Amazon S3 Client) or from your local copy
        JSONObject signFile = loadSignFileToMemory(s3Bucket, String.format("%s/%s",
 s3PrefixPath, "result_sign.json"));

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        List<String> hashList = new ArrayList<>();

        JSONArray jsonArray = signFile.getJSONArray("files");
```

```
       for (int i = 0; i < jsonArray.length(); i++) {
           JSONObject file = jsonArray.getJSONObject(i);
           String fileS3ObjectKey = String.format("%s/%s", s3PrefixPath,
file.getString("fileName"));

           // Load the export file from S3 (using Amazon S3 Client) or from your local
copy
           byte[] exportFileContent = loadCompressedExportFileInMemory(s3Bucket,
fileS3ObjectKey);
           messageDigest.update(exportFileContent);
           byte[] exportFileHash = messageDigest.digest();
           messageDigest.reset();
           byte[] expectedHash = Hex.decodeHex(file.getString("fileHashValue"));

           boolean signaturesMatch = Arrays.equals(expectedHash, exportFileHash);
           if (!signaturesMatch) {
               System.err.println(String.format("Export file: %s/%s hash doesn't
match.\tExpected: %s Actual: %s",
                       s3Bucket, fileS3ObjectKey,
                       Hex.encodeHexString(expectedHash),
Hex.encodeHexString(exportFileHash)));
           } else {
               System.out.println(String.format("Export file: %s/%s hash match",
                       s3Bucket, fileS3ObjectKey));
           }

           hashList.add(file.getString("fileHashValue"));
       }
       String hashListString = hashList.stream().collect(Collectors.joining(" "));

       /*
           NOTE:
           To find the right public key to verify the signature, call CloudTrail
ListPublicKey API to get a list
           of public keys, then match by the publicKeyFingerprint in the sign file.
Also, the public key bytes
           returned from ListPublicKey API are DER encoded in PKCS#1 format:

           PublicKeyInfo ::= SEQUENCE {
               algorithm       AlgorithmIdentifier,
               PublicKey       BIT STRING
           }
```

```
            AlgorithmIdentifier ::= SEQUENCE {
                algorithm       OBJECT IDENTIFIER,
                parameters      ANY DEFINED BY algorithm OPTIONAL
            }
        */
        byte[] pkcs1PublicKeyBytes =
 getPublicKey(signFile.getString("queryCompleteTime"),
                signFile.getString("publicKeyFingerprint"));
        byte[] signatureContent = Hex.decodeHex(signFile.getString("hashSignature"));

        // Transform the PKCS#1 formatted public key to x.509 format.
        RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
        AlgorithmIdentifier rsaEncryption = new
 AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
        SubjectPublicKeyInfo publicKeyInfo = new SubjectPublicKeyInfo(rsaEncryption,
 rsaPublicKey);

        // Create the PublicKey object needed for the signature validation
        PublicKey publicKey = KeyFactory.getInstance("RSA", "BC")
                .generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

        // Verify signature
        Signature signature = Signature.getInstance("SHA256withRSA", "BC");
        signature.initVerify(publicKey);
        signature.update(hashListString.getBytes("UTF-8"));

        if (signature.verify(signatureContent)) {
            System.out.println("Sign file signature is valid.");
        } else {
            System.err.println("Sign file signature failed validation.");
        }

        System.out.println("Sign file validation completed.");
    }
}
```

を使用して CloudTrail Lake クエリの実行と管理を行います。 AWS CLI

を使用して CloudTrail Lake クエリの実行と管理を行うことができます。 AWS CLI を使用するときは AWS CLI、 AWS リージョン コマンドはプロファイルに設定されているもので実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

CloudTrail Lake クエリで使用できるコマンド

CloudTrail Lake でクエリを実行および管理するためのコマンドには以下が含まれます。

- `start-query`クエリを実行するには。
- `describe-query`クエリに関するメタデータを返す。
- `get-query-results`指定したクエリ ID のクエリ結果を返します。
- `list-queries`指定したイベントデータストアのクエリのリストを取得します。
- `cancel-query`実行中のクエリをキャンセルします。

CloudTrail Lake イベントデータストアで使用できるコマンドのリストについては、を参照してください[イベントデータストアで使用できるコマンド]。

CloudTrail Lake インテグレーションで使用できるコマンドのリストについては、を参照してください [CloudTrail Lake インテグレーションで使用できるコマンド]。

でクエリを開始してください。 AWS CLI

AWS CLI start-query以下のコマンド例は、クエリステートメントで ID として指定されたイベントデータストアに対してクエリを実行し、クエリ結果を指定した S3 バケットに配信します。`--query-statement` パラメータは、一重引用符で囲まれた SQL クエリを提供します。オプションのパラメータには、指定された S3 バケットにクエリ結果を配信するための `--delivery-s3uri` が含まれます。 CloudTrail Lake で使用できるクエリ言語の詳細については、「」を参照してください[CloudTrail レイク SQL 制約]。

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3uri "s3://aws-cloudtrail-lake-query-results-123456789012-us-east-1"
```

レスポンスは `QueryId` 文字列です。クエリのステータスを取得するには、start-query によって返された `QueryId` 値を使用して describe-query を実行します。クエリが成功した場合は、get-query-results を実行して結果を取得できます。

出力

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE"
```

```
}
```

> **Note**
>
> 1 時間以上実行するクエリは、タイムアウトすることがあります。クエリがタイムアウトする前に、処理済みの部分的な結果を取得することはできます。`--delivery-s3uri`オプションのパラメータを使用してクエリ結果を S3 バケットに配信する場合、バケットポリシーは、 CloudTrailクエリ結果をバケットに配信する権限を付与する必要があります。バケットポリシーを手動で編集する方法については、CloudTrail レイククエリ結果の Amazon S3 バケットポリシー を参照してください。

を使用してクエリに関するメタデータを取得します。 AWS CLI

AWS CLI describe-query以下のコマンド例は、クエリに関するメタデータを取得します。これには、クエリの実行時間 (ミリ秒単位)、スキャンおよび照合されたイベントの数、スキャンされた合計バイト数、クエリステータスが含まれます。BytesScanned 値は、クエリが実行中でない限り、ユーザーのアカウントがクエリに対して請求されるバイト数と一致します。クエリ結果が S3 バケットに配信された場合、応答では S3 URI と配信ステータスも提供されます。

`--query-id` または `--query-alias` パラメータのいずれかの値を指定する必要があります。`--query-alias` パラメータを指定すると、エイリアスに対して最後に実行されたクエリに関する情報が返されます。

```
aws cloudtrail describe-query --query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

以下に、応答の例を示します。

```
{
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "EventsMatched": 10,
        "EventsScanned": 1000,
        "BytesScanned": 35059,
        "ExecutionTimeInMillis": 3821,
        "CreationTime": "1598911142"
```

```
    }
}
```

を使用してクエリ結果を取得します。 AWS CLI

以下のサンプル AWS CLI get-query-results コマンドは、クエリのイベントデータ結果を取得します。start-query コマンドによって返される --query-id 値を指定します。BytesScanned 値は、クエリが実行中でない限り、ユーザーのアカウントがクエリに対して請求されるバイト数と一致します。オプションのパラメータには、コマンドが単一のページに返す結果の最大数を指定する --max-query-results が含まれます。指定した --max-query-results 値よりも多くの結果がある場合は、返された NextToken 値を追加してコマンドを再度実行し、結果の次のページを取得します。

```
aws cloudtrail get-query-results
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

出力

```
{
    "QueryStatus": "RUNNING",
    "QueryStatistics": {
        "ResultsCount": 244,
        "TotalResultsCount": 1582,
        "BytesScanned":27044
    },
    "QueryResults": [
      {
        "key": "eventName",
        "value": "StartQuery",
      }
   ],
    "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
    "QueryString": "SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10",
    "NextToken": "20add42078135EXAMPLE"
}
```

を使用して、イベントデータストア上のすべてのクエリを一覧表示します。 AWS CLI

以下のサンプル AWS CLI list-queries コマンドは、指定されたイベントデータストアについて、過去 7 日間のクエリとクエリステータスのリストを返します。--event-data-store には、ARN、ま

たは ARN 値の ID サフィックスを指定する必要があります。オプションで、結果のリストを短くするために、--start-time と --end-time パラメータ、および --query-status 値を追加することで、タイムスタンプとしてフォーマットされた時間範囲を指定できます。QueryStatus に有効な値には、QUEUED、RUNNING、FINISHED、FAILED、または CANCELLED が含まれます。

list-queries には、オプションのページ分割パラメータもあります。--max-results を使用して、コマンドが単一のページに返す結果の最大数を指定します。指定した --max-results 値よりも多くの結果がある場合は、返された NextToken 値を追加してコマンドを再度実行し、結果の次のページを取得します。

```
aws cloudtrail list-queries
--event-data-store EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
--query-status CANCELLED
--start-time 1598384589
--end-time 1598384602
--max-results 10
```

出力

```
{
    "Queries": [
        {
          "QueryId": "EXAMPLE2-0add-4207-8135-2d8a4EXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598911142
        },
        {
          "QueryId": "EXAMPLE2-4e89-9230-2127-5dr3aEXAMPLE",
          "QueryStatus": "CANCELLED",
          "CreationTime": 1598296624
        }
     ],
    "NextToken": "20add42078135EXAMPLE"
}
```

実行中のクエリを以下のコマンドでキャンセルします。 AWS CLI

AWS CLI cancel-query以下のコマンド例は、RUNNINGステータスがのクエリをキャンセルします。--query-id に値を指定する必要があります。cancel-query を実行すると、cancel-query 操作がまだ終了していない場合でも、クエリのステータスに CANCELLED が表示されることがあります。

> **Note**
>
> キャンセルされたクエリには、料金が発生する可能性があります。アカウントには、クエリをキャンセルする前にスキャンされたデータ量に対する料金が請求されます。

以下は CLI の例です。

```
aws cloudtrail cancel-query
--query-id EXAMPLEd-17a7-47c3-a9a1-eccf7EXAMPLE
```

出力

```
QueryId -> (string)
QueryStatus -> (string)
```

CloudTrail レイク SQL 制約

CloudTrail レイククエリは SQL 文字列です。このセクションでは、サポートされている関数、演算子、スキーマについて説明します。

SELECT ステートメントのみが許可されます。データを変更できるクエリ文字列はありません。

CloudTrail Lake は Presto のすべての有効な SQL SELECT ステートメント、関数、演算子をサポートしています。サポートされている SQL 関数と演算子の詳細については、Presto ドキュメントウェブサイトの「関数と演算子」を参照してください。

CloudTrail コンソールには、独自のクエリの作成を始めるのに役立つサンプルクエリが多数用意されています。詳細については、「 CloudTrail コンソールにサンプルクエリが表示されます。」を参照してください。

トピック

- サポートされている関数、条件、結合演算子
- 高度なマルチテーブルクエリのサポート

サポートされている関数、条件、結合演算子

サポートされている関数

CloudTrail Lake は Presto のすべての機能をサポートしています。サポートされている関数の詳細については、Presto ドキュメントウェブサイトの「関数と演算子」を参照してください。

CloudTrail Lake INTERVAL はこのキーワードをサポートしていません。

サポートされている条件演算子

以下は、サポートされている条件演算子です。

```
AND
OR
IN
NOT
IS (NOT) NULL
LIKE
BETWEEN
GREATEST
LEAST
IS DISTINCT FROM
IS NOT DISTINCT FROM
<
>
<=
>=
<>
!=
( conditions ) #parenthesised conditions
```

サポートされている結合演算子

以下は、サポートされている JOIN 演算子です。複数テーブルクエリの実行の詳細については、「高度なマルチテーブルクエリのサポート」を参照してください。

```
UNION
UNION ALL
EXCEPT
INTERSECT
LEFT JOIN
RIGHT JOIN
INNER JOIN
```

高度なマルチテーブルクエリのサポート

CloudTrail Lake は複数のイベントデータストアにわたる高度なクエリ言語をサポートしています。

- UNION|UNION ALL|EXCEPT|INTERSECT
- LEFT|RIGHT|INNER JOIN

クエリを実行するには、 AWS CLIの start-query コマンドを使用します。このセクションのサンプルクエリのいずれかを使用した例を次に示します。

```
aws cloudtrail start-query
--query-statement "Select eventId, eventName from EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE
 UNION Select eventId, eventName from EXAMPLEg741-6y1x-9p3v-bnh6iEXAMPLE UNION ALL
 Select eventId, eventName from EXAMPLEb529-4e8f9l3d-6m2z-lkp5sEXAMPLE ORDER BY eventId
 LIMIT 10;"
```

レスポンスは QueryId 文字列です。クエリのステータスを取得するには、start-query によって返された QueryId 値を使用して describe-query を実行します。クエリが成功した場合は、get-query-results を実行して結果を取得できます。

UNION|UNION ALL|EXCEPT|INTERSECT

3 つのイベントデータストア (EDS1、EDS2、および EDS3) 内のイベント ID とイベント名でイベントを検索するために UNION と UNION ALL を使用するサンプルクエリを次に示します。結果は最初に各イベントデータストアから選択されてから連結され、イベント ID 順に並べられます。10 個のイベントに制限されます。

```
Select eventId, eventName from EDS1
UNION
Select eventId, eventName from EDS2
UNION ALL
Select eventId, eventName from EDS3
ORDER BY eventId LIMIT 10;
```

LEFT|RIGHT|INNER JOIN

edsB にマッピングされた eds2 という名前のイベントデータストアから、プライマリ (左) イベントデータストア edsA 内のイベントと一致するすべてのイベントを検索するために LEFT JOIN を使用

するサンプルクエリを次に示します。返されるイベントは 2020 年 1 月 1 日以前に発生したものであり、イベント名のみが返されます。

```
SELECT edsA.eventName, edsB.eventName, element_at(edsA.map, 'test')
FROM eds1 as edsA
LEFT JOIN eds2 as edsB
ON edsA.eventId = edsB.eventId
WHERE edsA.eventtime <= '2020-01-01'
ORDER BY edsB.eventName;
```

サポートされているイベントデータストア用の SQL スキーマ

以下のセクションでは、イベントデータストアの各タイプでサポートされている SQL スキーマについて説明します。

トピック

- CloudTrail イベントレコードフィールドでサポートされるスキーマ
- CloudTrail Insights イベントレコードフィールドでサポートされているスキーマ
- AWS Config 設定項目レコードフィールド用にサポートされているスキーマ
- AWS Audit Manager エビデンスレコードフィールドでサポートされるスキーマ
- 非イベントフィールドのスキーマに対応しました。AWS

CloudTrail イベントレコードフィールドでサポートされるスキーマ

CloudTrail 管理およびデータイベントレコードフィールド用の有効な SQL スキーマを以下に示します。 CloudTrail イベントレコードフィールドの詳細については、を参照してくださいCloudTrail レコードの内容。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "useridentity",
        "Type":
 "struct<type:string,principalid:string,arn:string,accountid:string,accesskeyid:string,
```

```
username:string,sessioncontext:struct<attributes:struct<creationdate:timestamp,

mfaauthenticated:string>,sessionissuer:struct<type:string,principalid:string,arn:string,

accountid:string,username:string>,webidfederationdata:struct<federatedprovider:string,

attributes:map<string,string>>,sourceidentity:string,ec2roledelivery:string,
                ec2issuedinvpc:string>,invokedby:string,identityprovider:string>"
   },
   {
       "Name": "eventtime",
       "Type": "timestamp"
   },
   {
       "Name": "eventsource",
       "Type": "string"
   },
   {
       "Name": "eventname",
       "Type": "string"
   },
   {
       "Name": "awsregion",
       "Type": "string"
   },
   {
       "Name": "sourceipaddress",
       "Type": "string"
   },
   {
       "Name": "useragent",
       "Type": "string"
   },
   {
       "Name": "errorcode",
       "Type": "string"
   },
   {
       "Name": "errormessage",
       "Type": "string"
   },
   {
       "Name": "requestparameters",
```

```
        "Type": "map<string,string>"
    },
    {
        "Name": "responseelements",
        "Type": "map<string,string>"
    },
    {
        "Name": "additionaleventdata",
        "Type": "map<string,string>"
    },
    {
        "Name": "requestid",
        "Type": "string"
    },
    {
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "readonly",
        "Type": "boolean"
    },
    {
        "Name": "resources",
        "Type":
 "array<struct<accountid:string,type:string,arn:string,arnprefix:string>>"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
    {
        "Name": "apiversion",
        "Type": "string"
    },
    {
        "Name": "managementevent",
        "Type": "boolean"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
```

```
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "annotation",
        "Type": "string"
    },
    {
        "Name": "vpcendpointid",
        "Type": "string"
    },
    {
        "Name": "serviceeventdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "edgedevicedetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightdetails",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "tlsdetails",
        "Type":
 "struct<tlsversion:string,ciphersuite:string,clientprovidedhostheader:string>"
    },
    {
        "Name": "sessioncredentialfromconsole",
        "Type": "string"
    },
    {
        "Name": "eventjson",
        "Type": "string"
    }
```

```
    {
        "Name": "eventjsonchecksum",
        "Type": "string"
    }
]
```

CloudTrail Insights イベントレコードフィールドでサポートされているスキーマ

以下は、Insights イベントレコードフィールドのための有効な SQL スキーマです。Insights イベントの場合、eventcategory の値は Insight に、eventtype の値は AwsCloudTrailInsight になります。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
```

```
        "Name": "sharedeventid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "insightsource",
        "Type": "string"
    },
    {
        "Name": "insightstate",
        "Type": "string"
    },
    {
        "Name": "insighteventsource",
        "Type": "string"
    },
    {
        "Name": "insighteventname",
        "Type": "string"
    },
    {
        "Name": "insighterrorcode",
        "Type": "string"
    },
    {
        "Name": "insighttype",
        "Type": "string"
    },
    {
        "Name": "insightContext",
        "Type":
 "struct<baselineaverage:double,insightaverage:double,baselineduration:integer,

 insightduration:integer,attributions:struct<attribute:string,insightvalue:string,
                insightaverage:double,baselinevalue:string,baselineaverage:double>>"
    }
]
```

AWS Config 設定項目レコードフィールド用にサポートされているスキーマ

設定項目レコードフィールドの有効な SQL スキーマを次に示します。設定項目では、eventcategory の値は ConfigurationItem であり、eventtype の値は AwsConfigurationItem です。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<configurationitemversion:string,configurationitemcapturetime:

 string,configurationitemstatus:string,configurationitemstateid:string,accountid:string,
```

```
 resourcetype:string,resourceid:string,resourcename:string,arn:string,awsregion:string,

 availabilityzone:string,resourcecreationtime:string,configuration:map<string,string>,
                supplementaryconfiguration:map<string,string>,relatedevents:string,

 relationships:struct<name:string,resourcetype:string,resourceid:string,
                resourcename:string>,tags:map<string,string>>"
    }
]
```

AWS Audit Manager エビデンスレコードフィールドでサポートされるスキーマ

Audit Manager エビデンスレコードフィールドの有効な SQL スキーマを次に示します。Audit Manager エビデンスレコードフィールドでは、`eventcategory` の値は `Evidence` であり、`eventtype` の値は `AwsAuditManagerEvidence` です。Audit Manager を使用して CloudTrail Lake でエビデンスを集約する方法について詳しくは、『AWS Audit Manager ユーザーガイド』の「エビデンスファインダー」を参照してください。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
```

```
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type": "map<string,string>"
    },
    {
        "Name": "eventdata",
        "Type":
 "struct<attributes:map<string,string>,awsaccountid:string,awsorganization:string,

 compliancecheck:string,datasource:string,eventname:string,eventsource:string,

 evidenceawsaccountid:string,evidencebytype:string,iamid:string,evidenceid:string,

 time:timestamp,assessmentid:string,controlsetid:string,controlid:string,

 controlname:string,controldomainname:string,frameworkname:string,frameworkid:string,

 service:string,servicecategory:string,resourcearn:string,resourcetype:string,

 evidencefolderid:string,description:string,manualevidences3resourcepath:string,
                evidencefoldername:string,resourcecompliancecheck:string>"
    }
]
```

非イベントフィールドのスキーマに対応しました。AWS

AWS 非イベント用の有効な SQL スキーマは次のとおりです。AWS 非イベントの場合、eventcategoryActivityAuditLogの値はで、eventtypeの値はですActivityLog。

```
[
    {
        "Name": "eventversion",
        "Type": "string"
    },
    {
        "Name": "eventcategory",
        "Type": "string"
```

```
    },
    {
        "Name": "eventtype",
        "Type": "string"
    },
        "Name": "eventid",
        "Type": "string"
    },
    {
        "Name": "eventtime",
        "Type": "timestamp"
    },
    {
        "Name": "awsregion",
        "Type": "string"
    },
    {
        "Name": "recipientaccountid",
        "Type": "string"
    },
    {
        "Name": "addendum",
        "Type":
 "struct<reason:string,updatedfields:string,originalUID:string,originaleventid:string>"
    },
    {
        "Name": "metadata",
        "Type": "struct<ingestiontime:string,channelarn:string>"
    },
    {
        "Name": "eventdata",
        "Type": "struct<version:string,useridentity:struct<type:string,

 principalid:string,details:map<string,string>>,useragent:string,eventsource:string,

 eventname:string,eventtime:string,uid:string,requestparameters:map<string,string>>,

 responseelements":map<string,string>>,errorcode:string,errormssage:string,sourceipaddress:stri
                recipientaccountid:string,additionaleventdata":map<string,string>>"
    }
]
```

CloudTrail Lake のユーザー権限の制御

AWS CloudTrail AWS Identity and Access Management (IAM) と統合することで、 CloudTrail Lake AWS やその他の必要なリソースへのアクセスを制御できます。 CloudTrail IAM を使用して、 AWS CloudTrail どのユーザーがイベントデータストアやチャネルを作成、設定、削除できるか、イベントの取り込みを開始または停止できるか、トレイルイベントをコピーできるかを制御できます。詳細については、「Identity and Access Management AWS CloudTrail」を参照してください。

以下のトピックは、権限、ポリシー、 CloudTrail およびセキュリティを理解するのに役立ちます。

- CloudTrail 管理権限の付与
- CloudTrail レイククエリ結果の Amazon S3 バケットポリシー
- 証跡イベントのコピーに必要な許可
- フェデレーションに必要なアクセス許可
- タグに基づいてイベントデータストアへのアクセスを制限するポリシーの例:例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否
- AWS CloudTrail リソースベースのポリシーの例
- 委任された管理者を割り当てるために必要な許可
- Lake CloudTrail イベントデータストア用のデフォルト KMS キーポリシー

CloudTrail Lake コストの管理

AWS CloudTrail Lake イベントデータストアとクエリには料金が発生します。ベストプラクティスとして、 CloudTrail コスト管理に役立つ AWS のサービス および ツールを使用することをお勧めします。また、コスト効率を維持しながら必要なデータをキャプチャするように、イベントデータストアを構成することもできます。 CloudTrail の料金については、「AWS CloudTrail の料金」を参照してください。

トピック

- イベントデータストアの料金オプション
- CloudTrail Lake 料金について
- コスト削減方法に関する推奨事項
- コスト管理に役立つツール
- 以下も参照してください。

イベントデータストアの料金オプション

イベントデータストアを作成するときは、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかるコスト、および、そのイベントデータストアの保持期間のデフォルトと最大が決まります。

次の表は利用可能な料金オプションを説明しています。この表には、コンソールの [料金オプション] とそれに対応する API の `BillingMode` の値と、各オプションの保持期間のデフォルトと最大が一覧表示されています。

料金オプション (コンソール)	BillingMode (API)	説明
[延長可能な 1 年間の保持料金]	`EXTENDABLE_RETENTION_PRICING`	1 か月あたり取り込むイベントデータが 25 TB 未満と予想され、最大 10 年間の柔軟な保持期間を希望する場合にお勧めします。このオプションは、イベントデータストアが AWS Config 設定項目、Audit Manager の証拠、およびイベントを AWS外から収集する場合にもお勧めします。 最初の 366 日間 (デフォルトの保持期間) のストレージは、取り込み料金に含まれており追加コストはありません。366 日が経過すると、延長保持は料金で pay-as-you-go利用できます。 これがデフォルトのオプションです。 デフォルトの保持期間: 366 日間 最大保持期間: 3,653 日
[7 年間の保持料金]	`FIXED_RETENTION_PRICING`	1 か月あたり取り込むイベントデータが 25 TB を超えると予想され、必要な保持期間が最長 7 年の場合にお勧めします。 データの保持は取り込み料金に含まれており、追加料金は発生しません。

料金オプション (コンソール)	BillingMode (API)	説明
		デフォルトの保持期間: 2,557 日間 最長保持期間: 2,557 日間

CloudTrail Lake 料金について

次の表は、 CloudTrail Lake イベントデータストアとクエリで料金が発生する方法に関する情報です。 CloudTrail の料金については、「AWS CloudTrail の料金」を参照してください。

料金タイプ	課金の方法
データの取り込み (非圧縮データ)	CloudTrail Lake の場合、取り込まれた非圧縮データに基づいて支払います。イベントデータストアの料金オプションによって、イベントを取り込むコストが決まります。 • [延長可能な 1 年間の保持料金]: イベントタイプに基づく取り込み料金が設定されます。 • [7 年間の保持料金]: 取り込んだデータ量に基づく取り込み料金が設定されます。毎月取り込まれるデータ量が 25 TB を超えると、非常に大きな節約になります。 証跡イベントのコピー 証跡イベントを Lake にコピーすると、 は gzip (圧縮) 形式で保存されているログを CloudTrail 解凍します。 CloudTrail 次に、ログに含まれるイベントをイベントデータストア CloudTrail にコピーします。非圧縮データのサイズは、実際の Amazon S3 ストレージサイズよりも大きくなる可能性があります。非圧縮データのサイズを概算するには、S3 バケット内のログのサイズに 10 を掛けます。

料金タイプ	課金の方法
	Note CloudTrail は、イベント時間が指定された保持期間よりも古い場合、イベントをコピーしません。適切な保持期間を決定するには、次の式に示すように、コピーしたい最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数の合計を計算します。 保持期間 = *oldest-event-in-days* + *number-days-to-retain* 例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。
データ保持 (最適化され圧縮されたデータ)	CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、圧縮データを高速に取得するために最適化された列指向ストレージ形式です。 イベントデータストアの保持期間は、イベントデータがイベントデータストアに保持される期間を決定します。 CloudTrail Lake は、イベントのイベント時間が指定された保持期間内であるかどうかをチェックして、イベントを保持するかどうかを決定します。例えば、保持期間を 90 日と指定すると、イベント時刻が 90 日を超えると、 はイベント CloudTrail を削除します。 [7 年間の保持料金] オプションを使用するイベントデータストアの場合、ストレージは追加料金なしで取り込み料金に含まれます。 [延長可能な 1 年間の保持料金] オプションを使用するイベントデータストアの場合、最初の 366 日間 (デフォルトの保持期間) のストレージは取り込み料金に無料で含まれています。366 日後、ストレージは で提供され pay-as-you-pricing 、イベントデータストア内の最適化および圧縮されたデータに基づいて課金されます。

料金タイプ	課金の方法
CloudTrail Lake でのクエリの実行 (最適化および圧縮されたデータ)	CloudTrail Lake でクエリを実行すると、スキャンされた最適化および圧縮されたデータの量に基づいて料金が発生します。

コスト削減方法に関する推奨事項

このセクションでは、 CloudTrail Lake を使用する際にコストを削減する方法に関する推奨事項を提供します。

イベントデータストアが収集するイベントの種類と、予想される毎月の取り込み量に基づいて料金オプションを選択する

イベントデータストアを作成するときに、イベントデータストアが収集するイベントの種類と、予想される毎月の取り込み量に基づいて料金オプションを選択します。

1 か月あたり取り込むイベントデータが 25 TB 未満と予想され、最大 10 年間の柔軟な保持期間を希望する場合、[延長可能な 1 年間の保持料金] オプションをお勧めします。通常、このオプションは、設定項目、Audit Manager の証拠、および の外部からイベントを収集する AWS Config イベントデータストアにもお勧めします AWS。

1 か月あたり取り込むイベントデータが 25 TB を超えると予想され、7 年間の保持期間が必要な場合、[7 年間の保持料金] オプションをお勧めします。

イベントデータストアの毎月の取り込み量を時系列で評価する

イベントデータストアの毎月の取り込み量の履歴を評価して、ニーズにより適した料金オプションがあるかどうかを確認します。

[7 年間の保持料金] オプションを使用する既存のイベントデータストアがあり、1 か月あたり取り込むデータが 25 TB 未満の場合は、[延長可能な 1 年間の保持料金] を使用するようにイベントデータストアを更新することを検討してください。7 年間の保持料金オプションを使用するイベントデータストアの場合、CloudTrail コンソール 、、AWS CLIまたは UpdateEventDataStore API オペレーションを使用して料金オプションを変更できます。

[延長可能な 1 年間の保持料金] オプションを使用する既存のイベントデータストアがあり、1 か月あたり取り込むイベントデータが 25 TB を超える場合は、[7 年間の保持料金] の方がニーズに適しているかどうか検討してください。新しい料金オプションを使用するには、イベントデータ

ストアへの取り込みを停止し、[7 年間の保持料金] オプションで新しいイベントデータストアを作成します。

高度なイベントセレクタを使用して、関連性の低いイベントを除外する

CloudTrail 管理イベントまたはデータイベント用にイベントデータストアを設定する場合は、高度なイベントセレクタを使用して、関心のないイベントを除外します。

管理イベントを収集するイベントデータストアを作成する場合は、 AWS Key Management Service （ AWS KMS) または Amazon Relational Database Service (Amazon RDS) Data API イベントを除外できます。通常、`Encrypt`、、 などの AWS KMS アクションは`Decrypt`、イベントの 99% 以上`GenerateDataKey`を生成します。

データイベントを収集するイベントデータストアを作成する場合は、高度なイベントセレクタを使用して、`eventName`、`resources.type`、`resources.ARN`、`readOnly` の各フィールドで絞り込むことができます。例については、例: S3 データイベントのイベントデータストアを作成するを参照してください。

証跡イベントをコピーするときは、時間範囲を短くします。

証跡イベントを CloudTrail Lake にコピーするときは、取り込まれるデータの量を減らすために、開始イベント時間と終了イベント時間を短く指定します。

履歴分析のために証跡イベントを CloudTrail Lake にコピーしていて、今後のイベントを取り込まない場合は、イベントを取り込むオプションの選択を解除して、追加のイベントを取り込む際に料金が発生しないようにします。

`eventTime` の開始と終了を使用するようにクエリをフォーマットします。

Lake でクエリを実行すると、スキャンされたデータ量に基づいて料金が発生します。クエリの `eventTime` の開始と終了を指定することでコストを抑えることができます。

コスト管理に役立つツール

AWS の機能である Budgets では AWS Billing and Cost Management、コストまたは使用量が予算額を超えたとき (または超えると予測されるとき) に警告するカスタム予算を設定できます。

イベントデータストアを作成する際、 AWS Budgets CloudTrail を使用して の予算を作成することが推奨されるベストプラクティスであり、 CloudTrail 支出の追跡に役立ちます。コストベースの予算は、 CloudTrail 使用量の請求額についての認識を高めるのに役立ちます。 予算アラートは、請求額が定義したしきい値に達したときに通知します。予算アラートを受け取ったら、請求サイクルの終了前に変更を加えて、コストを管理できます。

予算を作成したら、 AWS Cost Explorer を使用して、 CloudTrail コストが AWS 請求全体にどのような影響を与えているかを確認できます。 AWS Cost Explorer では、 CloudTrail をサービスフィルターに追加した後、リージョンとアカウントの両方で、過去の CloudTrail支出と現在の month-to-date (MTD) 支出を比較できます。この機能は、月 CloudTrail額支出の予期しないコストをモニタリングおよび検出するのに役立ちます。Cost Explorer の追加機能を使用すると、特定のリソースレベルで CloudTrail 支出と月額支出を比較し、コストの増減を促進している要因に関する情報を提供できます。

AWS Budgets の使用を開始するには、 を開きAWS Billing and Cost Management、左側のナビゲーションバーで Budgets を選択します。 CloudTrail 支出を追跡する予算を作成する際には、予算アラートを設定することをお勧めします。 AWS Budgets の使用方法の詳細については、「 によるコストの管理 AWS Budgets」およびAWS 「 Budgets のベストプラクティス」を参照してください。

CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成

ユーザー定義のコスト配分タグを作成して、Lake イベントデータストアのクエリコストと取り込みコストを追跡できます CloudTrail。ユーザー定義のコスト配分タグは、イベントデータストアに関連付けられるキーと値のペアです。コスト配分タグを有効にすると、 AWS はタグを使用してコスト配分レポートでリソースコストを整理します。

- コンソールでタグを作成するには、「 CloudTrail 管理イベントまたはデータイベント用のイベントデータストアを作成するには」手順のステップ 9 を参照してください。
- API を使用してタグを作成するには、 CloudTrail 「 API リファレンスAddTags」のCreateEventDataStore「」および「」を参照してください。 AWS CloudTrail
- を使用してタグを作成するには AWS CLI、AWS CLI 「 コマンドリファレンス」のcreate-event-data-store「」および「タグの追加」を参照してください。 https://awscli.amazonaws.com/v2/documentation/api/latest/reference/cloudtrail/add-tags.html

タグの有効化に関する詳細については、「ユーザー定義のコスト配分タグのアクティブ化」を参照してください。

以下も参照してください。

- AWS CloudTrail の料金
- サポートされている CloudWatch メトリクス
- によるコストの管理 AWS Budgets
- Cost Explorer を開始する

CloudWatch サポート対象の指標

CloudTrail レイクは Amazon CloudWatch メトリクスをサポートしています。 CloudWatch AWS はリソースのモニタリングサービスです。を使用すると CloudWatch 、メトリクスの収集と追跡、アラームの設定、 AWS リソースの変化への自動対応を行うことができます。

AWS/CloudTrail名前空間には、Lake の以下のメトリクスが含まれます。 CloudTrail

メトリクス	説明	単位
HourlyDataIngested	過去 1 時間にイベントデータストアに取り込まれたデータ量。この指標は 1 時間ごとに更新されます。 このメトリクスは、すべてのイベントデータストアタイプで使用できます。	バイト
TotalDataRetained	保持期間全体にわたってイベントデータストアに保持されるデータの量。この指標は毎晩更新されます。 このメトリクスは、すべてのイベントデータストアタイプで使用できます。	バイト
TotalStorageBytes	当日現在のイベントデータストア内の圧縮バイト数の合計。 このメトリクスは、すべてのイベントデータストアタイプで使用できます。	バイト
TotalPaidStorageBytes	延長可能な 1 年間の保持料金オプションを使用するイベントデータストアの場合、これ	バイト

メトリクス	説明	単位
	はイベントデータストアに設定された最大保持期間に向けて 366 日経過した後の圧縮バイトの合計です。 延長可能な 1 年間の保持料金オプションを使用するイベントデータストアの場合、最初の 366 日間 (イベントデータストアのデフォルトの保持期間) のストレージは取り込み料金に追加コストなしで含まれています。366 日が経過すると、ストレージは有効になります。 pay-as-you-go料金については、「AWS CloudTrail 料金表」を参照してください。 このメトリクスは、延長可能な 1 年間の保持料金オプションを使用するイベントデータストアでのみ利用できます。	
`HourlyEventsAnalyzed`	CloudTrail Insights がイベントデータストアで分析したイベントの総数。この指標は 1 時間ごとに更新されます。 この指標は CloudTrail Insights CloudTrail を有効にするイベントデータストアを対象としています。	カウント

CloudWatch 指標について詳しくは、以下のトピックを参照してください。

- Amazon CloudWatch メトリクスの使用

- Amazon CloudWatch アラームを使用する

CloudTrail トレイルでの作業

AWS トレイルはアクティビティの記録をキャプチャし、これらのイベントを Amazon S3 バケットに配信して保存します。オプションで CloudWatch Logs と Amazon EventBridge への配信も可能です。

CloudTrail 証跡を作成することで、進行中の管理イベントのコピーを 1 つ無料でS3バケットに配信できますが、Amazon S3 ストレージには料金がかかります。 CloudTrail 料金の詳細については、「AWS CloudTrail 料金表」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

には、マルチリージョントレイルとシングルリージョントレイルの 2 種類のトレイルを作成できます AWS アカウント。

マルチリージョントレイル

マルチリージョントレイルを作成すると、 CloudTrail AWS リージョン AWS 作業中のパーティションのすべてのイベントが記録され、指定した S3 CloudTrail バケットにイベントログファイルが配信されます。マルチリージョントレイルを作成した後にを追加すると、その新しいリージョンが自動的に含まれ、そのリージョンのイベントが記録されます。 AWS リージョン マルチリージョンの証跡を作成すると、アカウント内のすべてのリージョンでのアクティビティを把握できるため、推奨されるベストプラクティスとなります。 CloudTrail コンソールを使用して作成したトレイルはすべてマルチリージョンです。単一リージョンのトレイルをマルチリージョンのトレイルに変換するには、を使用します。 AWS CLI詳細については、「コンソールで証跡を作成する」および「1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用」を参照してください。

単一リージョントレイル

単一リージョントレイルを作成すると、 CloudTrail そのリージョンのイベントのみを記録します。次に、指定した Amazon S3 CloudTrail バケットにイベントログファイルを配信します。AWS CLIを使用する際は、単一のリージョンの証跡のみを作成することができます。さらに 1 つの証跡を作成すると、それらの証跡から同じ S3 CloudTrail バケットまたは別のバケットにイベントログファイルを配信できます。 AWS CLI または API を使用して証跡を作成する場合、これがデフォルトのオプションです。 CloudTrail 詳細については、「を使用した証跡の作成、更新、管理 AWS CLI」を参照してください。

> **Note**
>
> どちらのタイプの証跡でも、任意のリージョンから Amazon S3 バケットを指定できます。

で組織を作成した場合は AWS Organizations、 AWS その組織内のすべてのアカウントのすべてのイベントを記録する組織証跡を作成できます。 AWS 組織証跡はすべての地域に適用することも、現在の地域に適用することもできます。組織の証跡は管理アカウントまたは委任された管理者アカウントで作成する必要があり、組織への適用として指定されている場合は、組織内のすべてのメンバーアカウントに自動的に適用されます。メンバーアカウントは組織記録を見ることができますが、変更や削除はできません。デフォルトでは、メンバーアカウントは Amazon S3 バケット内にある組織の証跡のログファイルにアクセスできません。詳細については、「組織の証跡の作成」を参照してください。

トピック

- あなたのためのトレイルの作成 AWS アカウント
- 組織の証跡の作成
- CloudTrail トレイルのインサイトイベントの表示
- トレイルイベントを CloudTrail Lake にコピーする
- CloudTrail ログファイルの取得と表示
- の Amazon SNS 通知の設定 CloudTrail
- 証跡を管理するためのヒント
- CloudTrail トレイルのユーザー権限の制御
- インターフェイス VPC AWS CloudTrail エンドポイントでの使用
- AWS アカウント クロージャーとトレイル

あなたのためのトレイルの作成 AWS アカウント

証跡を作成するときは、指定した Amazon S3 バケットへのログファイルとしてのイベントの継続的な配信を有効にします。証跡の作成には、次のような多くの利点があります。

- 90 日間を過ぎたイベントの記録。
- Amazon CloudWatch Logs にログイベントを送信することで、指定したイベントを自動的に監視してアラームを鳴らすオプション。

- Amazon Athena を使用してログをクエリし、 AWS サービスアクティビティを分析するオプション。

2019 年 4 月 12 日以降、 AWS トレイルはイベントを記録したリージョンでのみ表示できます。 AWS すべてのリージョンのイベントを記録するトレイルを作成すると、 AWS 作業中のパーティション内のすべてのリージョンのコンソールに表示されます。単一の リージョン内のイベントのみを口グ記録する証跡を作成した場合は、その リージョン内でのみ、それを表示および管理できます。 AWS CloudTrail コンソールを使用して証跡を作成する場合、マルチリージョントレールの作成はデフォルトのオプションであり、おすすめのベストプラクティスです。単一リージョンの証跡を作成するには、 AWS CLIを使用する必要があります。

を使用すると AWS Organizations、 AWS 組織内のすべてのアカウントのイベントを記録する証跡を作成できます。同じ名前の証跡が各メンバーアカウントに作成され、各証跡からのイベントは指定した Amazon S3 バケットに配信されます。

> **Note**
>
> 組織の管理アカウントまたは委任された管理者アカウントのみが、組織の証跡を作成できます。組織の証跡を作成すると、 CloudTrail とOrganizations 間の統合が自動的に有効になります。詳細については、「組織の証跡の作成」を参照してください。

トピック

- コンソールで証跡を作成および更新する
- を使用した証跡の作成、更新、管理 AWS CLI

コンソールで証跡を作成および更新する

CloudTrail コンソールを使用してトレイルを作成、更新、削除できます。コンソールを使用して作成した証跡はマルチリージョンです。1 つのイベントのみを記録する証跡を作成するには AWS リージョン、を使用します。 AWS CLI

リージョンごとに最大 5 つの証跡を作成できます。証跡を作成すると、アカウント内の API 呼び出しと関連イベントを、指定した Amazon S3 CloudTrail バケットに自動的に記録し始めます。口グ記録を停止するには、証跡の口グ記録を無効にするか、または削除します。

CloudTrail コンソールを使用して証跡を作成または更新することには、以下の利点があります。

- 証跡を初めて作成する場合は、 CloudTrail コンソールを使用して利用できる機能やオプションを確認できます。
- データイベントをログに記録するように証跡を設定する場合、 CloudTrail コンソールを使用して利用可能なデータタイプを表示できます。データイベントのログ記録の詳細については、「データイベントをログ記録する」を参照してください。

内の組織用の証跡の作成に関する具体的な情報については AWS Organizations、を参照してください組織の証跡の作成。

トピック

- 証跡の作成
- 証跡の更新
- 証跡の削除
- 証跡のログ記録をオフにする

証跡の作成

ベストプラクティスとして、すべての AWS リージョンに適用される証跡を作成します。これは、コンソールで証跡を作成するときの CloudTrailデフォルト設定です。証跡がすべてのリージョンに適用されると、 は、指定した S3 バケットに作業しているAWS パーティション内のすべてのリージョンからログファイルを CloudTrail 配信します。証跡を作成すると、 は指定したイベントのログ AWS CloudTrail 記録を自動的に開始します。

> **Note**
>
> 証跡を作成したら、 CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づいて処理 AWS のサービス するように他の を設定できます。詳細については、「AWS CloudTrail ログと サービスの統合」を参照してください。

トピック

- コンソールで証跡を作成する
- 次のステップ

コンソールで証跡を作成する

次の手順を使用して、作業している AWS パーティション AWS リージョン のすべての でイベントをログに記録する証跡を作成します。これは推奨されるベストプラクティスです。単一リージョンでイベントのログ記録を行うには (非推奨)、AWS CLIを使用します。

を使用して CloudTrail 証跡を作成するには AWS Management Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. CloudTrail サービスのホームページ、証跡ページ、またはダッシュボードページの証跡セクションで、証跡の作成 を選択します。
3. [Create Trail] (証跡の作成) ページの [Trail name] (証跡名) に証跡の名前を入力します。詳細については、「命名の要件」を参照してください。
4. これが AWS Organizations 組織の証跡である場合は、組織内のすべてのアカウントの証跡を有効にできます。このオプションを表示するには、管理アカウントまたは委任された管理者アカウントのユーザーまたはロールでコンソールにサインインする必要があります。組織の証跡を正しく作成するには、ユーザーまたはロールに十分なアクセス許可があることを確認してください。詳細については、「組織の証跡の作成 」を参照してください。
5. [ストレージの場所] で、[新しい S3 バケットを作成する] を選択すると、新しいバケットが作成されます。バケットを作成すると、 CloudTrail は必要なバケットポリシーを作成して適用します。新しい S3 バケットを作成する場合は、デフォルトでバケットのサーバー側の暗号化が有効になっているため、IAM ポリシーに `s3:PutEncryptionConfiguration`アクションのアクセス許可を含める必要があります。

> **Note**
>
> [既存の S3 バケットを使用する] を選択した場合、[証跡ログバケット名] のバケットを指定するか、[参照] を選択してお使いのアカウントのバケットを選択します。別のアカウントのバケットを使用する場合は、バケット名を指定する必要があります。バケットポリシーは、バケットポリシーに書き込むアクセス CloudTrail 許可を付与する必要があります。バケットポリシーを手動で編集する方法については、の Amazon S3 バケットポリシー CloudTrail を参照してください。

ログを見つけやすくするには、既存のバケットに新しいフォルダ (プレフィックス とも呼ばれます) を作成して CloudTrail ログを保存します。プレフィックスを [プレフィックス] に入力します。

6. [Log file SSE-KMS encryption] (ログファイルの SSE-KMS 暗号化) で、SSE-S3 暗号化を使用する代わりに SSE-KMS 暗号化を使用してログファイルを暗号化する場合は、[Enabled] (有効) を選択します。デフォルトは [Enabled] です。SSE-KMS 暗号化を有効にしない場合、ログは SSE-S3 暗号化を使用して暗号化されます。SSE-KMS 暗号化の詳細については、AWS Key Management Service 「 (SSE-KMS) によるサーバー側の暗号化の使用」を参照してください。SSE-S3 暗号化の詳細については、「Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3) の使用」を参照してください。

   SSE-KMS 暗号化を有効にする場合は、新規または既存の AWS KMS keyを選択します。AWS KMS エイリアス で、 形式でエイリアスを指定しますalias/*MyAliasName*。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。 CloudTrail は AWS KMS 、マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

   > **Note**
   >
   > 別のアカウントのキーの ARN を入力することもできます。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。キーポリシーでは、CloudTrail が キーを使用してログファイルを暗号化し、指定したユーザーが暗号化されていない形式でログファイルを読み取れるようにする必要があります。キーポリシーを手動で編集する方法については、AWS KMS の主要ポリシーの設定 CloudTrail を参照してください。

7. [Additional settings] で、次の操作を行います。

   a. [ログファイル検証を有効にする] で [Enabled] を選択して、S3 バケットにログダイジェストが配信されるようにします。ダイジェストファイルを使用して、 CloudTrail 配信後にログファイルが変更されていないことを確認できます。詳細については、「 CloudTrail ログファイルの整合性の検証」を参照してください。

   b. SNS 通知配信 では、ログがバケットに配信されるたびに通知されるように有効化 を選択します。 は複数のイベントをログファイルに CloudTrail 保存します。SNS 通知は、ログファ

イルごとに送信されます (イベントごとではありません)。詳細については、「の Amazon SNS 通知の設定 CloudTrail」を参照してください。

SNS 通知を有効にすると、[Create a new SNS topic] で、[New] を選択してトピックを作成するか、[Existing] を選択して既存のトピックを使用します。すべてのリージョンに適用される証跡を作成した場合、すべてのリージョンからのログファイル配信を知らせる SNS 通知は、ユーザーが作成した単一の SNS トピックに送信されます。

新しい を選択した場合、 は新しいトピックの名前 CloudTrail を指定するか、名前を入力できます。[Existing] を選択した場合、ドロップダウンリストから SNS トピックを選択します。別のリージョンにあるトピックの ARN を入力したり、適切なアクセス許可を持ったアカウントにあるトピックの ARN を入力することもできます。詳細については、「の Amazon SNS トピックポリシー CloudTrail」を参照してください。

トピックを作成する場合は、ログファイル配信の通知を受けるトピックを受信登録する必要があります。受信登録は Amazon SNS コンソールから行うことができます。通知頻度の都合上、受信登録については、Amazon SQS キューを使用して通知をプログラムで処理するように設定することをお勧めします。詳細については、[Amazon Simple 通知サービスデベロッパーガイド] の [Amazon SNS の使用開始] を参照してください。

8. オプションで、 CloudWatch ログ で有効 を選択してログファイルをCloudWatch ログに送信する CloudTrail ように を設定します。詳細については、「 CloudWatch ログへのイベントの送信」を参照してください。

   a. CloudWatch ログとの統合を有効にする場合は、新規 を選択して新しいロググループを作成するか、既存 を選択して既存のロググループを使用します。新しい を選択した場合、 は新しいロググループの名前 CloudTrail を指定するか、名前を入力できます。

   b. [Existing] を選択した場合、ドロップダウンリストからロググループを選択します。

   c. 新規 を選択して、ログを ログに送信するアクセス許可用の新しい IAM CloudWatch ロールを作成します。[Existing] を選択して、ドロップダウンリストから既存の IAM ロールを選択します。新しいロールまたは既存のロールのポリシーステートメントは、[ポリシードキュメント] を展開すると表示されます。このロールの詳細については、「 CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント」を参照してください。

> **Note**
>
> - 証跡を設定する際には、別のアカウントに属している S3 バケットや SNS トピックを選択することもできます。ただし、イベント CloudTrail を Logs CloudWatch ロググループに配信する場合は、現在のアカウントに存在するロググループを選択する必要があります。
> - 管理アカウントのみが、 コンソールを使用して組織の証跡の CloudWatch ロググループを設定できます。委任管理者は、 AWS CLI または CloudTrail `CreateTrail` `UpdateTrail` API オペレーションを使用して Logs CloudWatch ロググループを設定できます。

9. [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) を証跡に追加します。タグは、証 CloudTrail 跡と CloudTrail ログファイルを含む Amazon S3 バケットの両方を識別するのに役立ちます。その後、リソースに CloudTrail リソースグループを使用できます。詳細については、「AWS Resource Groups」および「タグ」を参照してください。
10. [Choose log events] ページで、ログに記録するイベントタイプを選択します。[管理イベント] で、次の操作を行います。

    a. [API activity] で、証跡で記録する対象を [読み取り] イベント、[書き込み] イベント、またはその両方を選択します。詳細については、「管理イベント」を参照してください。

    b. AWS KMS イベントを除外を選択して、証跡から AWS Key Management Service （ AWS KMS) イベントをフィルタリングします。デフォルト設定では、すべての AWS KMS イベントが含まれます。

    AWS KMS イベントをログまたは除外するオプションは、証跡に管理イベントをログに記録する場合にのみ使用できます。管理イベントを記録しないことを選択した場合、 AWS KMS イベントは記録されず、 AWS KMS イベントログ設定を変更することはできません。

    AWS KMS `Encrypt`、、 などの アクションは`Decrypt`、`GenerateDataKey`通常、大量のイベント (99% 以上) を生成します。これらのアクションは、[読み取り] イベントとしてログに記録されるようになりました。、、 `Delete` `ScheduleKey` (通常は AWS KMS イベントボリュームの 0.5% 未満を占める) `Disable`などの少量の関連 AWS KMS アクションは、書き込みイベントとして記録されます。

Encrypt、、 などの大量のイベントを除外してもGenerateDataKey、、Decrypt、 などの関連イベントをログに記録するにはDisableDeleteScheduleKey、書き込み管理イベントをログに記録し、イベントを除外 AWS KMS のチェックボックスをオフにします。

c. [Exclude Amazon RDS Data API events] を選択して、証跡から Amazon Relational Database Service データ API イベントを除外できます。デフォルト設定では、すべての Amazon RDS Data API イベントが含まれています。Amazon RDS Data API イベントの詳細については、Aurora の　Amazon RDS Amazon RDS ユーザーガイドの「AWS CloudTrailによる Data API コールのログ記録」を参照してください。

11. データイベントをログに記録するには、[データイベント] を選択します。データイベントのログ記録には追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

12.

> **Important**
>
> ステップ 12 ~ 16 は、デフォルトである高度なイベントセレクターを使用してデータイベントを設定するためのものです。高度なイベントセレクターでは、より多くのデータイベントタイプを設定し、証跡でキャプチャするデータイベントをきめ細かく制御できます。基本的なイベントセレクターを使用する場合は、基本的なイベントセレクターを使用してデータイベント設定を構成する のステップを完了してから、この手順のステップ 17 に戻ってください。

[データイベントタイプ] で、データイベントをログ記録するリソースのタイプを選択します。使用可能なデータイベントタイプの詳細については、「データイベント」を参照してください。

> **Note**
>
> Lake Formation によって作成された AWS Glue テーブルのデータイベントをログに記録するには、Lake Formation を選択します。

13. ログセレクタテンプレートを選択します。 には、リソースタイプのすべてのデータイベントをログに記録する事前定義されたテンプレート CloudTrail が含まれています。カスタムログセレクタテンプレートを構築するには、[Custom] を選択します。

> **Note**
>
> S3 バケットの事前定義されたテンプレートを選択すると、 AWS 現在アカウントにあるすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、アカウント内の任意の IAM ID によって実行されたデータイベントアクティビティのログ記録も有効にします AWS 。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。
> 証跡が 1 つのリージョンのみに適用される場合、すべての S3 バケットを口グ記録する事前定義済みテンプレートを選択すると、同じリージョン内のすべてのバケット、およびそのリージョンで後に作成するバケットに対して、データイベントの口グ記録が可能になります。 AWS アカウントの他のリージョンの Amazon S3 バケットのデータイベントは口グに記録されません。
> すべてのリージョンの証跡を作成する場合、Lambda 関数の事前定義されたテンプレートを選択すると、 AWS アカウントで現在使用しているすべての関数と、証跡の作成後に任意のリージョンで作成できる Lambda 関数のデータイベント口グ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して実行 AWS CLI) 、この選択により AWS 、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベント口グ記録が有効になります。他のリージョンで作成された Lambda 関数のデータイベントの口グ記録は有効になりません。
> すべての関数のデータイベントを口グに記録すると、 AWS アカウント内の任意の IAM アイデンティティによって実行されたデータイベントアクティビティの口グ記録も可能になります。これは、そのアクティビティが別の AWS アカウントに属する関数で実行された場合でも同様です。

14. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。
15. [Advanced event selectors] で、データイベントを口グに記録する特定のリソースの式を作成します。事前定義済みの口グテンプレートを使用している場合は、このステップをスキップできます。

    a. 次のフィールドから選択します。

- **readOnly** - readOnly は、 または の値と等しくなるように設定できますfalse。true読み取り専用データイベントは、Get* または Describe* イベントなどのリソースの状態を変更しないイベントです。書き込みイベントは、Put*、Delete*、または Write* イベントなどのリソース、属性、またはアーティファクトを追加、変更、または削除します。read および write イベントの両方を記録するには、readOnly セレクタを追加しないでください。
- **eventName** - eventName は任意の演算子を使用できます。これを使用して、、、 などCloudTrail、 に口グ記録されたデータイベントを含めたり除外PutBucketPutItemしたりできますGetSnapshotBlock。
- **resources.ARN** - 任意の演算子を で使用できますがresources.ARN、等号または不等号を使用する場合、値はテンプレートで の値として指定したタイプの有効なリソースの ARN と完全に一致する必要がありますresources.type。

  以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

  > **Note**
  >
  > resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方が口グ記録されます。ストリームイベント を除外するには、 eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントを口グ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

データイベントリソースの ARN 形式の詳細については、AWS Identity and Access Management ユーザーガイドの「アクション、リソース、条件キー」を参照してください。

b. 各フィールドについて、[条件の追加] を選択して、必要な条件をすべて追加します。すべての条件に対して最大 500 個の指定値を設定できます。例えば、証跡に記録されたデータイベントから 2 つの S3 バケットのデータイベントを除外するには、 フィールドを resources.ARN に設定し、 の演算子を で始まらないように設定してから、S3 バケット ARN に貼り付けるか、イベントをログに記録したくない S3 バケットを参照します。

2 番目の S3 バケットを追加するには、[条件の追加] を選択した後に上記の手順を繰り返し、ARN に貼り付けるか、別のバケットをブラウズします。

> **Note**
>
> 証跡上のすべてのセレクタに対して、最大 500 の値を設定できます。これには、`eventName` などのセレクタの複数の値の配列が含まれます。すべてのセレクタに単一の値がある場合、セレクタに最大 500 個の条件を追加できます。アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時に CloudTrail コンソールですべての関数を表示または選択することはできません。表示されていない場合でも、事前定義済みのセレクタテンプレートを使用してすべての関数をログ記録できます。特定の関数のデータイベントをログ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡の作成を終了し、 AWS CLI および put-event-selectors コマンドを使用して、特定の Lambda 関数のデータイベントログ記録を設定することもできます。詳細については、「を使用した証跡の管理 AWS CLI」を参照してください。

c. [+ Field] を選択し、必要に応じてフィールドを追加します。エラーを回避するには、フィールドに競合する値や重複する値を設定しないでください。例えば、あるセレクタで ARN を値と等しく指定せず、次に、別のセレクタで同じ値に等しくない ARN を指定します。

16. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。ステップ 12 からこのステップを繰り返し、データイベントタイプのアドバンストイベントセレクタを設定します。

17. 証跡で Insights イベントをログ CloudTrailに記録する場合は、Insights イベントを選択します。

    [Event type] で、[Insights events] を選択します。[API コール率] の Insights イベントをログに記録するには、[Write] 管理イベントをログ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、[Read] または [Write] 管理イベントをログ記録している必要があります。

CloudTrail Insights は、異常なアクティビティの管理イベントを分析し、異常が検出されたときにイベントを記録します。デフォルトでは、証跡は Insights イベントを記録しません。Insights イベントの詳細については、「Insights イベントのログ記録」を参照してください。Insights イベントの記録には追加料金が適用されます。 CloudTrail 料金については、「 AWS CloudTrail の料金」を参照してください。

Insights イベントは、証跡の詳細ページのストレージロケーションエリアで指定されているのと同じ S3 バケット/`CloudTrail-Insight`の という名前の別のフォルダに配信されます。CloudTrail は新しいプレフィックスを作成します。たとえば、現在の送信先 S3 バケットの名前が `S3bucketName/AWSLogs/CloudTrail/` の場合、新しいプレフィックスが付いた S3 バケットの名前は `S3bucketName/AWSLogs/CloudTrail-Insight/` になります。

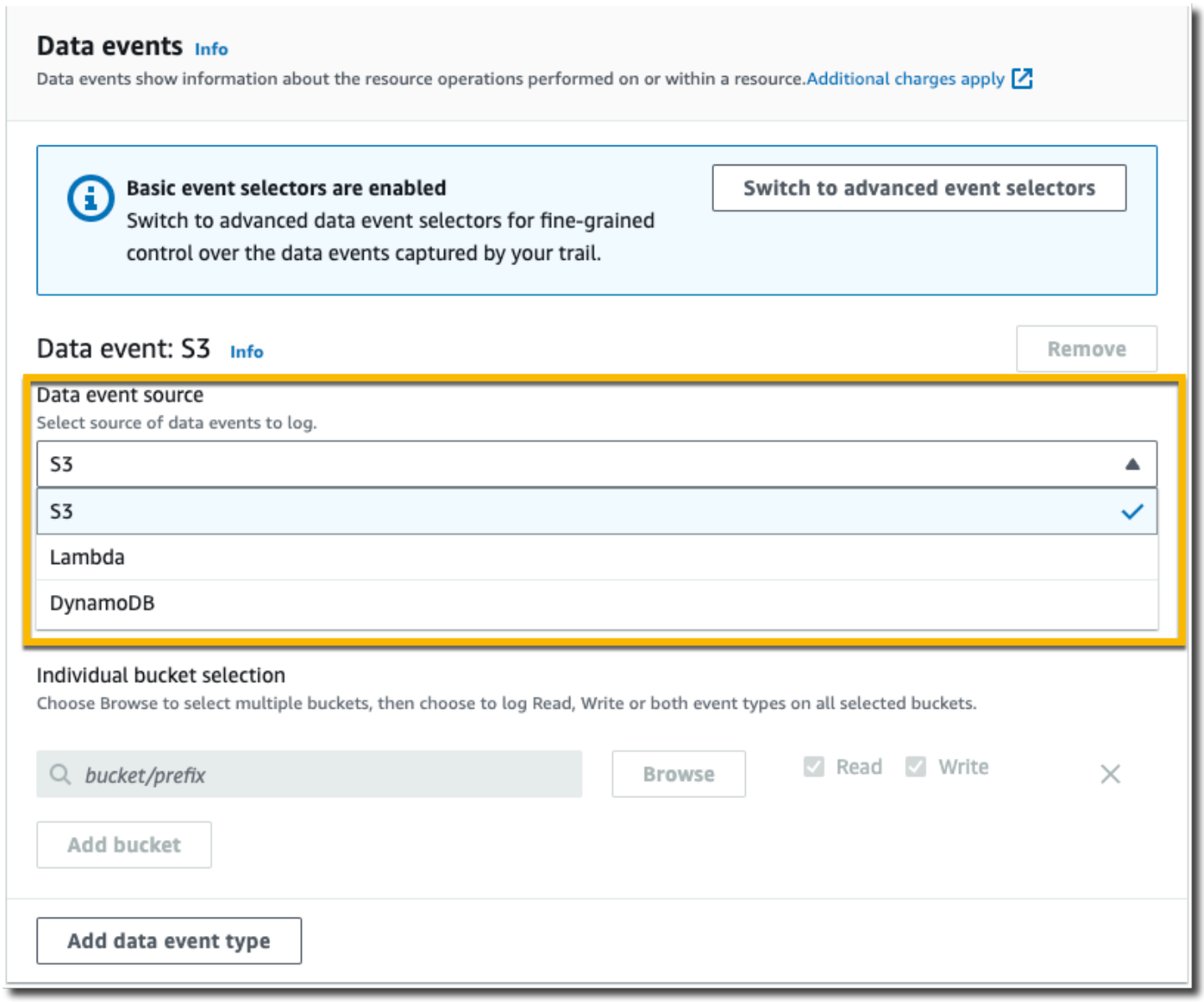
18. ログに記録するイベントタイプの選択が終了したら、[Next] を選択します。
19. [Review and create] ページで選択内容を確認します。[Edit] を選択して、そのセクションに表示される証跡設定を変更します。証跡を作成する準備ができたら、[Create trail] を選択します。
20. 新しい証跡が [Trails] (証跡) ページに表示されます。約 5 分で、 CloudTrail はアカウントで行われた AWS API コールを示すログファイルを発行します。ユーザーは、指定した S3 バケット内のログファイルを確認することができます。Insights イベントログを有効にしていて、異常なアクティビティが検出された場合、 が最初の Insights イベントを配信 CloudTrail するまでに最大 36 時間かかることがあります。

> **Note**
>
> CloudTrail は通常、API コールから平均約 5 分以内にログを配信します。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。
> 証跡を誤って設定した場合 (S3 バケットに到達できないなど) 、 はログファイルを S3 バケットに 30 日間再配信 CloudTrail しようとします。これらの attempted-to-deliver イベントには標準 CloudTrail 料金が適用されます。証跡の不適切な設定による課金を避けるには、その証跡を削除する必要があります。

基本的なイベントセレクターを使用してデータイベント設定を構成する

アドバンストイベントセレクタを使用して、すべてのデータイベントタイプを設定できます。高度なイベントセレクタを使用すると、対象のイベントのみをログに記録する詳細なセレクタを作成できます。

基本的なイベントセレクタを使用してデータイベントをログに記録する場合、Amazon S3 バケット、 AWS Lambda 関数、および Amazon DynamoDB テーブルのデータイベントのログ記録に制限されます。基本的なイベントセレクタを使用して`eventName`フィールドをフィルタリングすることはできません。



以下の手順で、基本的なイベントセレクターを使用して、データイベント設定を構成します。

基本的なイベントセレクターを使用してデータイベント設定を構成するには

1. データイベントをログ記録するには、[イベント] で [データイベント] を選択します。データイベントのログ記録には追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

2. Amazon S3 バケットの場合

   a. [Data source] で、[S3] を選択します。

   b. すべての現在および将来の S3 バケットを記録することを選択するか、バケットまたは関数を個々に指定することができます。デフォルトでは、現在および将来のすべての S3 バケットのデータイベントが記録されます。

   > **Note**
   >
   > デフォルトの「現在および将来のすべての S3 バケット」オプションを保持すると、 AWS 現在アカウントにあるすべてのバケットと、証跡の作成後に作成するすべてのバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意の IAM ID によって実行されたデータイベントアクティビティのログ記録も有効にします。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。
   > 1 つのリージョンの証跡を作成する場合 (を使用して作成 AWS CLI)、現在および将来の S3 バケットをすべて選択すると、証跡と同じリージョン内のすべてのバケットと、そのリージョンで後で作成するバケットのデータイベントログ記録が有効になります。 AWS アカウントの他のリージョンの Amazon S3 バケットのデータイベントはログに記録されません。

   c. デフォルトの [All current and future S3 buckets] で、[読み取り] イベント、[書き込み] イベント、またはその両方をログ記録することを選択します。

   d. 個々のバケットを選択するには、[All current and future S3 buckets] の [読み取り] および [書き込み] のチェックボックスをオフにします。[Individual bucket selection] で、データイベントをログ記録するバケットを参照します。目的のバケットのバケットプレフィックスを入力して、特定のバケットを検索します。このウィンドウで、複数のバケットを選択できます。[Add bucket] を選択してより多くのバケットのデータイベントをログ記録します。[読み取り] イベント (例: `GetObject`) か、[書き込み] イベント (例: `PutObject`)、または両方を選択します。

      この設定は、個別のバケットに設定した個々の設定よりも優先されます。たとえば、すべての S3 バケットにログ記録 [読み取り] イベントを指定し、データイベントログ記録に特定のバケットの追加を選択した場合、追加したバケットには既に [読み取り] が設定されています。選択を解除することはできません。[書き込み] のオプションしか設定することができません。

      ログ記録からバケットを削除するには、[X] を選択します。

3. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。
4. Lambda 関数の場合

   a. [Data source] で、[Lambda] を選択します。

   b. [Lambda 関数] で、[All regions] を選択してすべての Lambda 関数を口グ記録するか、[Input function as ARN] を使用して、特定の関数のデータイベントを口グ記録します。

      AWS アカウント内のすべての Lambda 関数のデータイベントをログに記録するには、現在および将来の関数をすべて口グに記録するを選択します。この設定は、関数に個々に設定した各設定よりも優先されます。すべての関数が表示されていなくても、関数はすべて口グ記録されます。

      > **Note**
      >
      > すべてのリージョンで証跡を作成している場合は、この選択によって、 AWS アカウントの現時点のすべての関数や、証跡作成後に任意のリージョンに作成する可能性のある Lambda 関数のデータイベントの口グ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して実行 AWS CLI) 、この選択により AWS 、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベント口グ記録が有効になります。他のリージョンで作成された Lambda 関数のデータイベントの口グ記録は有効になりません。
      > すべての関数のデータイベントを口グに記録すると、そのアクティビティが別のアカウントに属する関数で実行されている場合でも、アカウント AWS 内の任意の IAM ID によって実行されたデータイベントアクティビティの口グ記録も可能になります AWS 。

   c. [Input function as ARN] を選択した場合、Lambda 関数の ARN を入力します。

      > **Note**
      >
      > アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時に CloudTrail コンソールですべての関数を表示または選択することはできません。表示されていない場合でも、すべての関数を口グ記録するオプションを選択することができます。特定の関数のデータイベントを口グ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡の作成を終了し、 AWS CLI および put-event-selectors コマンドを使用して、特定の Lambda 関数のデータ

イベントログ記録を設定することもできます。詳細については、「を使用した証跡の管理 AWS CLI」を参照してください。

5. DynamoDB テーブルの場合

   a. [Data event source] で、[DynamoDB] を選択します。

   b. [DynamoDB table selection] で、[Browse] を選択してテーブルを選択するか、アクセス許可を持つ DynamoDB テーブルの ARN に貼り付けます。DynamoDB テーブルの ARN は次の形式です。

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   別のテーブルを追加するには、[Add row] を選択し、テーブルを参照するか、アクセス許可のあるテーブルの ARN に貼り付けます。

6. 証跡の Insights イベントとその他の設定を行うには、このトピックで前述した手順、??? に戻ります。

次のステップ

証跡を作成したら、証跡に戻って次の変更を加えることができます。

- ログファイルを Logs に送信する CloudTrail ように をまだ設定していない場合は、 CloudWatch を設定できます。詳細については、「 CloudWatch ログへのイベントの送信」を参照してください。
- テーブルを作成し、Amazon Athena でのクエリの実行に使用して、 AWS サービスアクティビティを分析します。詳細については、「Amazon Athena ユーザーガイド」の CloudTrail 「コンソールでの CloudTrail ログのテーブルの作成」を参照してください。 Amazon Athena
- 証跡にカスタムタグ (キーと値のペア) を追加する。
- 別の証跡を作成するには、[証跡] ページを開き、[証跡の作成] を選択します。

証跡の更新

このセクションでは、証跡の設定を変更する方法について説明します。

単一リージョンの証跡を更新して、作業しているAWS パーティションのすべての AWS リージョンでイベントを口グに記録するか、マルチリージョンの証跡を更新して 1 つのリージョンのみでイベ

ントを口グに記録するには、 を使用する必要があります AWS CLI。単一リージョンの証跡を更新してすべてのリージョンのイベントを口グ記録する方法の詳細については、「1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用」を参照してください。マルチリージョンの証跡を更新して単一のリージョンのイベントを口グ記録する方法の詳細については、「マルチリージョンの証跡から単一リージョンの証跡への変換」を参照してください。

Amazon Security Lake で CloudTrail 管理イベントを有効にしている場合は、マルチリージョンで との両方readwriteの管理イベントを記録する組織証跡を少なくとも 1 つ維持する必要があります。資格を満たしている証跡を、Security Lake の要件に従わない方法で更新することはできません。例えば、証跡を単一リージョンに変更したり、read または write 管理イベントの口グ記録をオフにしたりするなどです。

> **Note**
>
> CloudTrail は、リソースの検証が失敗した場合でも、メンバーアカウントの組織の証跡を更新します。検証の失敗の例は次のとおりです。
>
> - Amazon S3 バケットポリシーが正しくない
> - Amazon SNS トピックポリシーが正しくない
> - Logs CloudWatch ロググループに配信できない
> - KMS キーを使用して暗号化するアクセス許可が不十分
>
> アクセス CloudTrail 許可を持つメンバーアカウントは、 CloudTrail コンソールで証跡の詳細ページを表示するか、 コマンドを実行して AWS CLI get-trail-status、組織の証跡の検証に失敗したことを確認できます。

を使用して証跡を更新するには AWS Management Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションメニューで、 [証跡] を選択し、証跡を選択します。
3. [General details] で、[Edit] を選択して次の設定を変更します。証跡の名前は変更できません。
   - 組織に証跡を適用する - この証跡が AWS Organizations 組織の証跡であるかどうかを変更します。

> **Note**
>
> 組織の証跡を非組織の証跡に変換したり、非組織の証跡を組織の証跡に変換したりできるのは、組織の管理アカウントだけです。

- [Trail log location] - この証跡のログを保存する S3 バケットまたはプレフィックスの名前を変更します。
- [Log file SSE-KMS encryption] で、SSE-S3 を使用する代わりに SSE-KMS を使用してログファイルを暗号化の有効または無効を選択します。
- [Log file validation] - ログファイルの整合性の検証の有効または無効を選択します。
- [SNS notification delivery] - 証跡に指定されているバケットにログファイルが配信された Amazon Simple Notification Service (Amazon SNS) 通知の有効または無効を選択します。

a. 証跡を AWS Organizations 組織の証跡に変更するには、組織内のすべてのアカウントの証跡を有効にすることを選択できます。詳細については、「組織の証跡の作成」を参照してください。

b. 指定したバケットを [ストレージの場所] で、[新しい S3 バケットの作成] を選択してバケットを作成します。バケットを作成すると、 は必要なバケットポリシー CloudTrail を作成して適用します。新しい S3 バケットを作成する場合は、デフォルトでバケットのサーバー側の暗号化が有効になっているため、IAM ポリシーに `s3:PutEncryptionConfiguration`アクションのアクセス許可を含める必要があります。

> **Note**
>
> [Use existing S3 bucket] を選択した場合、[Trail log bucket name] のバケットを指定するか、[Browse] を選択してバケットを選択します。バケットポリシーは、バケットポリシーに書き込むアクセス CloudTrail 許可を付与する必要があります。バケットポリシーを手動で編集する方法については、の Amazon S3 バケットポリシー CloudTrail を参照してください。

ログを見つけやすくするには、既存のバケットに新しいフォルダ (プレフィックス とも呼ばれます) を作成して CloudTrail ログを保存します。プレフィックスを [プレフィックス] に入力します。

c. [Log file SSE-KMS encryption] (ログファイルの SSE-KMS 暗号化) で、SSE-S3 暗号化を使用する代わりに SSE-KMS 暗号化を使用してログファイルを暗号化する場合は、[Enabled] (有効) を選択します。デフォルトは [Enabled] です。SSE-KMS 暗号化を有効にしない場合、ログは SSE-S3 暗号化を使用して暗号化されます。SSE-KMS 暗号化の詳細については、AWS Key Management Service 「 (SSE-KMS) によるサーバー側の暗号化の使用」を参照してください。SSE-S3 暗号化の詳細については、「Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3) の使用」を参照してください。

SSE-KMS 暗号化を有効にする場合は、新規または既存の AWS KMS keyを選択します。AWS KMS エイリアス で、 形式でエイリアスを指定しますalias/*MyAliasName*。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。CloudTrail は AWS KMS 、マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

> **Note**
>
> 別のアカウントのキーの ARN を入力することもできます。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。キーポリシーでは、 CloudTrail が キーを使用してログファイルを暗号化し、指定したユーザーが暗号化されていない形式でログファイルを読み取れるようにする必要があります。キーポリシーを手動で編集する方法については、AWS KMS の主要ポリシーの設定 CloudTrail を参照してください。

d. [ログファイル検証を有効にする] で [Enabled] を選択して、S3 バケットにログダイジェストが配信されるようにします。ダイジェストファイルを使用して、 CloudTrail 配信後にログファイルが変更されていないことを確認できます。詳細については、「 CloudTrail ログファイルの整合性の検証」を参照してください。

e. SNS 通知配信 では、ログがバケットに配信されるたびに通知されるように有効化 を選択します。 は複数のイベントをログファイルに CloudTrail 保存します。SNS 通知は、ログファイルごとに送信されます (イベントごとではありません)。詳細については、「の Amazon SNS 通知の設定 CloudTrail」を参照してください。

SNS 通知を有効にすると、[Create a new SNS topic] で、[New] を選択してトピックを作成するか、[Existing] を選択して既存のトピックを使用します。すべてのリージョンに適用される証跡を作成した場合、すべてのリージョンからのログファイル配信を知らせる SNS 通知は、ユーザーが作成した単一の SNS トピックに送信されます。

新しい を選択した場合、 は新しいトピックの名前 CloudTrail を指定するか、名前を入力できます。[Existing] を選択した場合、ドロップダウンリストから SNS トピックを選択します。別のリージョンにあるトピックの ARN を入力したり、適切なアクセス許可を持ったアカウントにあるトピックの ARN を入力することもできます。詳細については、「の Amazon SNS トピックポリシー CloudTrail」を参照してください。

トピックを作成する場合は、ログファイル配信の通知を受けるトピックを受信登録する必要があります。受信登録は Amazon SNS コンソールから行うことができます。通知頻度の都合上、受信登録については、Amazon SQS キューを使用して通知をプログラムで処理するように設定することをお勧めします。詳細については、[Amazon Simple 通知サービスデベロッパーガイド] の [Amazon SNS の使用開始] を参照してください。

4. CloudWatch ログ で、編集 を選択して CloudTrail ログファイルを CloudWatch ログに送信するための設定を変更します。ログファイルの送信を有効にするにはCloudWatch 、ログで有効を選択します。詳細については、「 CloudWatch ログへのイベントの送信」を参照してください。

   a. CloudWatch ログとの統合を有効にする場合は、新規 を選択して新しいロググループを作成するか、既存 を選択して既存のロググループを使用します。新しい を選択した場合、 は新しいロググループの名前 CloudTrail を指定するか、名前を入力できます。

   b. [Existing] を選択した場合、ドロップダウンリストからロググループを選択します。

   c. 新規 を選択して、ログを ログに送信するアクセス許可用の新しい IAM CloudWatch ロールを作成します。[Existing] を選択して、ドロップダウンリストから既存の IAM ロールを選択します。新しいロールまたは既存のロールのポリシーステートメントは、[ポリシードキュメント] を展開すると表示されます。このロールの詳細については、「 CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント」を参照してください。

   > **Note**
   >
   > - 証跡を設定する際には、別のアカウントに属している S3 バケットや SNS トピックを選択することもできます。ただし、イベント CloudTrail を Logs CloudWatch ロググループに配信する場合は、現在のアカウントに存在するロググループを選択する必要があります。
   > - 管理アカウントのみが、 コンソールを使用して組織の証跡の CloudWatch ロググループを設定できます。委任管理者は、 AWS CLI または CloudTrail

CreateTrail UpdateTrail API オペレーションを使用して CloudWatch Logs ロググループを設定できます。

5. [タグ] で、[編集] を選択して、証跡のタグを変更、追加、または削除します。1 つまたは複数のカスタムタグ (キーと値のペア) を証跡に追加します。タグは、証 CloudTrail 跡と CloudTrail ログファイルを含む Amazon S3 バケットの両方を識別するのに役立ちます。その後、リソースに CloudTrail リソースグループを使用できます。詳細については、「AWS Resource Groups」および「タグ」を参照してください。
6. [Management events] で、[編集] を選択して、管理イベントのログ設定を変更します。

   a. [API activity] で、証跡で記録する対象を [読み取り] イベント、[書き込み] イベント、またはその両方を選択します。詳細については、「管理イベント」を参照してください。

   b. AWS KMS イベントを除外を選択して、証跡から (AWS KMS) イベントをフィルタリング AWS Key Management Service します。デフォルト設定では、すべての AWS KMS イベントが含まれています。

      AWS KMS イベントをログまたは除外するオプションは、証跡に管理イベントをログに記録する場合にのみ使用できます。管理イベントをログに記録しないことを選択した場合、AWS KMS イベントはログに記録されず、 AWS KMS イベントログ設定を変更することはできません。

      AWS KMS Encrypt、、 などの アクションはDecrypt、GenerateDataKey通常、大量のイベント (99% 以上) を生成します。これらのアクションは、[読み取り] イベントとしてログに記録されるようになりました。、、 Delete ScheduleKey (通常は AWS KMS イベントボリュームの 0.5% 未満を占める) Disableなどの少量の関連 AWS KMS アクションは、書き込みイベントとして記録されます。

      Encrypt、Decrypt、GenerateDataKey のようなボリュームの大きなイベントを除外し、Disable、Delete、ScheduleKey などの関連イベントを記録する場合は、[書き込み] 管理イベントを記録することを選択し、[Exclude AWS KMS events] チェックボックスをオフにします。

   c. [Exclude Amazon RDS Data API events] を選択して、証跡から Amazon Relational Database Service データ API イベントを除外できます。デフォルト設定では、すべての Amazon RDS Data API イベントが含まれています。Amazon RDS Data API イベントの詳細については、「Aurora の　Amazon RDS Amazon RDS ユーザーガイド」の「AWS CloudTrailによる Data API コールのログ記録」を参照してください。

7.

> **Important**
>
> ステップ 7 ~ 11 は、高度なイベントセレクターを使用してデータイベントを設定するためのものです。高度なイベントセレクターでは、より多くのデータイベントタイプを設定し、証跡でキャプチャするデータイベントをきめ細かく制御できます。基本的なイベントセレクターを使用している場合は、「基本的なイベントセレクターを使用したデータイベント設定の更新」を参照してから、この手順のステップ 12 に戻ってください。

[Data events] で、[編集] を選択して、データイベントのログ設定を変更します。デフォルトでは、証跡はデータイベントを記録しません。データイベントのログ記録には追加料金が適用されます。 CloudTrail の料金については、「AWS CloudTrail 料金表」を参照してください。

[データイベントタイプ] で、データイベントをログ記録するリソースのタイプを選択します。使用可能なデータイベントタイプの詳細については、「データイベント」を参照してください。

> **Note**
>
> Lake Formation によって作成された AWS Glue テーブルのデータイベントをログに記録するには、Lake Formation を選択します。

8. ログセレクタテンプレートを選択します。 には、リソースタイプのすべてのデータイベントをログに記録する事前定義されたテンプレート CloudTrail が含まれています。カスタムログセレクタテンプレートを構築するには、[Custom] を選択します。

> **Note**
>
> S3 バケットの事前定義されたテンプレートを選択すると、 AWS 現在アカウントにあるすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティのログ記録も有効にします。そのアクティビティが別の AWS アカウントに属するバケットで実行されている場合でも同様です。
> 証跡が 1 つのリージョンのみに適用される場合、すべての S3 バケットを口グ記録する事前定義済みテンプレートを選択すると、同じリージョン内のすべてのバケット、およびそのリージョンで後に作成するバケットに対して、データイベントのログ記録が可能になります。 AWS アカウント内の他のリージョンの Amazon S3 バケットのデータイベントは記録されません。

すべてのリージョンの証跡を作成する場合は、Lambda 関数の事前定義されたテンプレートを選択すると、 AWS アカウントで現在使用されているすべての関数と、証跡の作成後に任意のリージョンで作成できる Lambda 関数のデータイベントログ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して実行 AWS CLI)、この選択により、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベントログ記録が有効になります AWS 。他のリージョンで作成された Lambda 関数のデータイベントの記録は有効になりません。
すべての関数のデータイベントをログに記録すると、 AWS アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティの記録も可能になります。これは、そのアクティビティが別の AWS アカウントに属する関数で実行された場合でも同様です。

9. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。

10. [Advanced event selectors] で、データイベントを収集する特定のリソースの式を作成します。事前定義済みのログテンプレートを使用している場合は、このステップをスキップできます。

    a. 次のフィールドから選択します。

    - **readOnly** - readOnly は、 または の値と等しくなるように設定できますfalse。trueread および write イベントの両方を記録するには、readOnly セレクタを追加しないでください。
    - **eventName** - eventName は任意の演算子を使用できます。これを使用して、 や など CloudTrail、 に記録されたデータイベントを含めたり除外PutBucketしたりできますGetSnapshotBlock。
    - **resources.ARN** - 任意の演算子を で使用できますがresources.ARN、等しい または等しくない場合、値はテンプレートで の値として指定したタイプの有効なリソースの ARN と完全に一致する必要がありますresources.type。

      以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

> **Note**
>
> resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*

resources.type	resources.ARN
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*

resources.type	resources.ARN
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environment/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_ID* :table/*database_name* /*table_name*
AWS::GreengrassV2::ComponentVersion	arn:*partition* :greengrass: *region*:*account_ID* :components/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengrass: *region*:*account_ID* :deployments/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guardduty: *region*:*account_ID* :detector/ *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_ID* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*

resources.type	resources.ARN
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain :::networks/ *network_name*

resources.type	resources.ARN
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain : *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*

resources.type	resources.ARN
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*
AWS::SageMaker::ExperimentT rialComponent	arn:*partition* :sagemake r: *region*:*account_ID* :experiment- trial-component/ *experiment_trial_c omponent_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemake r: *region*:*account_ID* :feature- group/ *feature_group_name*

resources.type	resources.ARN
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*

resources.type	resources.ARN
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方が口グ記録されます。ストリームイベント を除外するには、 eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントを口グ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

データイベントリソースの ARN 形式の詳細については、AWS Identity and Access Management ユーザーガイドの「アクション、リソース、条件キー」を参照してください。

b. 各フィールドについて、[条件の追加] を選択して、必要な条件をすべて追加します。すべての条件に対して最大 500 個の指定値を設定できます。例えば、証跡に記録されたデータイベントから 2 つの S3 バケットのデータイベントを除外するには、 フィールドを resources.ARN に設定し、 の演算子を で始まらないように設定してから、S3 バケット ARN に貼り付けるか、イベントを口グに記録したくない S3 バケットを参照します。

2 番目の S3 バケットを追加するには、[条件の追加] を選択した後に上記の手順を繰り返し、ARN に貼り付けるか、別のバケットをブラウズします。

> **Note**
>
> 証跡上のすべてのセレクタに対して、最大 500 の値を設定できます。これには、eventName などのセレクタの複数の値の配列が含まれます。すべてのセレクタに単一の値がある場合、セレクタに最大 500 個の条件を追加できます。
> アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時に CloudTrail コンソールですべての関数を表示または選択することはできません。表示されていない場合でも、事前定義済みのセレクタテンプレートを使用してすべての関数を口グ記録できます。特定の関数のデータイベントを口グ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡の作成を終了し、 AWS CLI および put-event-selectors コマンドを使用して、特定の Lambda 関数のデータイベント口グ記録を設定することもできます。詳細については、「を使用した証跡の管理 AWS CLI」を参照してください。

c. [+ Field] を選択し、必要に応じてフィールドを追加します。エラーを回避するには、フィールドに競合する値や重複する値を設定しないでください。例えば、あるセレクタで ARN を値と等しく指定せず、次に、別のセレクタで同じ値に等しくない ARN を指定します。

11. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。ステップ 3 からこのステップを繰り返し、データイベントタイプのアドバンストイベントセレクタを設定します。

12. Insights Events で、証跡に CloudTrail Insights イベントを口グに記録する場合は、編集を選択します。

    [Event type] で、[Insights events] を選択します。

    Insights イベントで、API コールレート、API エラーレート、または両方を選択します。[API コール率] の Insights イベントをログに記録するには、[Write] 管理イベントを口グ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、[Read] または [Write] 管理イベントを口グ記録している必要があります。

    CloudTrail Insights は管理イベントを分析して異常なアクティビティがないか確認し、異常が検出されるとイベントを記録します。デフォルトでは、証跡は Insights イベントを記録しません。Insights トイベントの詳細については、「Insights イベントの口グ記録」を参照してください。Insights イベントの記録には追加料金が適用されます。 CloudTrail 料金については、「AWS CloudTrail の料金」を参照してください。

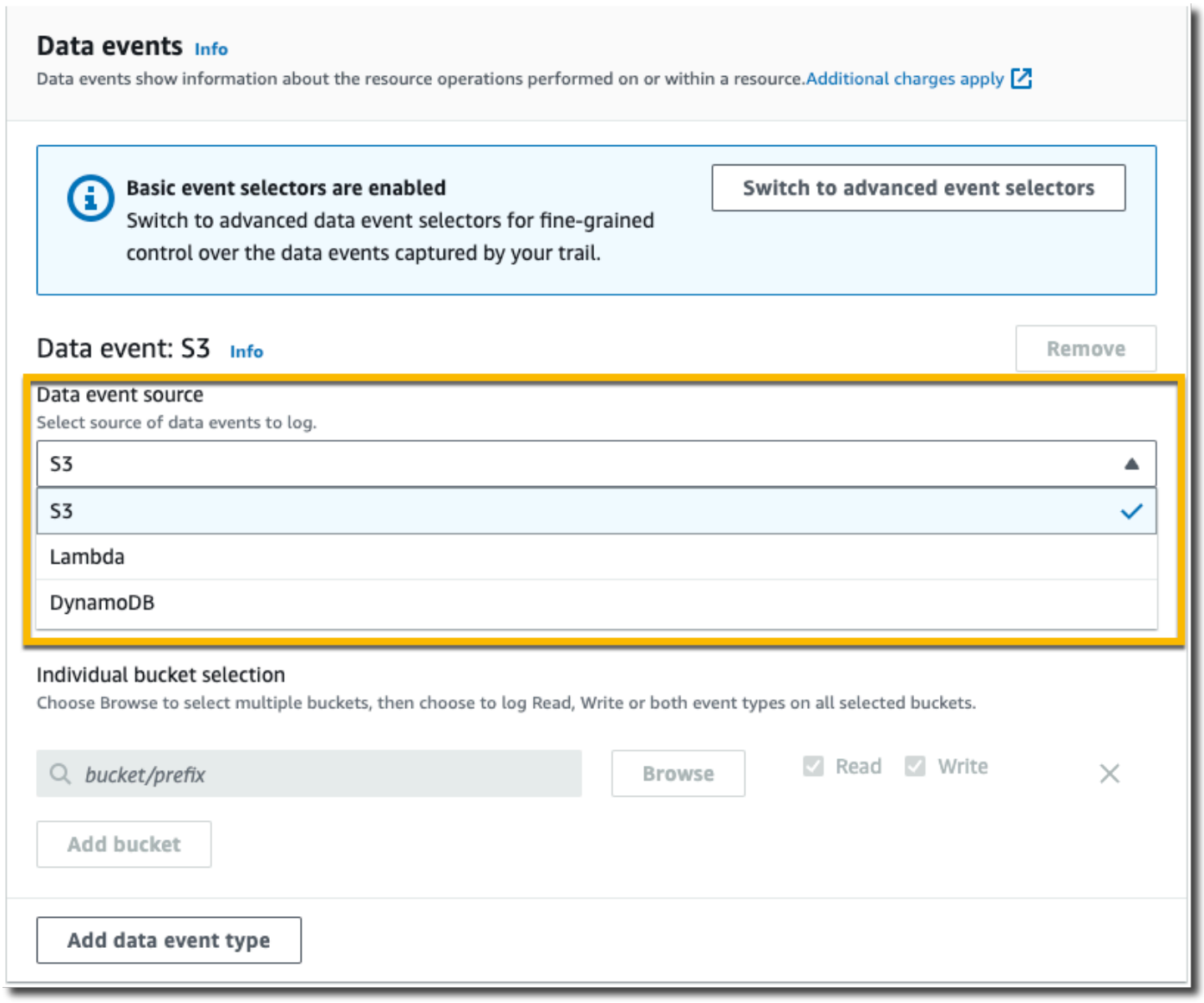
Insights イベントは、証跡の詳細ページのストレージロケーションエリアで指定されているのと同じ S3 バケット/CloudTrail-Insightの という名前の別のフォルダに配信されます。CloudTrail は新しいプレフィックスを作成します。たとえば、現在の送信先 S3 バケットの名前が S3bucketName/AWSLogs/CloudTrail/ の場合、新しいプレフィックスが付いた S3 バケットの名前は S3bucketName/AWSLogs/CloudTrail-Insight/ になります。

13. 証跡の設定を変更し終えたら、[Update trail] を選択します。

基本的なイベントセレクターを使用したデータイベント設定の更新

高度なイベントセレクタを使用して、すべてのデータイベントタイプを設定できます。高度なイベントセレクタを使用すると、対象のイベントのみをログに記録する詳細なセレクタを作成できます。

基本的なイベントセレクタを使用してデータイベントをログに記録する場合、Amazon S3 バケット、 AWS Lambda 関数、および Amazon DynamoDB テーブルのデータイベントのログ記録に制限されます。基本的なイベントセレクタを使用してeventNameフィールドをフィルタリングすることはできません。



以下の手順で、基本的なイベントセレクターを使用して、データイベント設定を構成します。

1. [Data events] で、[編集] を選択して、データイベントのログ設定を変更します。基本的なイベントセレクタを使用すると、Amazon S3 バケット、 AWS Lambda 関数、DynamoDBtables、またはそれらのリソースの組み合わせのログ記録データイベントを指定できます。追加のデータイベントタイプは、アドバンストイベントセレクタでサポートされています。デフォルトでは、証跡はデータイベントを記録しません。データイベントのログ記録には追加料金が適用されます。詳細については、「データイベント」を参照してください。 CloudTrail の料金については、「AWS CloudTrail 料金表」を参照してください。

   Amazon S3 バケットの場合

a. [Data source] で、[S3] を選択します。

b. すべての現在および将来の S3 バケットを記録することを選択するか、バケットまたは関数を個々に指定することができます。デフォルトでは、現在および将来のすべての S3 バケットのデータイベントが記録されます。

> **Note**
>
> デフォルトの「現在および将来のすべての S3 バケット」オプションを保持すると、 AWS 現在アカウント内のすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティのログ記録も有効にします。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。
> 証跡が 1 つのリージョンのみに適用される場合、すべての現在および将来の S3 バケットを選択すると、同じリージョン内のすべてのバケット、およびそのリージョンで後に作成するバケットに対して、データイベントのログ記録が可能になります。 AWS アカウント内の他のリージョンの Amazon S3 バケットのデータイベントはログに記録されません。

c. デフォルトの [All current and future S3 buckets] で、[読み取り] イベント、[書き込み] イベント、またはその両方をログ記録することを選択します。

d. 個々のバケットを選択するには、[All current and future S3 buckets] の [読み取り] および [書き込み] のチェックボックスをオフにします。[Individual bucket selection] で、データイベントをログ記録するバケットを参照します。特定のバケットを検索するには、目的のバケットのバケットプレフィックスを入力します。このウィンドウで、複数のバケットを選択できます。[Add bucket] を選択してより多くのバケットのデータイベントをログ記録します。[読み取り] イベント (例: `GetObject`) か、[書き込み] イベント (例: `PutObject`)、または両方を選択します。

この設定は、個別のバケットに設定した個々の設定よりも優先されます。たとえば、すべての S3 バケットにログ記録 [読み取り] イベントを指定し、データイベントログ記録に特定のバケットの追加を選択した場合、追加したバケットには既に [読み取り] が設定されています。選択を解除することはできません。[書き込み] のオプションしか設定することができません。

ログ記録からバケットを削除するには、[X] を選択します。

2. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。
3. Lambda 関数の場合

   a. [Data source] で、[Lambda] を選択します。

   b. [Lambda 関数] で、[All regions] を選択してすべての Lambda 関数を口グ記録するか、[Input function as ARN] を使用して、特定の関数のデータイベントを口グ記録します。

      AWS アカウント内のすべての Lambda 関数のデータイベントをログに記録するには、現在および将来のすべての関数を口グに記録するを選択します。この設定は、関数に個々に設定した各設定よりも優先されます。すべての関数が表示されていなくても、関数はすべて口グ記録されます。

      > **Note**
      >
      > すべてのリージョンの証跡を作成する場合、この選択により、 AWS アカウントで現在使用しているすべての関数と、証跡の作成後に任意のリージョンで作成できる Lambda 関数のデータイベント口グ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して実行 AWS CLI) 、この選択により AWS 、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベント口グ記録が有効になります。他のリージョンで作成された Lambda 関数のデータイベントの口グ記録は有効になりません。
      > すべての関数のデータイベントを口グに記録すると、そのアクティビティが別の AWS アカウントに属する関数で実行されている場合でも、アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティの口グ記録も可能になります AWS 。

   c. [Input function as ARN] を選択した場合、Lambda 関数の ARN を入力します。

      > **Note**
      >
      > アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時に CloudTrail コンソールですべての関数を表示または選択することはできません。表示されていない場合でも、すべての関数を口グ記録するオプションを選択することができます。特定の関数のデータイベントを口グ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡を作成したら、 AWS CLI や put-event-selectors コマンドを使用して、特定の Lambda 関数のデータイベント

の口グ記録を設定することもできます。詳しくは、を使用した証跡の管理 AWS CLI を参照してください。

4. データイベントを口グに記録する別のデータタイプを追加するには、[Add data event type] を選択します。
5. DynamoDB テーブルの場合

   a. [Data event source] で、[DynamoDB] を選択します。

   b. [DynamoDB table selection] で、[Browse] を選択してテーブルを選択するか、アクセス許可を持つ DynamoDB テーブルの ARN に貼り付けます。DynamoDB テーブルの ARN は次の形式です。

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   別のテーブルを追加するには、[Add row] を選択し、テーブルを参照するか、アクセス許可のあるテーブルの ARN に貼り付けます。
6. 証跡の Insights イベントとその他の設定を行うには、このトピックで前述した手順、証跡の更新に戻ります。

証跡の削除

CloudTrail 証跡はコンソールで削除できます。組織の管理アカウントまたは委任された管理者アカウントが組織の証跡を削除すると、その証跡は、組織のすべてのメンバーアカウントから削除されます。

Amazon Security Lake で CloudTrail 管理イベントを有効にしている場合は、マルチリージョンでと の両方readwriteの管理イベントを記録する組織証跡を少なくとも 1 つ維持する必要があります。Security Lake で CloudTrail 管理イベントをオフにしない限り、この要件を満たす唯一の証跡である場合、証跡を削除することはできません。

CloudTrail コンソールで証跡を削除するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. CloudTrail コンソールの証跡ページを開きます。
3. 証跡名を選択します。
4. 証跡の詳細ページの上部で、[削除] を選択します。

5. 削除の確認を求められたら、[削除] を選択して証跡を永久的に削除します。証跡のリストから証跡が削除されます。すでに Amazon S3 バケットに配信されているログファイルは削除されません。

> **Note**
>
> Amazon S3 バケットに配信されるコンテンツには、カスタマーコンテンツが含まれている場合があります。機密データの削除の詳細については、Amazon S3 ユーザーガイド」の「バケットを空にする」および「バケットを削除する」を参照してください。

証跡のログ記録をオフにする

証跡を作成すると、自動的にログ記録が有効になります。証跡のログ記録をオフにすることができます。

ログへの記録をオフにしても、既存のログは引き続き証跡の Amazon S3 バケットに保存され、引き続き S3 料金が発生します。

CloudTrail コンソールでトレイルのロギングをオフにするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
2. ナビゲーションメニューで、 [証跡] を選択し、証跡の名前を選択します。
3. 証跡の詳細ページの上部で、[Stop logging] を選択して証跡のログ記録をオフにします。
4. 確認を求められたら、[ログを停止] を選択します。 CloudTrailそのトレイルのアクティビティの記録を停止します。
5. その証跡のログ記録を再開するには、証跡設定ページの [Start logging] を選択します。

を使用した証跡の作成、更新、管理 AWS CLI

を使用して、証跡 AWS CLI を作成、更新、管理できます。を使用する場合 AWS CLI、コマンドはプロファイル用に設定された AWS リージョンで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

> **Note**
>
> このトピックの AWS Command Line Interface （ AWS CLI) AWS コマンドを実行するには、コマンドラインツールが必要です。の最新バージョン AWS CLI がインストールされていることを確認します。詳細については、『AWS Command Line Interface ユーザーガイド』を参照してください。 AWS CLI コマンドラインでの CloudTrail コマンドに関するヘルプについては、「」と入力しますaws cloudtrail help。

証跡の作成、管理、およびステータスに一般的に使用されるコマンド

で証跡を作成および更新するために一般的に使用されるコマンドには CloudTrail 、次のようなものがあります。

- 証跡を作成する create-trail。
- 既存の証跡の設定を変更する update-trail。
- 既存の証跡に 1 つ以上のタグ (キーと値のペア) を追加する add-tags。
- 証跡から 1 つ以上のタグを削除する remove-tags。
- 証跡に関連付けられたタグのリストを返すための list-tags。
- 証跡のイベントセレクタを追加または変更するための put-event-selectors。
- put-insight-selectors既存の証跡の Insights イベントセレクタを追加または変更したり、Insights イベントを有効または無効にしたりするための 。
- 証跡でイベントのログ記録を開始する start-logging。
- 証跡でイベントのログ記録を一時停止する stop-logging。
- 証跡を削除する delete-trail。このコマンドは、その証跡のログファイルが格納されている Amazon S3 バケットは削除しません (存在する場合)。
- describe-trails は、 AWS リージョンの証跡に関する情報を返します。
- 証跡の設定情報を返す get-trail。
- 証跡の現在のステータスに関する情報を返す get-trail-status。
- 証跡用に設定されたイベントセレクタに関する情報を返す get-event-selectors。
- get-insight-selectors証跡用に設定された Insights イベントセレクタに関する情報を返す 。

証跡を作成および更新するためにサポートされているコマンド: create-trail および update-trail。

`create-trail` と `update-trail` コマンドは証跡を作成および管理するための以下のようなさまざまな機能を提供します。

- リージョン間でログを受け取る証跡を作成するか、`--is-multi-region-trail` オプションで証跡を更新します。ほとんどの場合、すべての AWS リージョンのイベントを記録する証跡を作成する必要があります。
- --is-organization-trail オプションを使用して、組織内のすべての AWS アカウントのログを受信する証跡を作成します。
- `--no-is-multi-region-trail` オプションを使用して、マルチリージョンの証跡を単一リージョンの証跡に変換します。
- `--kms-key-id` オプションを使用して、ログファイルの暗号化を有効または無効にします。オプションは、ログの暗号化を CloudTrail に許可するポリシーを既に作成し、アタッチした AWS KMS キーを指定します。詳細については、「CloudTrail による ログファイルの暗号化の有効化と無効化 AWS CLI」を参照してください。
- `--enable-log-file-validation` オプションと `--no-enable-log-file-validation` オプションを使用してログファイルの検証を有効または無効にします。詳細については、「CloudTrail ログファイルの整合性の検証」を参照してください。
- が CloudWatch Logs ロググループにイベントを CloudTrail 配信できるように Logs CloudWatch ロググループとロールを指定します。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

廃止されたコマンド: create-subscription および update-subscription

> **Important**
>
> `create-subscription` と `update-subscription` コマンドは証跡の作成および更新に使用されていましたが、廃止されました。これらのコマンドは使用しないでください。これらのコマンドは証跡を作成および管理するための完全な機能を提供しません。
> これらのコマンドのいずれかまたは両方を使用するオートメーションを設定した場合は、create-trail などのサポートされているコマンドを使用するようにコードまたはスクリプトを更新することをお勧めします。

「create-trail の使用」

create-trail コマンドを実行して、ビジネスニーズに合わせて特別に設定された証跡を作成できます。を使用する場合 AWS CLI、コマンドはプロファイル用に設定された AWS リージョンで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

すべてのリージョンに適用される証跡の作成

すべてのリージョンに適用される証跡を作成するには、--is-multi-region-trail オプションを使用します。デフォルトでは、create-trail コマンドは、証跡が作成された AWS リージョンでのみイベントを記録する証跡を作成します。グローバルサービスイベントを確実にログに記録し、AWS アカウント内のすべての管理イベントアクティビティをキャプチャするには、すべての AWS リージョンでイベントをログに記録する証跡を作成する必要があります。

> **Note**
>
> 証跡を作成するときに、 で作成されていない Amazon S3 バケットを指定する場合は CloudTrail、適切なポリシーをアタッチする必要があります。の Amazon S3 バケットポリシー CloudTrail を参照してください。

次の例では、*my-trail* という名前の証跡と、すべてのリージョンから *my-bucket* という名前の既存のバケットにログを配信する *Marketing* の値を持つ *Group* という名前のキーを持つタグを作成します。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --tags-list [key=Group,value=Marketing]
```

証跡がすべてのリージョンに存在することを確認するために、出力の IsMultiRegionTrail 要素に true と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
```

```
}
```

> **Note**
>
> 証跡のログ記録を開始するには start-logging コマンドを使用します。

証跡のログ記録の開始

create-trail コマンドが完了したら、start-logging コマンドを実行してその証跡のログ記録を開始します。

> **Note**
>
> CloudTrail コンソールで証跡を作成すると、ログ記録が自動的に有効になります。

次の例は、証跡のログ記録を開始します。

```
aws cloudtrail start-logging --name my-trail
```

このコマンドは出力を返しませんが、get-trail-status コマンドを使用すると、ログ記録が開始されたことを確認できます。

```
aws cloudtrail get-trail-status --name my-trail
```

証跡がログを記録していることを確認するために、出力の IsLogging 要素に true と表示されます。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
```

```
}
```

単一リージョンの証跡の作成

次のコマンドは、単一のリージョンの証跡を作成します。指定された Amazon S3 バケットは既に存在し、適切な CloudTrail アクセス許可が適用されている必要があります。詳細については、「の Amazon S3 バケットポリシー CloudTrail」を参照してください。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket
```

詳しくは、命名の要件 を参照してください。

以下は出力例です。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

すべてのリージョンに適用され、ログファイルの検証が有効にされている証跡の作成

create-trail を使用しているときにログファイルの検証を有効にするには、--enable-log-file-validation オプションを使用します。

ログファイルの検証については、「 CloudTrail ログファイルの整合性の検証」を参照してください。

次の例では、すべてのリージョンから指定したバケットにログを配信する証跡を作成します。このコマンドでは、--enable-log-file-validation オプションを使用します。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail --enable-log-file-validation
```

ログファイルの検証が有効になっていることを確認するために、出力の LogFileValidationEnabled 要素に true と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

update-trail の使用

> **Important**
>
> 2021 年 11 月 22 日、 は証跡がグローバルサービスイベントをキャプチャする方法 AWS CloudTrail を変更しました。これで、Amazon CloudFront、、および によって作成されたイベント AWS STS は AWS Identity and Access Management、作成されたリージョン、米国東部 (バージニア北部) リージョン、us-east-1 に記録されます。これにより、 はこれらのサービスを他の AWS グローバルサービスのサービスと一貫して CloudTrail 処理します。米国東部 (バージニア北部) 以外でグローバルサービスイベントを受信するには、米国東部 (バージニア北部) 以外のグローバルサービスイベントを使用するシングルリージョン証跡を、必ずマルチリージョン証跡に変換してください。グローバルサービスイベントのキャプチャの詳細については、このセクション後半の グローバルサービスイベントのログ記録の有効化と無効化 を参照してください。
> 対照的に、 CloudTrail コンソールのイベント履歴と aws cloudtrail lookup-events コマンドは、これらのイベントが発生した AWS リージョン にイベントを表示します。

update-trail コマンドを使用して、証跡の設定を変更できます。add-tags と remove-tags コマンドを使用して、証跡のタグを追加および削除することもできます。更新できるのは、証跡が作成された AWS リージョン (ホームリージョン) からのみです。を使用する場合 AWS CLI、コマンドはプロファイル用に設定された AWS リージョンで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

Amazon Security Lake で CloudTrail 管理イベントを有効にしている場合は、マルチリージョンで との両方readwriteの管理イベントを記録する組織証跡を少なくとも 1 つ維持する必要があります。資格を満たしている証跡を、Security Lake の要件に従わない方法で更新することはできません。例

えば、証跡を単一リージョンに変更したり、read または write 管理イベントのログ記録をオフにしたりするなどです。

> **Note**
>
> AWS CLI またはいずれかの AWS SDKs を使用して証跡を変更する場合は、証跡のバケットポリシーが であることを確認してください up-to-date。バケットが新しい からイベントを自動的に受信するには AWS リージョン、ポリシーに完全なサービス名 が含まれている必要がありますcloudtrail.amazonaws.com。詳細については、「の Amazon S3 バケットポリシー CloudTrail」を参照してください。

トピック

- 1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用
- マルチリージョンの証跡から単一リージョンの証跡への変換
- グローバルサービスイベントのログ記録の有効化と無効化
- ログファイルの検証の有効化
- ログファイルの検証の無効化

1 つのリージョンに適用される証跡を変換してすべてのリージョンに適用

既存の証跡を変更し、すべてのリージョンに適用されるようにするには、--is-multi-region-trail オプションを使用します。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

証跡がすべてのリージョンに適用されるようになったことを確認するために、出力の IsMultiRegionTrail 要素に true と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
```

```
}
```

マルチリージョンの証跡から単一リージョンの証跡への変換

作成元のリージョンにのみ適用されるように既存のマルチリージョンの証跡を変更するには、--no-is-multi-region-trail オプションを使用します。

```
aws cloudtrail update-trail --name my-trail --no-is-multi-region-trail
```

証跡が単一リージョンに適用されるようになったことを確認するために、出力の IsMultiRegionTrail 要素に false と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

グローバルサービスイベントのログ記録の有効化と無効化

証跡を変更し、グローバルサービスイベントをログに記録しないようにするには、--no-include-global-service-events オプションを使用します。

```
aws cloudtrail update-trail --name my-trail --no-include-global-service-events
```

証跡がグローバルサービスイベントをログに記録しなくなったことを確認するために、出力の IncludeGlobalServiceEvents 要素に false と表示されます。

```
{
    "IncludeGlobalServiceEvents": false,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
```

```
}
```

証跡を変更し、グローバルサービスイベントをログに記録するには、`--include-global-service-events` オプションを使用します。

米国東部 (バージニア北部) リージョン us-east-1 では、すでに表示されていない限り、2021 年 11 月 22 日以降、単一リージョン証跡はグローバルサービスイベントを受け取れなくなります。グローバルサービスイベントのキャプチャを続行するには、証跡の設定をマルチリージョン証跡に更新します。例えば、このコマンドは、米国東部 (オハイオ) us-east-2 の単一リージョン証跡をマルチリージョン証跡に更新します。*myExistingSingleRegionTrailWithGSE* を、設定に適した証跡名に置き換えます。

```
aws cloudtrail --region us-east-2 update-trail --
name myExistingSingleRegionTrailWithGSE --is-multi-region-trail
```

2021 年 11 月 22 日以降、グローバルサービスイベントを利用できるのは米国東部 (バージニア北部) のみとなるため、米国東部 (バージニア北部) リージョン us-east-1 では、単一リージョン証跡を作成して、グローバルサービスイベントをサブスクライブすることも可能です。次のコマンドは、us-east-1 に単一リージョンの証跡を作成して CloudFront、、IAM、および AWS STS イベントを受信します。

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name DOC-EXAMPLE-BUCKET
```

ログファイルの検証の有効化

証跡のログファイルの検証を有効にするには、`--enable-log-file-validation` オプションを使用します。ダイジェストファイルは、その証跡の Amazon S3 バケットに配信されます。

```
aws cloudtrail update-trail --name my-trail --enable-log-file-validation
```

ログファイルの検証が有効になっていることを確認するために、出力の `LogFileValidationEnabled` 要素に `true` と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
```

```
    "LogFileValidationEnabled": true,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

ログファイルの検証の無効化

証跡のログファイルの検証を無効にするには、--no-enable-log-file-validation オプションを使用します。

```
aws cloudtrail update-trail --name my-trail-name --no-enable-log-file-validation
```

ログファイルの検証が無効になっていることを確認するために、出力の LogFileValidationEnabled 要素に false と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

でログファイルを検証するには、 AWS CLI「」を参照してください CloudTrail とのログファイルの整合性の検証 AWS CLI。

を使用した証跡の管理 AWS CLI

AWS CLI には、証跡の管理に役立つ他のコマンドがいくつか含まれています。これらのコマンドは、証跡へのタグの追加、証跡ステータスの取得、証跡に対するログ記録の開始と停止、および証跡の削除を行います。これらのコマンドは、証跡が作成されたのと同じ AWS リージョン (ホームリージョン) から実行する必要があります。を使用する場合 AWS CLI、コマンドはプロファイル用に設定された AWS リージョンで実行されることに注意してください。別のリージョンでコマンドを実行する場合は、プロファイルのデフォルトのリージョンを変更するか、コマンドに --region パラメータを使用します。

トピック

- 証跡に 1 つ以上のタグを追加します。
- 1 つ以上の証跡のリストのタグ
- 証跡から 1 つ以上のタグを削除します。
- 証跡の設定と証跡のステータスの取得
- CloudTrail Insights イベントセレクタの設定
- イベントセレクタの設定
- アドバンストイベントセレクタの設定
- 証跡のログ記録の停止と開始
- 証跡の削除

証跡に 1 つ以上のタグを追加します。

既存の証跡に 1 つ以上のタグを追加するには、add-tags コマンドを実行します。

以下の例は、*Owner* という名前と *Mary* の値を持つタグを、米国東部 (オハイオ) リージョンの *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* の ARN を持つ証跡に追加します。

```
aws cloudtrail add-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/my-trail --tags-list Key=Owner,Value=Mary --region us-east-2
```

成功した場合、このコマンドは何も返しません。

1 つ以上の証跡のリストのタグ

1 つ以上の既存の証跡に関連付けられているタグを表示するには、list-tags コマンドを使用します。

次の例では、*Trail1* と *Trail2*のタグを一覧表示します。

```
aws cloudtrail list-tags --resource-id-list arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2
```

正常に完了した場合、このコマンドは以下のような出力を返します。

```
{
 "ResourceTagList": [
```

```
    {
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail1",
        "TagsList": [
            {
                "Value": "Alice",
                "Key": "Name"
            },
            {
                "Value": "Ohio",
                "Key": "Location"
            }
        ]
    },
    {
        "ResourceId": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Trail2",
        "TagsList": [
            {
                "Value": "Bob",
                "Key": "Name"
            }
        ]
    }
  ]
}
```

証跡から 1 つ以上のタグを削除します。

既存の証跡から 1 つ以上のタグを削除するには、remove-tags コマンドを実行します。

以下の例は、米国東部 (オハイオ) リージョンの *arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail* の ARN を持つ証跡から *Location* および *Name* という名前を持つタグを削除します。

```
aws cloudtrail remove-tags --resource-id arn:aws:cloudtrail:us-
east-2:123456789012:trail/Trail1 --tags-list Key=Name Key=Location --region us-east-2
```

成功した場合、このコマンドは何も返しません。

証跡の設定と証跡のステータスの取得

describe-trails コマンドを実行して、 AWS リージョンの証跡に関する情報を取得します。次の例では、米国東部 (オハイオ) リージョンに設定された証跡に関する情報を返します。

```
aws cloudtrail describe-trails --region us-east-2
```

コマンドが正常に完了した場合は、以下のような出力が表示されます。

```
{
  "trailList": [
    {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
    },
    {
      "Name": "my-special-trail",
      "S3BucketName": "another-bucket",
      "S3KeyPrefix": "example-prefix",
      "IncludeGlobalServiceEvents": false,
      "IsMultiRegionTrail": false,
      "HomeRegion": "us-east-2",
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-special-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": true,
      "IsOrganizationTrail": false
    },
    {
      "Name": "my-org-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-1"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-org-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": true
```

```
    }
  ]
}
```

特定の証跡に関する設定情報を取得するには、get-trail コマンドを実行します。次の使用例は、*my-trail* という名前の証跡の設定情報を返します。

```
aws cloudtrail get-trail - -name my-trail
```

正常に完了した場合、このコマンドは以下のような出力を返します。

```
{
   "Trail": {
      "Name": "my-trail",
      "S3BucketName": "my-bucket",
      "S3KeyPrefix": "my-prefix",
      "IncludeGlobalServiceEvents": true,
      "IsMultiRegionTrail": true,
      "HomeRegion": "us-east-2"
      "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
      "LogFileValidationEnabled": false,
      "HasCustomEventSelectors": false,
      "SnsTopicName": "my-topic",
      "IsOrganizationTrail": false,
   }
}
```

証跡のステータスを取得するには get-trail-status コマンドを実行します。このコマンドは、作成された AWS リージョン (ホームリージョン) から実行するか、 --regionパラメータを追加してそのリージョンを指定する必要があります。

> **Note**
>
> 証跡が組織の証跡であり、 の組織のメンバーアカウントである場合は AWS Organizations、名前だけでなく、その証跡の完全な ARN を指定する必要があります。

```
aws cloudtrail get-trail-status --name my-trail
```

コマンドが正常に完了した場合は、以下のような出力が表示されます。

```
{
    "LatestDeliveryTime": 1441139757.497,
    "LatestDeliveryAttemptTime": "2015-09-01T20:35:57Z",
    "LatestNotificationAttemptSucceeded": "2015-09-01T20:35:57Z",
    "LatestDeliveryAttemptSucceeded": "2015-09-01T20:35:57Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-09-01T00:54:02Z",
    "StartLoggingTime": 1441068842.76,
    "LatestDigestDeliveryTime": 1441140723.629,
    "LatestNotificationAttemptTime": "2015-09-01T20:35:57Z",
    "TimeLoggingStopped": ""
}
```

前述の JSON コードに表示されているフィールドに加えて、Amazon SNS または Amazon S3 エラーがある場合はステータスに以下のフィールドが含まれます。

- `LatestNotificationError`。トピックのサブスクリプションに失敗した場合に、Amazon SNS によって出力されたエラーが含まれています。
- `LatestDeliveryError`。 がログファイルをバケットに配信 CloudTrail できない場合に、Amazon S3 によって出力されるエラーが含まれます。

CloudTrail Insights イベントセレクタの設定

put-insight-selectors を実行し、`InsightType` 属性の値として `ApiCallRateInsight`、`ApiErrorRateInsight`、またはその両方を指定して、証跡でInsights イベントを有効にします。証跡の Insights イベントセレクタの設定を表示するには、`get-insight-selectors` コマンドを実行します。証跡が作成された AWS リージョン (ホームリージョン) からこのコマンドを実行するか、 コマンドに --regionパラメータを追加してそのリージョンを指定する必要があります。

> **Note**
>
> `ApiCallRateInsight` の Insights イベントを記録するには、証跡は `write` の管理イベントを記録している必要があります。`ApiErrorRateInsight` の Insights イベントを記録するには、証跡は `read` または `write` の管理イベントを記録している必要があります。

Insights イベントを記録する証跡例

次の例ではput-insight-selectors、 を使用して、*TrailName3* という名前の証跡の Insights イベントセレクタを作成します。これにより、*TrailName3* つの証跡の Insights イベント収集が有効になります。Insightsイベントセレクタは、ApiErrorRateInsight と ApiCallRateInsight Insights の両方のイベントタイプを ログに記録します。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

この例では、証跡用に設定された Insights イベントセレクタを返します。

```
{
   "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

例: 証跡の Insights イベントの収集をオフにする

次の例ではput-insight-selectors、 を使用して、*TrailName3* という名前の証跡の Insights イベントセレクタを削除します。Insights セレクタの JSON 文字列をクリアすると、*TrailName3* つの証跡の Insights イベント収集が無効になります。

```
aws cloudtrail put-insight-selectors --trail-name TrailName3 --insight-selectors '[]'
```

この例では、証跡用に設定された現在空の Insights イベントセレクタを返します。

```
{
   "InsightSelectors": [ ],
   "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName3"
}
```

イベントセレクタの設定

証跡のイベントセレクタの設定を表示するには、get-event-selectors コマンドを実行します。このコマンドは、作成された AWS リージョン (ホームリージョン) から実行するか、 --regionパラメータを使用してそのリージョンを指定する必要があります。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 証跡が組織の証跡であり、 の組織のメンバーアカウントである場合は AWS Organizations、名前だけでなく、その証跡の完全な ARN を指定する必要があります。

次の例は、証跡のイベントセレクタのデフォルト設定を返します。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

イベントセレクタを作成するには、put-event-selectors コマンドを実行します。証跡で Insights イベントを記録する場合は、イベントセレクターで、証跡を設定したい Insights タイプの口ギングが有効になっていることを確認してください。Insights イベントのログ記録に関する詳細については、「Insights イベントのログ記録」を参照してください。

アカウントでイベントが発生すると、 は証跡の設定 CloudTrail を評価します。イベントが証跡のいずれかのイベントセレクタと一致する場合は、証跡がイベントを処理し、ログに記録します。証跡あたり最大 5 つのイベントセレクタと、証跡あたり最大 250 の データリソースを設定できます。詳しくは、データイベントをログ記録する を参照してください。

トピック

- 特定のイベントセレクタを使用した証跡例
- すべての管理イベントとデータイベントを記録する証跡例
- AWS Key Management Service イベントを記録しない証跡の例
- 関連する少量の AWS Key Management Service イベントを記録する証跡の例
- Amazon RDS データ API イベントを記録しない証跡例

特定のイベントセレクタを使用した証跡例

次の例では、 という名前の証跡のイベントセレクタを作成し、読み取り専用と書き込み専用の管理イベント、2 つの Amazon S3 バケット/プレフィックスの組み合わせのデータイベント、および という名前の 1 つの AWS Lambda 関数のデータイベント*TrailName*を含めます*hello-world-python-function*。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/
prefix","arn:aws:s3:::mybucket2/prefix2"]},{"Type": "AWS::Lambda::Function","Values":
 ["arn:aws:lambda:us-west-2:999999999999:function:hello-world-python-function"]}]}]'
```

例では、証跡に対して設定されているイベントセレクタを返します。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda:us-west-2:123456789012:function:hello-world-
python-function"
                    ],
                    "Type": "AWS::Lambda::Function"
```

```
                },
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

すべての管理イベントとデータイベントを記録する証跡例

次の例では、読み取り専用と書き込み専用の管理イベントを含むすべてのイベント、および AWS アカウント内のすべての Amazon S3 バケット、 AWS Lambda 関数、Amazon DynamoDB テーブルのすべてのデータイベントを含む、*TrailName2* という名前の証跡のイベントセレクタを作成します。この例では基本的なイベントセレクタを使用しているため、 での S3 イベントのログ記録 AWS Outposts、Ethereum ノードでの Amazon Managed Blockchain JSON-RPC 呼び出し、またはその他の高度なイベントセレクタリソースタイプを設定することはできません。これらのリソースのデータイベントをログに記録するには、アドバンストイベントセレクタを使用する必要があります。詳しくは、アドバンストイベントセレクタの設定 を参照してください。

> **Note**
>
> 証跡が 1 つのリージョンにのみ適用される場合、イベントセレクタのパラメータですべての Amazon S3 バケットと Lambda 関数が指定されていても、そのリージョン内のイベントのみがログに記録されます。イベントセレクタは、証跡が作成されたリージョンにのみ適用されます。

```
aws cloudtrail put-event-selectors --trail-name TrailName2 --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::"]},{"Type":
 "AWS::Lambda::Function","Values": ["arn:aws:lambda"]},{"Type":
 "AWS::DynamoDB::Table","Values": ["arn:aws:dynamodb"]}]}]'
```

例では、証跡に対して設定されているイベントセレクタを返します。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
```

```
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::"
                    ],
                    "Type": "AWS::S3::Object"
                },
                {
                    "Values": [
                        "arn:aws:lambda"
                    ],
                    "Type": "AWS::Lambda::Function"
                },
{
                    "Values": [
                        "arn:aws:dynamodb"
                    ],
                    "Type": "AWS::DynamoDB::Table"
                }
            ],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName2"
}
```

AWS Key Management Service イベントを記録しない証跡の例

次の例では、 という名前の証跡のイベントセレクタを作成し、読み取り専用と書き込み専用の管理イベント*TrailName*を含めますが、 AWS Key Management Service （ AWS KMS) イベントを除外します。 AWS KMS イベントは管理イベントとして扱われ、大量のイベントが発生する可能性があるため、管理イベントをキャプチャする証跡が複数ある場合、 CloudTrail 請求に大きな影響を与える可能性があります。この例のユーザーは、1 つを除くすべての証跡から AWS KMS イベントを除外することを選択しました。イベントソースを除外するには、イベントセレクタに `ExcludeManagementEventSources` を追加し、文字列値でイベントソースを指定します。

管理イベントをログに記録しないことを選択した場合、 AWS KMS イベントはログに記録されず、AWS KMS イベントログ設定を変更することはできません。

証跡への AWS KMS イベントのログ記録を再開するには、空の配列を の値として渡しますExcludeManagementEventSources。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

この例では、証跡に対して設定されているイベントセレクタを返します。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [ "kms.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

証跡への AWS KMS イベントのログ記録を再開するには、次のコマンドに示すようにExcludeManagementEventSources、空の配列を の値として渡します。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

関連する少量の AWS Key Management Service イベントを記録する証跡の例

次の例では、 という名前の証跡のイベントセレクタを作成しTrailName、書き込み専用管理イベントと AWS KMS イベントを含めます。 AWS KMS イベントは管理イベントとして扱われ、大量のイベントが発生する可能性があるため、管理イベントをキャプチャする証跡が複数ある場合、 CloudTrail 請求に大きな影響を与える可能性があります。この例のユーザーは、、、 を含む AWS KMS 書き込みイベントを含めることを選択しましたがDisableDeleteScheduleKey、、Encrypt、 などのハイボリュームなアクションは含まれません Decrypt GenerateDataKey (これらは読み取りイベントとして扱われます)。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

この例では、証跡に対して設定されているイベントセレクタを返します。これにより、イベントを含む書き込み専用管理 AWS KMS イベントがログに記録されます。

```
{
    "EventSelectors": [
        {
            "ExcludeManagementEventSources": [],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "WriteOnly"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Amazon RDS データ API イベントを記録しない証跡例

次の例では、 という名前の証跡のイベントセレクタを作成し、読み取り専用と書き込み専用の管理イベント*TrailName*を含めますが、Amazon RDS Data API イベントを除外します。Amazon RDS Data API イベントは管理イベントとして扱われ、大量のイベントが発生する可能性があるため、管理イベントをキャプチャする証跡が複数ある場合、 CloudTrail 請求に大きな影響を与える可能性があります。この例のユーザーは、1 つを除くすべての証跡から Amazon RDS Data API イベントを除外することを選択しました。イベントソースを除外するには、イベントセレクタに `ExcludeManagementEventSources` を追加し、Amazon RDS Data API 文字列値でイベントソースを指定します: `rdsdata.amazonaws.com`。

管理イベントをログに記録しないように選択した場合は、Amazon RDS Data API イベントはログに記録されず、 イベントログ設定は変更できません。

Amazon RDS Data API 管理イベントの証跡へのログ記録を再開するには、空の配列を の値として渡しますExcludeManagementEventSources。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["rdsdata.amazonaws.com"],"IncludeManagementEvents": true]}]'
```

この例では、証跡に対して設定されているイベントセレクタを返します。

```
{
    "EventSelectors": [
```

```
        {
            "ExcludeManagementEventSources": [ "rdsdata.amazonaws.com" ],
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

Amazon RDS Data API 管理イベントの証跡へのログ記録を再開するには、次のコマンドに示すようにExcludeManagementEventSources、空の配列を の値として渡します。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true]}]'
```

アドバンストイベントセレクタの設定

基本的なイベントセレクタの代わりに、アドバンストイベントセレクタを使用してデータイベントを含めるか除外するには、証跡の詳細ページでアドバンストイベントセレクタを使用します。高度なイベントセレクタを使用すると、基本的なイベントセレクタよりも多くのリソースタイプでデータイベントをログに記録できます。基本セレクタは S3 オブジェクトアクティビティ、 AWS Lambda 関数の実行アクティビティ、および DynamoDB テーブルをログに記録します。

アドバンストイベントセレクタ で、S3 バケット、 AWS Lambda 関数、DynamoDB テーブル、S3 Object Lambda アクセスポイント、EBS スナップショット上の Amazon EBS direct APIs、S3 アクセスポイント、DynamoDB ストリーム、Lake Formation によって作成された AWS Glue テーブルなど、特定のリソースタイプでデータイベントを収集する式を構築します。

高度なイベントセレクタの詳細については、アドバンストイベントセレクタの設定 を参照してください。

証跡のアドバンストイベントセレクタの設定を表示するには、get-event-selectors コマンドを実行します。証跡が作成された AWS リージョン (ホームリージョン) からこのコマンドを実行するか、 --regionパラメータを追加してそのリージョンを指定する必要があります。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 証跡が組織の証跡であり、 の組織のメンバーアカウントでサインインしている場合は AWS Organizations、名前だけでなく、証跡の完全な ARN を指定する必要があります。

次の例は、証跡のアドバンストイベントセレクタのデフォルト設定を返します。デフォルトでは、証跡用にはアドバンストイベントセレクタは設定されていません。

```
{
    "AdvancedEventSelectors": [],
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

アドバンストイベントセレクタを作成するには、put-event-selectors コマンドを実行します。アカウントでデータイベントが発生すると、 は証跡の設定 CloudTrail を評価します。イベントが証跡のいずれかのアドバンストイベントセレクタと一致する場合は、証跡がイベントを処理し、ログに記録します。1 つの証跡に最大 500 の条件を設定できます。これには、証跡上のすべてのアドバンストイベントセレクタに指定されたすべての値が含まれます。詳しくは、データイベントを口グ記録する を参照してください。

トピック

- 特定のアドバンストイベントセレクタを使用した証跡例
- カスタムアドバンストイベントセレクタを使用して Amazon S3 を AWS Outposts データイベントに記録する証跡の例
- アドバンストイベントセレクタを使用して AWS Key Management Service イベントを除外する証跡の例
- アドバンストイベントセレクタを使用して Amazon RDS Data API 管理イベントを除外する証跡の例

特定のアドバンストイベントセレクタを使用した証跡例

次の例では、 という名前の証跡のカスタムアドバンストイベントセレクタを作成し*TrailName*、読み取り/書き込み管理イベント (readOnlyセレクタを省略) PutObjectと、 という名前のバケットsample_bucket_nameと という名前の AWS Lambda 関数DeleteObjectのデータイベントを除くすべての Amazon S3 バケット/プレフィックスの組み合わせのデータイベントを含めますMyLambdaFunction。これらはカスタムアドバンストイベントセレクタであるため、セレクタの

各セットにはわかりやすい名前をつけます。末尾のスラッシュは S3 バケットの ARN 値の一部であることに注意してください。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
```

```
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
```

```
}
```

カスタムアドバンストイベントセレクタを使用して Amazon S3 を AWS Outposts データイベントに記録する証跡の例

次の例は、アウトポスト内の AWS Outposts オブジェクトにすべての Amazon S3 のすべてのデータイベントを含めるように証跡を設定する方法を示しています。このリリースでは、`resources.type`フィールドの AWS Outposts イベントで S3 でサポートされる値は `AWS::S3Outposts::Object`です。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

コマンドは、次の出力例を返します。

```
{
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
```

```
        }
    ],
  "TrailARN": "arn:aws:cloudtrail:region:123456789012:trail/TrailName"
}
```

アドバンストイベントセレクタを使用して AWS Key Management Service イベントを除外する証跡の例

次の例では、 という名前の証跡のアドバンストイベントセレクタを作成し*TrailName*、読み取り専用と書き込み専用の管理イベント (`readOnly`セレクタを省略) を含めますが、 AWS Key Management Service （ AWS KMS) イベントを除外します。 AWS KMS イベントは管理イベントとして扱われ、大量のイベントが発生する可能性があるため、管理イベントをキャプチャする証跡が複数ある場合、 CloudTrail 請求に大きな影響を与える可能性があります。

管理イベントをログに記録しないことを選択した場合、 AWS KMS イベントはログに記録されず、AWS KMS イベントログ設定を変更することはできません。

証跡への AWS KMS イベントのログ記録を再開するには、 `eventSource` セレクタを削除し、 コマンドを再度実行します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
```

```
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

除外されたイベントの証跡へのログ記録を再開するには、次のコマンドに示されるように、eventSource セレクタを削除します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

アドバンストイベントセレクタを使用して Amazon RDS Data API 管理イベントを除外する証跡の例

次の例では、 という名前の証跡のアドバンストイベントセレクタを作成し*TrailName*、読み取り専用と書き込み専用の管理イベント (readOnlyセレクタを省略) を含めますが、Amazon RDS Data API 管理イベントを除外します。Amazon RDS Data API 管理イベントを除外するには、 eventSourceフィールドの文字列値に Amazon RDS Data API イベントソースを指定しますrdsdata.amazonaws.com。

管理イベントをログに記録しない場合、Amazon RDS Data API 管理イベントはログに記録されず、Amazon RDS Data API イベントログ設定を変更することはできません。

Amazon RDS Data API 管理イベントの証跡へのログ記録を再開するには、 eventSource セレクタを削除し、 コマンドを再度実行します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
```

```
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

除外されたイベントの証跡へのログ記録を再開するには、次のコマンドに示されるように、eventSource セレクタを削除します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
```

```
]'
```

証跡のログ記録の停止と開始

次のコマンドは、 CloudTrail ログ記録を開始および停止します。

```
aws cloudtrail start-logging --name awscloudtrail-example
```

```
aws cloudtrail stop-logging --name awscloudtrail-example
```

> **Note**
>
> バケットを削除する前に、stop-logging コマンドを実行してバケットへのイベントの配信を停止します。ログ記録を停止しない場合、 CloudTrail は、一定期間、同じ名前のバケットにログファイルを配信しようとします。
> ログ記録を停止したり、証跡を削除したりすると、その証跡では CloudTrail Insights が無効になります。

証跡の削除

Amazon Security Lake で CloudTrail 管理イベントを有効にしている場合は、マルチリージョンでと の両方readwriteの管理イベントを記録する組織証跡を少なくとも 1 つ維持する必要があります。Security Lake で CloudTrail 管理イベントをオフにしない限り、この要件を満たす唯一の証跡である場合、証跡を削除することはできません。

次のコマンドを使用して証跡を削除することができます。証跡は、それが作成されたリージョン (ホームリージョン) でのみ削除できます。

```
aws cloudtrail delete-trail --name awscloudtrail-example
```

証跡を削除しても、Amazon S3 バケットまたはそれに関連付けられている Amazon SNS トピックは削除されません。 AWS Management Console、 AWS CLI、または サービス API を使用して、これらのリソースを個別に削除します。

組織の証跡の作成

で組織を作成した場合は AWS Organizations、その組織 AWS アカウント 内のすべての のすべてのイベントを記録する証跡を作成できます。これは、組織の証跡と呼ばれることもあります。

組織の管理アカウントは、新しい組織の証跡を作成する、または既存の組織の証跡を管理する委任された管理者を割り当てることができます。委任された管理者の追加の詳細については、「CloudTrail 委任された管理者を追加する」を参照してください。

組織の管理アカウントは、アカウントの既存の証跡を編集して組織に適用し、それを組織の証跡にすることができます。組織の証跡では、組織内の管理アカウントとすべてのメンバーアカウントのイベントが記録されます。の詳細については AWS Organizations、「Organizations の用語と概念」を参照してください。

> **Note**
>
> 組織の証跡を作成するには、その組織の管理アカウントまたは委任された管理者アカウントを使用してサインインする必要があります。また、証跡を作成するには、管理アカウントまたは委任された管理者アカウントのユーザーまたはロールに十分なアクセス許可が必要です。十分なアクセス許可がない場合は、証跡を組織に適用するオプションは使用できません。

コンソールを使用して作成されたすべての組織の証跡は、組織内の各メンバーアカウントで有効になっている AWS リージョン からのイベントをログに記録するマルチリージョン組織の証跡です。組織内のすべての AWS パーティションのイベントをログに記録するには、各パーティションにマルチリージョン組織の証跡を作成します。を使用して、単一リージョンまたはマルチリージョンの組織の証跡を作成できます AWS CLI。単一リージョンの証跡を作成する場合は、証跡の AWS リージョン （ ホームリージョンとも呼ばれる) でのみアクティビティを記録します。

ほとんどの AWS リージョン は でデフォルトで有効になっていますが AWS アカウント、特定のリージョン (オプトインリージョンとも呼ばれます) を手動で有効にする必要があります。デフォルトで有効になっているリージョンについては、「 AWS Account Management リファレンスガイド」の「リージョンを有効または無効にする前の考慮事項」を参照してください。が CloudTrail サポートするリージョンのリストについては、「」を参照してくださいCloudTrail サポートされているリージョン。

組織の証跡を作成すると、指定した名前の証跡のコピーが、組織に属するメンバーアカウントに作成されます。

- 組織の証跡が単一リージョン用で、証跡のホームリージョンがオプトリージョン でない場合、証跡のコピーは各メンバーアカウントの組織の証跡のホームリージョンに作成されます。

- 組織の証跡が単一リージョン用で、証跡のホームリージョンがオプトリージョン の場合、証跡のコピーは、そのリージョンを有効にしたメンバーアカウントの組織の証跡のホームリージョンに作成されます。
- 組織の証跡がマルチリージョンで、証跡のホームリージョンがオプトインリージョン でない場合、証跡のコピーは各メンバーアカウントで有効になっている各 AWS リージョン に作成されます。メンバーアカウントがオプトインリージョンを有効にすると、マルチリージョン証跡のコピーが、そのリージョンのアクティベーションが完了した後に、メンバーアカウントの新しくオプトインされたリージョンに作成されます。
- 組織の証跡がマルチリージョンで、ホームリージョンがオプトインリージョン の場合、 AWS リージョン マルチリージョン証跡が作成された をオプトインしない限り、メンバーアカウントは組織の証跡にアクティビティを送信しません。例えば、マルチリージョンの証跡を作成し、証跡のホームリージョンとして欧州 (スペイン) リージョンを選択した場合、そのアカウントの欧州 (スペイン) リージョンを有効にしたメンバーアカウントのみが、そのアカウントのアクティビティを組織の証跡に送信します。

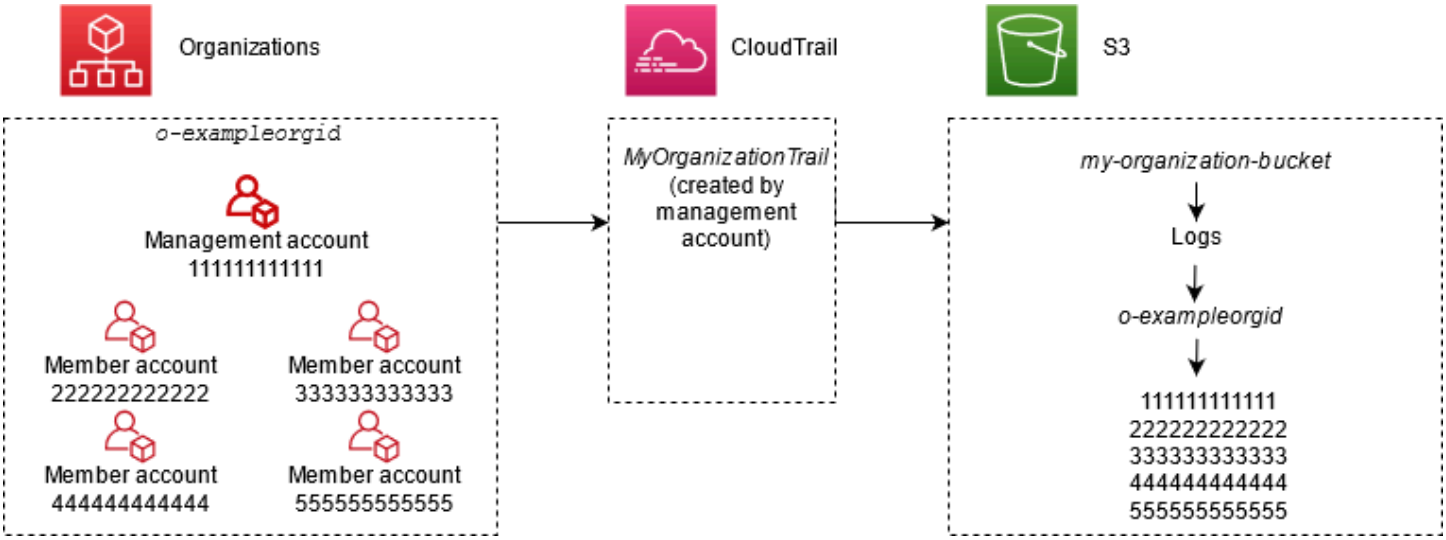
> **Note**
>
> CloudTrail は、リソースの検証が失敗した場合でも、メンバーアカウントに組織の証跡を作成します。検証の失敗の例は次のとおりです。
>
> - Amazon S3 バケットポリシーが正しくない
> - Amazon SNS トピックポリシーが正しくない
> - Logs CloudWatch ロググループに配信できない
> - KMS キーを使用して暗号化するアクセス許可が不十分
>
> アクセス CloudTrail 許可を持つメンバーアカウントは、 CloudTrail コンソールで証跡の詳細ページを表示するか、 コマンドを実行する AWS CLI get-trail-statusことで、組織の証跡の検証に失敗したことを確認できます。

メンバーアカウントで CloudTrail アクセス許可を持つユーザーは、 から AWS CloudTrail コンソールにログインするとき AWS アカウント、または などの AWS CLI コマンドを実行するときに、組織の証跡を表示できますdescribe-trails。ただし、メンバーアカウントのユーザーには、組織の証跡の削除、ログのオン/オフの切り替え、ログに記録されるイベントの種類の変更、または組織の証跡の変更を行うための十分なアクセス許可がありません。

コンソールで組織の証跡を作成するか、Organizations で信頼されたサービス CloudTrail として を有効にすると、組織のメンバーアカウントでログ記録タスクを実行するためのサービスにリンクされたロールが作成されます。このロールの名前は でAWSServiceRoleForCloudTrail、 が組織のイベントを ログ CloudTrail に記録するために必要です。 AWS アカウント が組織に追加されると、組織の証跡とサービスにリンクされたロールがその に追加され AWS アカウント、組織の証跡でそのアカウントのログ記録が自動的に開始されます。 AWS アカウント が組織から削除されると、組織の証跡とサービスにリンク AWS アカウント されたロールは、組織に含まれなくなった から削除されます。ただし、アカウントが削除される前に作成した削除されたアカウントのログファイルは、証跡用にログファイルが保存されている Amazon S3 バケットに残ります。

AWS Organizations 組織の管理アカウントが組織の証跡を作成し、その後組織の管理アカウントとして削除された場合、そのアカウントを使用して作成された組織の証跡は非組織の証跡になります。

次の例では、組織の管理アカウント 111111111111 が組織の *o-exampleorgid* *MyOrganizationTrail*に という名前の証跡を作成します。証跡は、同じ Amazon S3 バケット内の組織内のすべてのアカウントのアクティビティを記録します。組織内のすべてのアカウントは証跡のリスト*MyOrganizationTrail*に を表示できますが、メンバーアカウントは組織の証跡を削除または変更できません。組織の証跡を変更または削除できるのは、管理アカウントまたは委任された管理者アカウントのみです。組織からメンバーアカウントを削除できるのは、管理アカウントのみです。同様に、デフォルトでは、管理アカウントのみが証跡*my-organization-bucket*の Amazon S3 バケットとその中に含まれるログにアクセスできます。ログファイルの高レベルのバケット構造では、組織 ID で名前が付けられたフォルダと、組織内の各アカウントのアカウント ID で名前が付けられたサブフォルダが含まれます。各メンバーアカウントのイベントは、メンバーアカウント ID に対応するフォルダに記録されます。メンバーアカウント 444444444444 が組織から削除*MyOrganizationTrail*され、サービスにリンクされたロールが AWS アカウント 444444444444 に表示されなくなり、そのアカウントのイベントが組織の証跡によってログに記録されなくなります。ただし、444444444444 フォルダは Amazon S3 バケットに残り、組織からアカウントを削除する前にすべてのログが作成されます。



この例では、管理アカウントで作成した証跡の ARN は `aws:cloudtrail:us-east-2:111111111111:trail/MyOrganizationTrail` です。この ARN は、すべてのメンバーアカウントにおける証跡の ARN でもあります。

組織の証跡は多くの点で通常の証跡と似ています。組織に複数の証跡を作成し、他の証跡と同様に、すべてのリージョンまたは単一のリージョンに組織の証跡を作成するかどうか、および組織の証跡に記録するイベントの種類を選択できます。ただし、相違点がいくつかあります。例えば、コンソールで証跡を作成し、Amazon S3 バケットまたは AWS Lambda 関数のデータイベントをログに記録するかどうかを選択すると、 CloudTrail コンソールに表示されるリソースは管理アカウントのリソースのみですが、メンバーアカウントのリソースの ARNs を追加できます。指定されたメンバーアカウントリソースのデータイベントは、それらのリソースへのクロスアカウントアクセスを手動で設定しなくても記録されます。管理イベント、Insights イベント、およびデータイベントの口グ記録の詳細については、管理イベントのログ記録「」、データイベントをログ記録する「」、および「」を参照してくださいInsights イベントのログ記録。

> **Note**
>
> コンソールで、マルチリージョンの証跡を作成します。これは推奨されるベストプラクティスです。 のすべてのリージョンでアクティビティをログに記録すると AWS アカウント 、AWS 環境をより安全に維持できます。単一リージョンの証跡を作成するには、 AWS CLIを使用します。

の組織のイベント履歴でイベントを表示すると AWS Organizations、サインイン AWS アカウントしている のイベントのみを表示できます。例えば、組織管理アカウントでサインインしている場

合、[イベント履歴] には、管理アカウントの過去 90 日間の管理イベントが表示されます。組織メンバーのアカウントイベントは、管理アカウントの [Event history] (イベント履歴) に表示されません。[イベント履歴] のメンバーアカウントのイベントを表示するには、メンバーアカウントでサインインします。

組織の証跡の CloudTrail ログで収集されたイベントデータを、他の証跡と同じようにさらに分析して処理するように、他の AWS サービスを設定できます。例えば、Amazon Athena を使用して組織の証跡のデータを分析できます。詳細については、「AWS CloudTrail ログと サービスの統合」を参照してください。

トピック

メンバーアカウントの証跡から組織の証跡への移行

個々のメンバーアカウントに既に CloudTrail 証跡を設定しているが、組織の証跡に移動してすべてのアカウントのイベントをログ記録する場合は、組織の証跡を作成する前に個々のメンバーアカウントの証跡を削除してイベントを失わないようにします。ただし、証跡が 2 つあると、組織の証跡に配信されるイベントのコピー分、コストが高くなります。

コストを抑えながら、組織の証跡へのログ配信前にイベントが失われないようにするには、個々のメンバーアカウントの証跡と組織の証跡の両方を最大 1 日間、保持することを検討してください。これにより、組織の証跡ですべてのイベントが記録されますが、重複するイベントコストは 1 日間分で済みます。1 日目が過ぎれば、個々のメンバーアカウントの証跡へのログ記録を停止 (または削除) できます。

組織の証跡の作成を準備する

組織の証跡を作成する前に、組織の管理アカウントまたは委任された管理者アカウントが証跡の作成用に正しく設定されていることを確認してください。

- 証跡を作成する前に、組織ですべての機能を有効にしておく必要があります。詳細については、「組織内のすべての機能の有効化」を参照してください。

- 管理アカウントには AWSServiceRoleForOrganizations ロールが必要です。このロールは、組織の作成時に Organizations によって自動的に作成され、 が組織のイベント CloudTrail をログに記録するために必要です。詳細については、「Organizations およびサービスにリンクされたロール」を参照してください。
- 管理アカウントまたは委任された管理者アカウントで組織の証跡を作成するユーザーまたはロールには、組織の証跡を作成するのに十分なアクセス許可が必要です。少なくとも、AWSCloudTrail_FullAccess ポリシーまたは同等のポリシーをそのロールまたはユーザーに適用する必要があります。また、IAM と Organizations には、サービスリンクのロールを作成し、信頼されたアクセスを有効にするための十分なアクセス許可が必要です。 CloudTrail コンソールを使用して組織の証跡用に新しい S3 バケットを作成する場合は、ポリシーには も含める必要があります。 `s3:PutEncryptionConfiguration` アクション。デフォルトでは、バケットに対してサーバー側の暗号化が有効になっているためです。次のポリシー例は、これらの最低限必要なアクセス許可を示しています。

> **Note**
>
> AWSCloudTrail_FullAccess ポリシーを 間で広く共有しないでください AWS アカウント。代わりに、 AWS アカウント によって収集される情報の機密性が高いため、管理者に制限する必要があります CloudTrail。このロールを持つユーザーは、 AWS アカウントの最も機密かつ重要な監査機能を無効にしたり、再設定したりすることができます。このため、このポリシーへのアクセスは、厳密に管理および監視する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListAccounts",
                "iam:CreateServiceLinkedRole",
                "organizations:DisableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

- AWS CLI または CloudTrail APIs を使用して組織の証跡を作成するには、Organizations CloudTrail で の信頼されたアクセスを有効にし、組織の証跡のログ記録を許可するポリシーを使用して Amazon S3 バケットを手動で作成する必要があります。詳細については、「を使用して組織の証跡を作成する AWS Command Line Interface」を参照してください。
- 既存の IAM ロールを使用して組織の証跡のモニタリングを Amazon CloudWatch Logs に追加するには、次の例に示すように、IAM ロールを手動で変更して、メンバーアカウントの CloudWatch ログを管理アカウントの CloudWatch ロググループに配信できるようにする必要があります。

> **Note**
>
> 自分のアカウントに存在する IAM ロールと CloudWatch ロググループを使用する必要があります。別のアカウントが所有する IAM ロールまたは CloudWatch ロググループを使用することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
```

```
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

CloudTrail および Amazon CloudWatch Logs の詳細については、「」を参照してくださいAmazon CloudTrail CloudWatch ログによるログファイルのモニタリング。さらに、組織の証跡で エクスペリエンスを有効にする前に、 CloudWatch ログの制限とサービスの料金に関する考慮事項を考慮してください。詳細については、CloudWatch 「ログの制限」と「Amazon の料金」を参照してください。 CloudWatch

- メンバーアカウントの特定のリソースについて組織内のデータイベントを記録するには、それらの各リソースの Amazon リソースネーム (ARN) のリストを準備します。証跡の作成時にメンバーアカウントのリソースは CloudTrail コンソールに表示されません。S3 バケットなど、データイベント収集がサポートされている管理アカウントのリソースを参照できます。同様に、コマンドラインで組織の証跡を作成または更新するときに特定のメンバーリソースを追加する場合は、それらのリソースの ARN が必要です。

> **Note**
>
> データイベントのログ記録には追加料金が適用されます。 CloudTrail 料金については、「AWS CloudTrail の料金」を参照してください。

また、組織の trail. を作成する前に、管理アカウントとメンバーアカウントに既に存在する証跡の数を確認することも検討する必要があります。各リージョンで作成できる証跡の数 CloudTrail を制限します。管理アカウントで組織の証跡を作成するリージョンでは、この制限を超えることはできません。ただし、メンバーアカウントがリージョン内の証跡の上限に達した場合でも、証跡はメンバーアカウントに作成されます。どのリージョンでも管理イベントの最初の証跡は無料ですが、追加の証跡には料金がかかります。組織の証跡の潜在的なコストを削減するには、管理アカウントとメンバーアカウントの不要な証跡を削除することを検討してください。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

組織の証跡におけるセキュリティのベストプラクティス

セキュリティのベストプラクティスとして、組織証跡で使用するリソースポリシー (S3 バケット、KMS キー、SNS トピックなど) に aws:SourceArn 条件キーを追加することが奨励されています。aws:SourceArn の値は、組織の証跡 ARN (または、複数の証跡のログを保存するために同じ S3 バケットなど、複数の証跡に同じリソースを使用している場合は ARN) です。これにより、S3 バケットなどのリソースは、特定の証跡に関連付けられているデータのみを受け付けます。証跡 ARN は、管理アカウントのアカウント ID を使用する必要があります。次のポリシースニペットは、複数の証跡がリソースを使用している例を示しています。

```
"Condition": {
    "StringEquals": {
      "aws:SourceArn": ["Trail_ARN_1",..., "Trail_ARN_n"]
    }
}
```

リソースポリシーに条件キーを追加する方法については、以下を参照してください。

- の Amazon S3 バケットポリシー CloudTrail
- AWS KMS の主要ポリシーの設定 CloudTrail
- の Amazon SNS トピックポリシー CloudTrail

コンソールで組織の証跡を作成する

CloudTrail コンソールから組織の証跡を作成するには、十分なアクセス許可を持つ管理アカウントまたは委任管理者アカウントのユーザーまたはロールとしてコンソールにサインインする必要があります。管理アカウントまたは委任管理者アカウントでサインインしない場合、コンソールから CloudTrail証跡を作成または編集するときに、組織に証跡を適用するオプションは表示されません。

組織の証跡をさまざまな方法で設定することができます。たとえば、組織の証跡については、次の詳細を設定することができます。

- デフォルトでは、コンソールで証跡を作成すると、証跡によって、作業中の AWS パーティションのすべての AWS リージョン が ログ記録されます。ベストプラクティスとして、 のすべてのリージョンでイベントをログに記録することを強くお勧めします AWS アカウント。単一リージョンの証跡を作成するには、 AWS CLI を使用します。
- 証跡を組織に適用するかどうかを指定します。デフォルトでは、証跡は組織には適用されません。組織の証跡を作成するには、このオプションを選択する必要があります。

- 組織の証跡用のログファイルを受信する Amazon S3 バケットを指定します。既存の Amazon S3 バケットを選択するか、組織の証跡用に特別に作成することができます。
- 管理イベントとデータイベントについて、ログ記録の対象を [読み取り] イベントにするか、[書き込み] イベントにするか、それともすべてのイベントにするかを指定する。CloudTrail Insights イベントは、管理イベントにのみ記録されます。管理アカウントのリソースのログデータイベントを指定するには、コンソールのリストからそれらを選択します。データイベント記録を有効にする各リソースの ARM を指定した場合は、メンバーアカウントで指定できます。詳細については、「データイベント」を参照してください。

を使用して組織の証跡を作成するには AWS Management Console

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。

   組織の証跡を作成するには、十分な権限 を持つ管理アカウントまたは委任された管理者アカウントの IAM ID を使用してサインインする必要があります。
2. [Trails] (証跡) を選択し、[Create trail] (証跡の作成) を選択します。
3. [Create Trail] (証跡の作成) ページの [Trail name] (証跡名) に証跡の名前を入力します。詳細については、「命名の要件」を参照してください。
4. [組織内のすべてのアカウントに対して有効にする] を選択します。管理アカウントまたは委任された管理者アカウントのユーザーまたはロールでコンソールにサインインした場合にのみ、このオプションが表示されます。組織の証跡を正しく作成するには、ユーザーまたはロールに十分なアクセス許可があることを確認してください。
5. [ストレージの場所] の [S3 バケットを作成する] を選択すると、新しいバケットが作成されます。バケットを作成すると、 は必要なバケットポリシー CloudTrail を作成して適用します。

> **Note**
>
> [Use existing S3 bucket] を選択した場合、[Trail log bucket name] のバケットを指定するか、[Browse] を選択してバケットを選択します。任意のアカウントに属するバケットを選択できますが、バケットポリシーは、そのアカウントに書き込むアクセス許可を付与 CloudTrailする必要があります。バケットポリシーを手動で編集する方法については、の Amazon S3 バケットポリシー CloudTrail を参照してください。

ログを見つけやすくするには、既存のバケットに新しいフォルダ (プレフィックス とも呼ばれます) を作成して CloudTrail ログを保存します。プレフィックスを [プレフィックス] に入力します。

6. [Log file SSE-KMS encryption] (ログファイルの SSE-KMS 暗号化) で、SSE-S3 暗号化を使用する代わりに SSE-KMS 暗号化を使用してログファイルを暗号化する場合は、[Enabled] (有効) を選択します。デフォルトは [Enabled] です。SSE-KMS 暗号化を有効にしない場合、ログは SSE-S3 暗号化を使用して暗号化されます。SSE-KMS 暗号化の詳細については、「AWS Key Management Service (SSE-KMS) によるサーバー側の暗号化の使用」を参照してください。SSE-S3 暗号化の詳細については、「Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3) の使用」を参照してください。

   SSE-KMS 暗号化を有効にする場合は、新規または既存の AWS KMS keyを選択します。AWS KMS エイリアス で、 形式でエイリアスを指定しますalias/*MyAliasName*。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。

   > **Note**
   >
   > 別のアカウントのキーの ARN を入力することもできます。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。キーポリシーでは、CloudTrail が キーを使用してログファイルを暗号化し、指定したユーザーが暗号化されていない形式でログファイルを読み取れるようにする必要があります。キーポリシーを手動で編集する方法については、AWS KMS の主要ポリシーの設定 CloudTrail を参照してください。

7. [Additional settings] で、次の操作を行います。

   a. [ログファイル検証を有効にする] で [Enabled] を選択して、S3 バケットにログダイジェストが配信されるようにします。ダイジェストファイルを使用して、 CloudTrail 配信後にログファイルが変更されていないことを確認できます。詳細については、「 CloudTrail ログファイルの整合性の検証」を参照してください。

   b. SNS 通知配信 では、ログがバケットに配信されるたびに通知されるように有効化 を選択します。 は複数のイベントをログファイルに CloudTrail 保存します。SNS 通知は、ログファイルごとに送信されます (イベントごとではありません)。詳細については、「の Amazon SNS 通知の設定 CloudTrail」を参照してください。

SNS 通知を有効にすると、[Create a new SNS topic] で、[New] を選択してトピックを作成するか、[Existing] を選択して既存のトピックを使用します。すべてのリージョンに適用される証跡を作成した場合、すべてのリージョンからのログファイル配信を知らせる SNS 通知は、ユーザーが作成した単一の SNS トピックに送信されます。

新しい を選択した場合、 は新しいトピックの名前 CloudTrail を指定するか、名前を入力できます。[Existing] を選択した場合、ドロップダウンリストから SNS トピックを選択します。別のリージョンにあるトピックの ARN を入力したり、適切なアクセス許可を持ったアカウントにあるトピックの ARN を入力することもできます。詳細については、「の Amazon SNS トピックポリシー CloudTrail」を参照してください。

トピックを作成する場合は、ログファイル配信の通知を受けるトピックを受信登録する必要があります。受信登録は Amazon SNS コンソールから行うことができます。通知頻度の都合上、受信登録については、Amazon SQS キューを使用して通知をプログラムで処理するように設定することをお勧めします。詳細については、[Amazon Simple 通知サービスデベロッパーガイド] の [Amazon SNS の使用開始] を参照してください。

8. オプションで、 CloudWatch ログ で有効 を選択してログファイルをログに送信する CloudTrail ように CloudWatch を設定します。詳細については、「 CloudWatch ログへのイベントの送信」を参照してください。

> **Note**
>
> 管理アカウントのみが、 コンソールを使用して組織の証跡の CloudWatch ロググループを設定できます。委任管理者は、 AWS CLI または CloudTrail `CreateTrail` `UpdateTrail` API オペレーションを使用して CloudWatch Logs ロググループを設定できます。

   a. CloudWatch ログとの統合を有効にする場合は、新規 を選択して新しいロググループを作成するか、既存 を選択して既存のロググループを使用します。新しい を選択した場合、 は新しいロググループの名前 CloudTrail を指定するか、名前を入力できます。

   b. [Existing] を選択した場合、ドロップダウンリストからロググループを選択します。

   c. 新規 を選択して、ログを ログに送信するアクセス許可用の新しい IAM CloudWatch ロールを作成します。[Existing] を選択して、ドロップダウンリストから既存の IAM ロールを選択します。新しいロールまたは既存のロールのポリシーステートメントは、[ポリシードキュメント] を展開すると表示されます。このロールの詳細については、「 CloudTrail

CloudWatch ログを監視に使用するためのロールポリシードキュメント」を参照してください。

> **Note**
>
> 証跡を設定する際には、別のアカウントに属している S3 バケットや Amazon SNS トピックを選択することもできます。ただし、イベント CloudTrail を Logs CloudWatch ロググループに配信する場合は、現在のアカウントに存在するロググループを選択する必要があります。

9. [タグ] で、1 つまたは複数のカスタムタグ (キーと値のペア) を証跡に追加します。タグは、証 CloudTrail 跡と CloudTrail ログファイルを含む Amazon S3 バケットの両方を識別するのに役立ちます。その後、リソースに CloudTrail リソースグループを使用できます。詳細については、「AWS Resource Groups」および「タグ」を参照してください。
10. [Choose log events] ページで、ログに記録するイベントタイプを選択します。[管理イベント] で、次の操作を行います。

    a. [API activity] で、証跡で記録する対象を [読み取り] イベント、[書き込み] イベント、またはその両方を選択します。詳細については、「管理イベント」を参照してください。

    b. AWS KMS イベントを除外を選択して、証跡から (AWS KMS) イベントをフィルタリング AWS Key Management Service します。デフォルト設定では、すべての AWS KMS イベントが含まれています。

    AWS KMS イベントをログまたは除外するオプションは、証跡に管理イベントをログに記録する場合にのみ使用できます。管理イベントをログに記録しないことを選択した場合、AWS KMS イベントはログに記録されず、 AWS KMS イベントログ設定を変更することはできません。

    AWS KMS `Encrypt`、、 などの アクションは`Decrypt`、`GenerateDataKey`通常、大量のイベント (99% 以上) を生成します。これらのアクションは、[読み取り] イベントとしてログに記録されるようになりました。、、 `Delete` `ScheduleKey` (通常は AWS KMS イベントボリュームの 0.5% 未満を占める) `Disable`などの少量の関連 AWS KMS アクションは、書き込みイベントとして記録されます。

    `Encrypt`、`Decrypt`、`GenerateDataKey` のようなボリュームの大きなイベントを除外し、`Disable`、`Delete`、`ScheduleKey` などの関連イベントを記録する場合は、[書き込み] 管理イベントを記録することを選択し、[Exclude AWS KMS events] チェックボックスをオフにします。

c. [Exclude Amazon RDS Data API events] を選択して、証跡から Amazon Relational Database Service データ API イベントを除外できます。デフォルト設定では、すべての Amazon RDS Data API イベントが含まれています。Amazon RDS Data API イベントの詳細については、Aurora の　Amazon RDS Amazon RDS ユーザーガイドの「AWS CloudTrailによる Data API コールのログ記録」を参照してください。

11. データイベントをログに記録するには、[データイベント] を選択します。データイベントのログ記録には追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

12.

> **Important**
>
> ステップ 12 ~ 16 は、デフォルトである高度なイベントセレクターを使用してデータイベントを設定するためのものです。高度なイベントセレクターでは、より多くのデータイベントタイプを設定し、証跡でキャプチャするデータイベントをきめ細かく制御できます。基本的なイベントセレクターを使用する場合は、基本的なイベントセレクターを使用してデータイベント設定を構成する のステップを完了してから、この手順のステップ 17 に戻ってください。

[データイベントタイプ] で、データイベントをログ記録するリソースのタイプを選択します。使用可能なデータイベントタイプの詳細については、「データイベント」を参照してください。

> **Note**
>
> Lake Formation によって作成された AWS Glue テーブルのデータイベントをログに記録するには、Lake Formation を選択します。

13. ログセレクタテンプレートを選択します。 には、リソースタイプのすべてのデータイベントをログに記録する事前定義されたテンプレート CloudTrail が含まれています。カスタムログセレクタテンプレートを構築するには、[Custom] を選択します。

> **Note**
>
> S3 バケットの事前定義されたテンプレートを選択すると、 AWS 現在アカウントにあるすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意の IAM ID によって実行されたデータイベントアクティビティのログ記録も有効にします。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。

証跡が 1 つのリージョンのみに適用される場合、すべての S3 バケットを口グ記録する事前定義済みテンプレートを選択すると、同じリージョン内のすべてのバケット、およびそのリージョンで後に作成するバケットに対して、データイベントの口グ記録が可能になります。 AWS アカウント内の他のリージョンの Amazon S3 バケットのデータイベントは記録されません。
すべてのリージョンの証跡を作成する場合は、Lambda 関数の事前定義されたテンプレートを選択すると、 AWS アカウントで現在使用されているすべての関数と、証跡の作成後に任意のリージョンで作成できる Lambda 関数のデータイベント口グ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して実行 AWS CLI) 、この選択により、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベント口グ記録が有効になります AWS 。他のリージョンで作成された Lambda 関数のデータイベントの口グ記録は有効になりません。
すべての関数のデータイベントを口グに記録すると、 AWS アカウント内の任意の IAM アイデンティティによって実行されたデータイベントアクティビティの口グ記録も可能になります。これは、そのアクティビティが別の AWS アカウントに属する関数で実行された場合でも同様です。

14. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。

15. [Advanced event selectors] で、データイベントを口グに記録する特定のリソースの式を作成します。事前定義済みの口グテンプレートを使用している場合は、このステップをスキップできます。

    a. 次のフィールドから選択します。

    - **readOnly** - readOnly は、 または の値と等しくなるように設定できますfalse。true読み取り専用データイベントは、Get* または Describe* イベントなどのリソースの状態を変更しないイベントです。書き込みイベントは、Put*、Delete*、または Write* イベントなどのリソース、属性、またはアーティファクトを追加、変更、または削除します。read および write イベントの両方を記録するには、readOnly セレクタを追加しないでください。
    - **eventName** - eventName は任意の演算子を使用できます。これを使用して、、、 など CloudTrail、 に口グ記録されたデータイベントを含めたり除外PutBucketPutItemしたりできますGetSnapshotBlock。

- **resources.ARN** - 任意の演算子を で使用できますがresources.ARN、等号または不等号を使用する場合、値はテンプレートで の値として指定したタイプの有効なリソースの ARN と完全に一致する必要がありますresources.type。

  以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

  > **Note**
  >
  > resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*

resources.type	resources.ARN
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*

resources.type	resources.ARN
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*

resources.type	resources.ARN
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_ID* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitewise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitewise: *region*:*account_ID* :timeseries/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*

resources.type	resources.ARN
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*

resources.type	resources.ARN
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemake r: *region*:*account_ID* :endpoint / *endpoint_name*

resources.type	resources.ARN
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*

resources.type	resources.ARN
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方が口グ記録されます。ストリームイベント を除外するには、 eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントを口グ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

データイベントリソースの ARN 形式の詳細については、AWS Identity and Access Management ユーザーガイドの「アクション、リソース、条件キー」を参照してください。

b. 各フィールドについて、[条件の追加] を選択して、必要な条件をすべて追加します。すべての条件に対して最大 500 個の指定値を設定できます。例えば、証跡に記録されたデータイベントから 2 つの S3 バケットのデータイベントを除外するには、 フィールドを resources.ARN に設定し、 の演算子を で始まらないように設定して、S3 バケット ARN に貼り付けるか、イベントをログに記録したくない S3 バケットを参照します。

2 番目の S3 バケットを追加するには、[条件の追加] を選択した後に上記の手順を繰り返し、ARN に貼り付けるか、別のバケットをブラウズします。

> **Note**
>
> 証跡上のすべてのセレクタに対して、最大 500 の値を設定できます。これには、`eventName` などのセレクタの複数の値の配列が含まれます。すべてのセレクタに単一の値がある場合、セレクタに最大 500 個の条件を追加できます。アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時に CloudTrail コンソールですべての関数を表示または選択することはできません。表示されていない場合でも、事前定義済みのセレクタテンプレートを使用してすべての関数をログ記録できます。特定の関数のデータイベントをログ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡の作成を終了し、 AWS CLI および put-event-selectors コマンドを使用して、特定の Lambda 関数のデータイベントログ記録を設定することもできます。詳細については、「を使用した証跡の管理 AWS CLI」を参照してください。

c. [+ Field] を選択し、必要に応じてフィールドを追加します。エラーを回避するには、フィールドに競合する値や重複する値を設定しないでください。例えば、あるセレクタで ARN を値と等しく指定せず、次に、別のセレクタで同じ値に等しくない ARN を指定します。

16. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。ステップ 12 からこのステップを繰り返し、データイベントタイプのアドバンストイベントセレクタを設定します。

17. 証跡で Insights イベントをログ CloudTrailに記録する場合は、Insights イベントを選択します。

    [Event type] で、[Insights events] を選択します。Insights イベントで、API コールレート、API エラーレート、または両方を選択します。[API コール率] の Insights イベントをログに記録するには、[Write] 管理イベントをログ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、[Read] または [Write] 管理イベントをログ記録している必要があります。

CloudTrail Insights は、異常なアクティビティの管理イベントを分析し、異常が検出されたときにイベントを記録します。デフォルトでは、証跡は Insights イベントを記録しません。Insights イベントの詳細については、「Insights イベントのログ記録」を参照してください。Insights イベントの記録には追加料金が適用されます。 CloudTrail 料金については、「AWS CloudTrail の料金」を参照してください。

Insights イベントは、証跡の詳細ページのストレージロケーションエリアで指定されているのと同じ S3 バケット/`CloudTrail-Insight`の という名前の別のフォルダに配信されます。CloudTrail は新しいプレフィックスを作成します。たとえば、現在の送信先 S3 バケットの名前が `S3bucketName/AWSLogs/CloudTrail/` の場合、新しいプレフィックスが付いた S3 バケットの名前は `S3bucketName/AWSLogs/CloudTrail-Insight/` になります。

18. ログに記録するイベントタイプの選択が終了したら、[Next] を選択します。
19. [Review and create] ページで選択内容を確認します。[Edit] を選択して、そのセクションに表示される証跡設定を変更します。証跡を作成する準備ができたら、[Create trail] を選択します。
20. 新しい証跡が [Trails] (証跡) ページに表示されます。組織の証跡がすべてのメンバーアカウントのすべてのリージョンで作成されるまでに、最大で 24 時間かかることがあります。[Trails (証跡)] ページでは、すべてのリージョンを対象に、アカウント内の証跡が表示されます。約 5 分で、 は組織で行われた AWS API コールを示すログファイル CloudTrail を発行します。ユーザーは、指定した Amazon S3 バケット内のログファイルを確認することができます。

> **Note**
>
> 証跡の作成後に証跡名を変更することはできません。ただし、証跡を削除して新しい証跡を作成することは可能です。

次のステップ

証跡を作成したら、証跡に戻って次の変更を加えることができます。

- 証跡の設定を編集することによって変更します。詳細については、「証跡の更新」を参照してください。
- 必要に応じて、メンバーアカウント内の特定のユーザーが組織のログファイルを読み取れるように Amazon S3 バケットを設定します。詳細については、「CloudTrail AWS アカウント間でのログファイルの共有」を参照してください。

- ログファイル CloudTrail を Logs CloudWatch に送信するように を設定します。詳細については、CloudWatch ログへのイベントの送信「」および「 の CloudWatch ログ項目」を参照してください組織の証跡の作成を準備する。

> **Note**
>
> 組織の証跡の CloudWatch ロググループを設定できるのは、管理アカウントのみです。

- テーブルを作成し、Amazon Athena でのクエリの実行に使用して、 AWS サービスアクティビティを分析します。詳細については、「Amazon Athena ユーザーガイド」の CloudTrail 「コンソールでの CloudTrail ログのテーブルの作成」を参照してください。 Amazon Athena
- 証跡にカスタムタグ (キーと値のペア) を追加する。
- 別の組織の証跡を作成するには、[Trails] (証跡) ページに戻り、[Add new trail] (新しい証跡の追加) を選択します。

> **Note**
>
> 証跡を設定する際には、別のアカウントに属している Amazon S3 バケットや SNS トピックを選択することもできます。ただし、イベント CloudTrail を Logs CloudWatch ロググループに配信する場合は、現在のアカウントに存在するロググループを選択する必要があります。

を使用して組織の証跡を作成する AWS Command Line Interface

AWS CLIを使用して組織の証跡を作成できます。 AWS CLI は、追加の機能とコマンドで定期的に更新されます。確実に成功させるには、開始 AWS CLI する前に、最新バージョンをインストールまたは更新していることを確認してください。

> **Note**
>
> このセクションの例は、組織の証跡の作成と更新に固有のものです。を使用して証跡を管理する例については、 AWS CLI を使用した証跡の管理 AWS CLI「」および「」を参照してください CloudWatch を使用してログモニタリングを設定します。 AWS CLI。を使用して組織の証跡を作成または更新するときは AWS CLI、十分なアクセス許可を持つ管理アカウントまたは委任管理者アカウントの AWS CLI プロファイルを使用する必要があります。組織の証跡を非組織の証跡に変換する場合は、組織の管理アカウントを使用する必要があります。

組織の証跡に使用する Amazon S3 バケットを十分なアクセス許可で設定する必要があります。

組織の証跡のログファイルを保存するために使用する Amazon S3 バケットを作成または更新する

組織の証跡のログファイルを受信するには、Amazon S3 バケットを指定する必要があります。このバケットには、組織のログファイルをバケットに入れる CloudTrail ことを に許可するポリシーが必要です。

以下は、組織の管理アカウントが所有する *myOrganizationBucket*という名前の Amazon S3 バケットのポリシーの例です。*myOrganizationBucket*、*#### ##managementAccountIDtrailName*、および *o-organizationID* を組織の値に置き換えます。

このバケットには、3 つのステートメントがあります。

- 最初のステートメントでは CloudTrail 、 が Amazon S3 バケットで Amazon S3 `GetBucketAcl`アクションを呼び出すことができます。
- 2 番目のステートメントでは、証跡が組織の証跡からそのアカウントの証跡にのみ変更された場合に口グに記録することを許可します。
- 3 番目のステートメントでは、組織証跡を口グに記録することが可能になります。

ポリシー例には、Amazon S3 バケットポリシーの `aws:SourceArn` 条件キーが含まれています。IAM グローバル条件キーは、 が特定の証跡または証跡に対してのみ S3 バケットに CloudTrail 書き込むようにする`aws:SourceArn`のに役立ちます。組織の証跡の場合、`aws:SourceArn` の値は管理アカウントで保持され、管理アカウント ID を使用する証跡の ARN である必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
```

```
                }
            }
        }
    ]
}
```

このポリシー例では、メンバーアカウントのユーザーが組織用に作成されたログファイルにアクセスすることを許可していません。デフォルトでは、組織のログファイルは管理アカウントにのみアクセスできます。メンバーアカウントの IAM ユーザーに対して Amazon S3 バケットへの読み取りアクセスを許可する方法については、「CloudTrail AWS アカウント間でのログファイルの共有」を参照してください。

で信頼されたサービス CloudTrail として を有効にする AWS Organizations

組織の証跡を作成する前に、まず Organizations のすべての機能を有効化する必要があります。詳細については、「自分の組織のすべての機能を有効化する」を参照してください。または、管理アカウントで十分なアクセス許可を持つプロファイルを使用して、次のコマンドを実行します。

```
aws organizations enable-all-features
```

すべての機能を有効にしたら、信頼できるサービス CloudTrail として信頼するように Organizations を設定する必要があります。

AWS Organizations と の間に信頼されたサービス関係を作成するには CloudTrail、ターミナルまたはコマンドラインを開き、管理アカウントのプロファイルを使用します。以下の例のように、`aws organizations enable-aws-service-access` コマンドを実行します。

```
aws organizations enable-aws-service-access --service-principal
 cloudtrail.amazonaws.com
```

「create-trail の使用」

すべてのリージョンに適用される組織の証跡の作成

すべてのリージョンに適用される組織の証跡を作成するには、`--is-organization-trail` と `--is-multi-region-trail` のオプションを追加します。

> **Note**
>
> を使用して組織の証跡を作成する場合は AWS CLI、十分なアクセス許可を持つ管理アカウントまたは委任された管理者アカウントの AWS CLI プロファイルを使用する必要があります。

次の例では、すべてのリージョンから *my-bucket* という既存のバケットにログを配信する組織の証跡を作成します。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail --is-multi-region-trail
```

証跡がすべてのリージョンに存在することを確認するために、出力の IsOrganizationTrail および IsMultiRegionTrail パラメータは両方とも true に設定されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> 証跡のログ記録を開始するには start-logging コマンドを実行します。詳細については、「証跡のログ記録の停止と開始」を参照してください。

単一リージョンの証跡としての組織の証跡の作成

次のコマンドは、単一リージョンの証跡とも呼ばれる AWS リージョン単一の のイベントのみをログに記録する組織の証跡を作成します。イベントがログに記録される AWS リージョンは、 の設定プロファイルで指定されたリージョンです AWS CLI。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-
organization-trail
```

詳細については、「命名の要件」を参照してください。

サンプル出力:

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

デフォルトでは、create-trail コマンドはログファイルの検証を有効にしない単一リージョンの証跡を作成します。

> **Note**
>
> 証跡のログ記録を開始するには start-logging コマンドを実行します。

update-trail を実行して組織証跡を更新する

update-trail コマンドを実行して、組織の証跡の設定を変更したり、単一の AWS アカウントの既存の証跡を組織全体に適用したりできます。update-trail コマンドは、証跡が作成されたリージョンからしか実行できないことに注意してください。

> **Note**
>
> AWS CLI またはいずれかの AWS SDKs を使用して証跡を更新する場合は、証跡のバケットポリシーが であることを確認してください up-to-date。詳細については、「を使用して組織の証跡を作成する AWS Command Line Interface」を参照してください。
> で組織の証跡を更新する場合は AWS CLI、十分なアクセス許可を持つ管理アカウントまたは委任された管理者アカウントのプロファイルを使用する必要があります AWS CLI 。組織の証跡を非組織の証跡に変換する場合は、組織の管理アカウントを使用する必要があります。管理アカウントはすべての組織リソースの所有者であるためです。

CloudTrail は、リソースの検証が失敗した場合でも、メンバーアカウントの組織の証跡を更新します。検証の失敗の例は次のとおりです。

- Amazon S3 バケットポリシーが正しくない
- Amazon SNS トピックポリシーが正しくない
- Logs CloudWatch ロググループに配信できない
- KMS キーを使用して暗号化するアクセス許可が不十分

アクセス CloudTrail 許可を持つメンバーアカウントは、 CloudTrail コンソールで証跡の詳細ページを表示するか、 コマンドを実行する AWS CLI get-trail-statusことで、組織の証跡の検証に失敗したことを確認できます。

既存の証跡を組織に適用する

既存の証跡を変更して、単一の AWS アカウントではなく組織にも適用されるようにするには、次の例に示すように、 `--is-organization-trail`オプションを追加します。

> **Note**
> 管理アカウントを使用して、既存の非組織の証跡を組織の証跡に変更します。

```
aws cloudtrail update-trail --name my-trail --is-organization-trail
```

証跡が組織に適用されるようになったことを確認するために、出力の `IsOrganizationTrail` パラメータは `true` の値を持ちます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

前述の例では、証跡はすべてのリージョンに適用されるように構成されています ("IsMultiRegionTrail": true)。単一のリージョンにのみ適用される証跡は、出力には "IsMultiRegionTrail": false と表示されます。

1 つのリージョンに適用される組織の証跡を変換してすべてのリージョンに適用する

既存の組織証跡を変更してすべてのリージョンに適用されるようにするには、次の例に示すような --is-multi-region-trail オプションを追加します。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

証跡がすべてのリージョンに適用されるようになったことを確認するために、出力の IsMultiRegionTrail パラメータは true の値を持ちます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "my-bucket"
}
```

トラブルシューティング

このセクションでは、組織の証跡に関する問題のトラブルシューティング方法について説明します。

トピック

- CloudTrail はイベントを配信していません
- CloudTrail は、組織内のメンバーアカウントの Amazon SNS 通知を送信していません

CloudTrail はイベントを配信していません

CloudTrail が CloudTrail ログファイルを Amazon S3 バケットに配信していない場合

S3 バケットに問題があるかどうかを確認します。

- CloudTrail コンソールから、証跡の詳細ページを確認します。S3 バケットに問題がある場合、詳細ページには S3 バケットへの配信が失敗したという警告が表示されます。

- から AWS CLI、 get-trail-status コマンドを実行します。障害が発生した場合、コマンド出力には LatestDeliveryErrorフィールドが含まれます。このフィールドには、指定されたバケットにログファイルを配信しようとしたときに発生した Amazon S3 エラー CloudTrail が表示されます。このエラーは、送信先 S3 バケットに問題がある場合にのみ発生し、タイムアウトするリクエストでは発生しません。この問題を解決するには、 がバケットに CloudTrail 書き込めるようにバケットポリシーを修正するか、新しいバケットを作成してから、 update-trail を呼び出して新しいバケットを指定します。組織バケットポリシーの詳細については、「組織の証跡 のログファイルを保存するために使用する Amazon S3 バケットを作成または更新する」を参照してください。

CloudTrail がログを CloudWatch ログに配信していない場合

CloudWatch Logs ロールポリシーの設定に問題があるかどうかを確認します。

- CloudTrail コンソールから、証跡の詳細ページを確認します。 CloudWatch ログに問題がある場合、詳細ページには CloudWatch ログの配信が失敗したことを示す警告が表示されます。
- から AWS CLI、 get-trail-status コマンドを実行します。障害が発生した場合、コマンド出力には LatestCloudWatchLogsDeliveryErrorフィールドが含まれます。このフィールドには、 CloudWatch ログを ログに配信しようとしたときに CloudTrail 発生した CloudWatch ログエラーが表示されます。この問題を解決するには、 CloudWatch ログロールポリシーを修正します。 CloudWatch Logs ロールポリシーの詳細については、「」を参照してください CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント。

組織証跡のメンバーアカウントのアクティビティが表示されない場合

組織証跡のメンバーアカウントのアクティビティが表示されない場合は、以下を確認してください。

- 証跡のホームリージョンをチェックして、それがオプトインリージョンかどうかを確認します。

  ほとんどの AWS リージョン は でデフォルトで有効になっていますが AWS アカウント、特定のリージョン (オプトインリージョン とも呼ばれます) を手動で有効にする必要があります。デフォルトで有効になっているリージョンについては、「 AWS Account Management リファレンスガイド」の「リージョンを有効または無効にする前の考慮事項」を参照してください。が CloudTrail サポートするリージョンのリストについては、「」を参照してくださいCloudTrail サポートされているリージョン。

  組織の証跡がマルチリージョンで、ホームリージョンがオプトインリージョンの場合、 AWS リージョン マルチリージョン証跡が作成された をオプトインしない限り、メンバーアカウントは組織の証跡にアクティビティを送信しません。例えば、マルチリージョンの証跡を作成し、証跡の

ホームリージョンとして欧州 (スペイン) リージョンを選択した場合、そのアカウントの欧州 (スペイン) リージョンを有効にしたメンバーアカウントのみが、そのアカウントのアクティビティを組織の証跡に送信します。この問題を解決するには、組織内の各メンバーアカウントでオプトインリージョンを有効にします。オプトインリージョンの有効化については、「 AWS Account Management リファレンスガイド」の「組織内のリージョンの有効化または無効化」を参照してください。

- 組織リソースベースのポリシーが CloudTrail サービスにリンクされたロールポリシーと競合していないか確認する

  CloudTrail は、 という名前のサービスにリンクされたロール`AWSServiceRoleForCloudTrail`を使用して組織の証跡をサポートします。このサービスにリンクされたロールにより、 CloudTrail は などの組織リソースに対してアクションを実行できます`organizations:DescribeOrganization`。組織のリソースベースのポリシーが、サービスにリンクされたロールポリシーで許可されているアクションを拒否 CloudTrail した場合、 は、サービスにリンクされたロールポリシーで許可されている場合でも、アクションを実行できません。この問題を解決するには、サービスにリンクされたロールポリシーで許可されているアクションを拒否しないように、組織のリソースベースのポリシーを修正します。

CloudTrail は、組織内のメンバーアカウントの Amazon SNS 通知を送信していません

AWS Organizations 組織の証跡を持つメンバーアカウントが Amazon SNS 通知を送信していない場合、SNS トピックポリシーの設定に問題がある可能性があります。 は、リソースの検証に失敗した場合でも、メンバーアカウントに組織の証跡 CloudTrail を作成します。例えば、組織の証跡の SNS トピックには、すべてのメンバーアカウント IDsが含まれていません。SNS トピックポリシーが正しくない場合、認証エラーが発生します。

証跡の SNS トピックポリシーで認証に失敗したかどうかを確認するには：

- CloudTrail コンソールから、証跡の詳細ページを確認します。認証に失敗した場合、詳細ページには警告が表示され`SNS authorization failed`、SNS トピックポリシーの修正が示されます。
- から AWS CLI、 get-trail-status コマンドを実行します。認証に失敗した場合、コマンド出力にはの値が設定された `LastNotificationError`フィールドが含まれます`AuthorizationError`。この問題を解決するには、Amazon SNS トピックポリシーを修正します。Amazon SNS トピックポリシーの詳細については、「」を参照してくださいの Amazon SNS トピックポリシー CloudTrail。

SNS トピックとそのサブスクライブの詳細については、Amazon Simple Notification Service デベロッパーガイドのAmazon SNS の開始方法」を参照してください。

CloudTrail トレイルのインサイトイベントの表示

CloudTrail トレイルでインサイトを有効にすると、 CloudTrailコンソールまたはを使用して、最大 90 日間のインサイトイベントを表示できます AWS CLI。このセクションでは、Insights イベントのファイルを表示、参照、およびダウンロードする方法について説明します。`LookupEvents`API CloudTrail を使用してイベントから情報を取得する方法については、AWS CloudTrail API リファレンスをご覧ください。 CloudTrail Insights の詳細については、Insights イベントのログ記録このガイドのを参照してください。

証跡の作成と管理の詳細については、「証跡の作成」および「 CloudTrail ログファイルの取得と表示」を参照してください。

> **Note**
>
> API 呼び出し量に関する Insights イベントを記録するには、証跡が `write` 管理イベントを記録している必要があります。API エラー率に関する Insights イベントを記録するには、証跡が `read` または `write` 管理イベントを記録している必要があります。

トピック

- トレイルの CloudTrail Insights イベントをコンソールに表示する CloudTrail
- CloudTrail でトレイルのインサイトイベントを表示する AWS CLI

トレイルの CloudTrail Insights イベントをコンソールに表示する CloudTrail

トレイルで CloudTrail Insights イベントを有効にした後、異常な API CloudTrail またはエラー率のアクティビティを検出すると、Insights CloudTrail イベントが生成され、の [ダッシュボード] ページと [Insights] ページに表示されます AWS Management Console。コンソールで Insights イベントを表示して、異常なアクティビティのトラブルシューティングを行うことができます。直近 90 日間の Insights イベントがコンソールに表示されます。 AWS CloudTrail コンソールを使用して Insights イベントをダウンロードすることもできます。 AWS SDK またはを使用して、プログラムでイベントを検索できます。 AWS Command Line Interface CloudTrail Insights イベントの詳細については、Insights イベントのログ記録本ガイドのを参照してください。

> **Note**
>
> API 呼び出し量に関する Insights イベントを記録するには、証跡が `write` 管理イベントを記録している必要があります。API エラー率に関する Insights イベントを記録するには、証跡が `read` または `write` 管理イベントを記録している必要があります。

Insights イベントが記録されると、それらのイベントは [インサイト] ページに 90 日間表示されます。[インサイト] ページからイベントを手動で削除することはできません。 CloudTrail Insights を有効にするにはトレイルを作成する必要があるため、トレイル設定で設定した S3 バケットに保存されている限り、トレイルに記録された Insights イベントを表示できます。

トレイルログを監視し、Amazon CloudWatch Logs で特定の Insights イベントアクティビティが発生したときに通知を受けることができます。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

Insights イベントを表示するには

CloudTrail コンソールに Insights イベントを表示するには、トレイルで Insights イベントを有効にする必要があります。異常なアクティビティが検出された場合、最初の Insights イベントが配信されるまで最大 36 時間かかります。 CloudTrail

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/home/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインで、[ダッシュボード] を選択して最新の Insights イベント 5 つを表示するか、[Insights] を選択して過去 90 日間にアカウントにログインしたすべての Insights イベントを表示します。

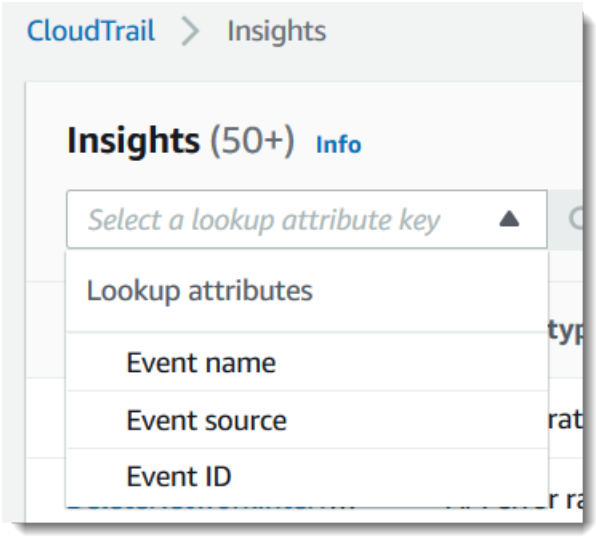
   [Insights] ページでは、Insights イベント API ソース、イベント名、イベント ID などの条件で Insights イベントをフィルタリングし、表示されるイベントを特定の時間範囲内に発生したイベントに制限できます。Insights イベントのフィルタリングの詳細については、「Insights イベントのフィルタリング」を参照してください。

目次

- グラフの期間設定の変更
- Insights イベントのダウンロード

Insights イベントのフィルタリング

[インサイト] におけるイベントのデフォルト表示では、イベントが日付の逆順に表示されます。イベント開始時刻でソートされた最新の Insights イベントが一番上に表示されます。次のリストでは、使用可能な属性について説明します。最初の 3 つの属性 Event name、Event source、Event ID でフィルタリングできます。



イベント名

イベントの名前。通常は異常なレベルのアクティビティが記録された AWS API。

Insight タイプ

CloudTrail Insights イベントのタイプ。API コール率または API エラー率のいずれかです。[API コール率] の Insight タイプは、ベースライン API コール量に対して 1 分ごとに集計された書き込み専用の管理 API コールを分析します。[API エラー率] は、エラーコードを発生させた管理 API 呼び出しを分析します。API 呼び出しに失敗すると、エラーが表示されます。

[イベントソース]

AWS リクエストが行われたサービス (`iam.amazonaws.com`やなど) `s3.amazonaws.com`。[Event source] フィルタを選択すると、イベントソースのリストをスクロールできます。

イベント ID

Insights イベントの ID。イベント ID は [Insights] ページのテーブルには表示されませんが、Insights イベントをフィルタリングできる属性です。Insights イベントを生成するために分析される管理イベントのイベント ID は、Insights イベントのイベント ID とは異なります。

イベント開始時間

Insights イベントの開始時刻。異常なアクティビティが記録された最初の分として測定されます。この属性は、[Insights] テーブルに表示されますが、コンソールでイベント開始時刻をフィルタリングすることはできません。

ベースライン平均

API コールレートアクティビティまたはエラーレートアクティビティの通常のパターン。ベースライン平均は、Insights イベントの開始前の 7 日間にわたって計算されます。ベースライン期間 (API CloudTrail での正常なアクティビティを分析する期間) の値は約 7 日間ですが、ベースライン期間を整数 1 CloudTrail 日に四捨五入するため、正確なベースライン期間は異なる場合があります。

インサイト平均

Insights イベントをトリガーした API コールの平均数、または API コールで返された特定エラーの平均数。 CloudTrail 開始イベントのインサイト平均は、インサイトイベントをトリガーした発生率です。通常、これは異常なアクティビティの最初の 1 分です。終了イベントのインサイト平均は、開始 Insights イベントと終了 Insights イベントの間の異常なアクティビティ期間の発生率です。

レートの変化

測定されたベースライン平均とインサイト平均の値 (割合) の差分。例えば、発生する `AccessDenied` エラーのベースライン平均が 1.0 で、インサイト平均が 3.0 の場合、レートの変化率は 300% です。インサイト平均の割合変化がベースライン平均を超えると、値の横に上矢印が表示されます。アクティビティがベースライン平均を下回り Insights イベントがログに記録された場合、[Rate change] (レートの変化) はパーセンテージの横に下向きの矢印を表示します。アクティビティがベースライン平均を下回っているために Insights イベントが記録された場合、レート変更パーセンテージの横に下向き矢印を示します。

選択した属性または時間に記録されたイベントがない場合、結果リストは空です。時間範囲に加えて、1 つの属性フィルタのみを適用できます。別の属性フィルタを選択した場合は、指定した時間範囲が保持されます。

次のステップでは、属性でフィルタリングする方法について説明します。

属性でフィルタリングするには

1. 属性で結果をフィルタリングするには、ドロップダウンメニューからルックアップ属性を選択し、[Enter lookup value] ボックスに値を入力するか、または選択します。
2. 属性フィルタを削除するには、属性フィルタボックスの右側にある [X] を選択します。

次のステップでは、開始と終了の日時でフィルタリングする方法について説明します。

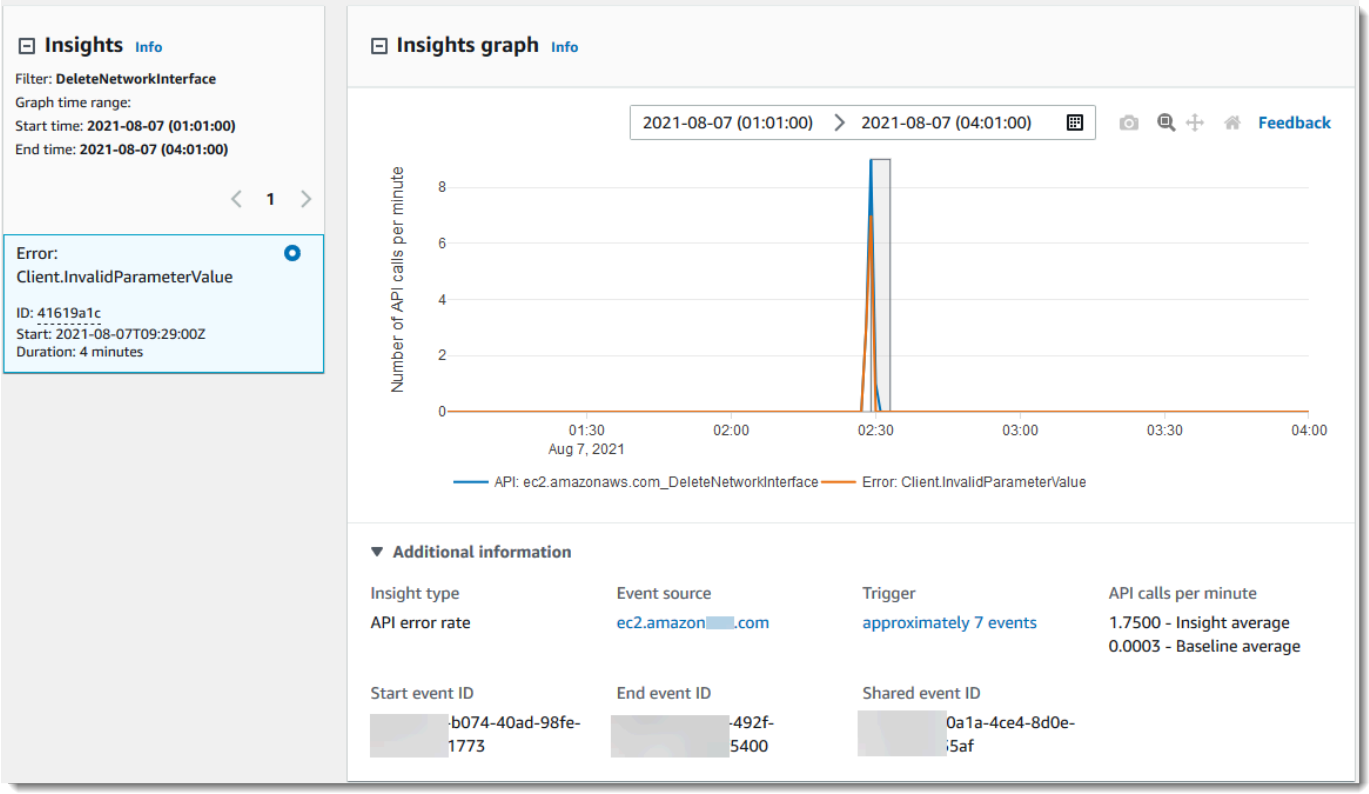
開始と終了の日時ででフィルタリングするには

1. 表示するイベントの時間範囲を絞り込むには、テーブル上部のタイムスパンバーで期間を選択します。プリセットされた時間範囲は、30 分、1 時間、3 時間、または 12 時間です。カスタムの時間範囲を指定するには、[Custom] を選択します。
2. 次のいずれかのテーブルを選択します。
   - [Absolute] - 特定の時間を選択できます。次のステップに進みます。
   - [Relative to value] - デフォルトで選択されています。Insights イベントの開始時刻を基準とした期間を選択できます。ステップ 4 に進みます。
3. [Absolute] の時間範囲を設定するには、次の操作を行います。
   a. [Absolute] タブで、時間範囲を開始する日を選択します。選択した日の開始時刻を入力します。手動で日付を入力するには、`yyyy/mm/dd` の形式で日付を手動で入力します。開始時刻と終了時刻は 24 時間制で、値は `hh:mm:ss` の形式である必要があります。例えば、午後 6 時 30 分の開始時刻を指定するには、**`18:30:00`** を入力します。
   b. カレンダーの範囲で終了日を選択するか、カレンダーの下にある終了日時を指定します。[適用] を選択します。
4. [Relative to selected event] の時間範囲を設定するには、次の操作を行います。
   a. Insights イベントの開始時刻を基準としたプリセット期間を選択します。プリセット値は、分、時間、日数、週数で使用できます。最大相対期間は 12 週間です。
   b. 必要に応じて、プリセットの下のボックスでプリセット値をカスタマイズします。[Clear] を選択して、必要に応じて変更をリセットします。相対時間を設定したら、[適用] を選択します。
5. [終了] で、日付を選択し、時間範囲の終了時刻を指定します。[適用] を選択します。

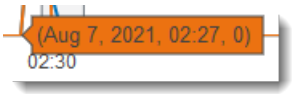
6. 時間範囲フィルタを削除するには、[時間範囲] ボックスの右側にあるカレンダーアイコンを選択し、[削除] を選択します。

Insights イベントの詳細の表示

1. 結果リストで Insights イベントを選択して、詳細を表示します。Insights イベントの詳細ページには、異常なアクティビティタイムラインのグラフが表示されます。



2. 強調表示されたバンドにマウスカーソルを合わせると、グラフ内の各 Insights イベントの開始時刻と継続期間が表示されます。



では、次の情報が示されています。追加情報グラフの面積:

- Insights タイプ。これは API コールレートまたは API エラーレートです。
- [トリガー] (トリガー) これは、[Cloudtrail イベント] タブが表示されます。このタブには、異常なアクティビティが発生したと判断するために分析された管理イベントが一覧表示されます。
- [1 分あたりの API 呼び出し数]

- Baseline average (ベースライン平均) - アカウントの特定のリージョンで、過去約 7 日内に測定された、Insights イベント がログに記録された API での 1 分あたりの標準的な発生率。
- Insights average (インサイト平均) - Insights イベントをトリガーしたこの API での 1 分あたりの発生率。 CloudTrail 開始イベントのインサイト平均は、インサイトイベントをトリガーした API の 1 分あたりのコール数またはエラー率です。通常、これは異常なアクティビティの最初の 1 分です。終了イベントのインサイト平均は、開始 Insights イベントと終了 Insights イベントの間の異常なアクティビティの期間における 1 分あたりの API コールまたはエラーの割合です。

- イベントソース 異常な数の API AWS 呼び出しまたはエラーが記録されたサービスエンドポイント。前の画像では、ソースは `ec2.amazonaws.com` で、これは Amazon EC2 のサービスエンドポイントです。
- イベント ID
  - Start event ID (開始イベント ID) - 異常なアクティビティの開始時に記録されたInsights イベントの ID。
  - End event ID (終了イベント ID) - 異常なアクティビティの終了時に記録された Insights イベントの ID。
  - 共有イベント ID-Insights イベントでは、共有イベント ID は Insights CloudTrail イベントの開始ペアと終了ペアを一意に識別するためにインサイトによって生成される GUID です。共有イベント ID は、Insights イベントの開始から終了まで共有され、両方のイベントの相関関係を作成して異常なアクティビティを一意的に識別するのに役立ちます。

3. [Attributions] (属性) タブを選択して、ユーザーID、ユーザーエージェント、API コールレート Insight イベント、異常なベースラインアクティビティに相関するエラーコードに関する情報を表示します。最大 5 つのユーザーアイデンティティ、5 つのユーザーエージェント、5 つのエラーコードが、アクティビティ数の平均でソートされ、高いものから低いものへの降順で [属性] タブのテーブルに表示されます。[属性] タブの詳細については、このガイドの「[Attributions] (属性) タブ」および「CloudTrail `insightDetails`インサイト要素」を参照してください。
4. [CloudTrail イベント] タブには、 CloudTrail異常なアクティビティが発生したかどうかが分析された関連イベントが表示されます。デフォルトで、フィルターはすでに Insights イベント名に適用されています。これは関連する API の名前でもあります。CloudTrail イベントタブには、Insights イベントの開始時間 (1 分を引いた時間) から終了時間 (さらに 1 分) までの間に発生した、対象 API CloudTrail に関連する管理イベントが表示されます。

グラフ内の他の Insights イベントを選択すると、CloudTrail イベントテーブルに表示されるイベントが変わります。これらのイベントは、より深い分析を実行して、Insights イベントの考えられる原因と、異常な API アクティビティの理由を特定するのに役立ちます。

関連する API CloudTrail のイベントだけでなく、Insights イベントの期間中に記録されたすべてのイベントを表示するには、フィルターをオフにします。

5. [Insights event record] タブを選択して、Insights の開始イベントと終了イベントを JSON 形式で表示します。
6. リンクされた [イベントソース] を選択すると、そのイベントソースによってフィルタリングされた [インサイト] ページに戻ります。

グラフのズーム、パン、ダウンロード

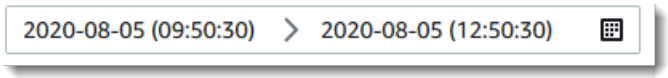
右上隅にあるツールバーを使用して、Insights イベントの詳細ページでグラフの軸をズーム、パン、リセットできます。

グラフツールバーのコマンドボタンは、次の操作を行います (左から右の順)。

- プロットを PNG としてダウンロード - 詳細ページに表示されているグラフ画像をダウンロードし、PNG 形式で保存します。
- ズーム - ドラッグしてグラフ上の領域を選択し、拡大して詳細を表示します。
- パン - グラフをシフトして、隣接する日付または時刻を表示します。
- 軸のリセット - グラフ軸を元の軸に戻し、ズームとパンの設定をクリアします。

グラフの期間設定の変更

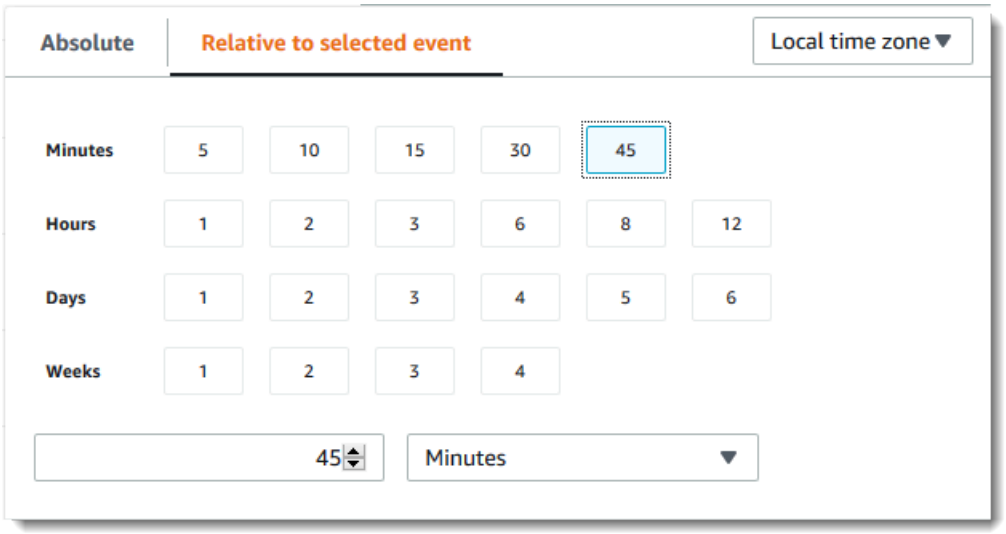
グラフの右上隅にある設定を選択すると、グラフに表示されるタイムスパン (X 軸上に示される選択したイベントの継続時間) を変更できます。



グラフに表示されるデフォルトの期間は、選択した Insights イベントの期間によって異なります。

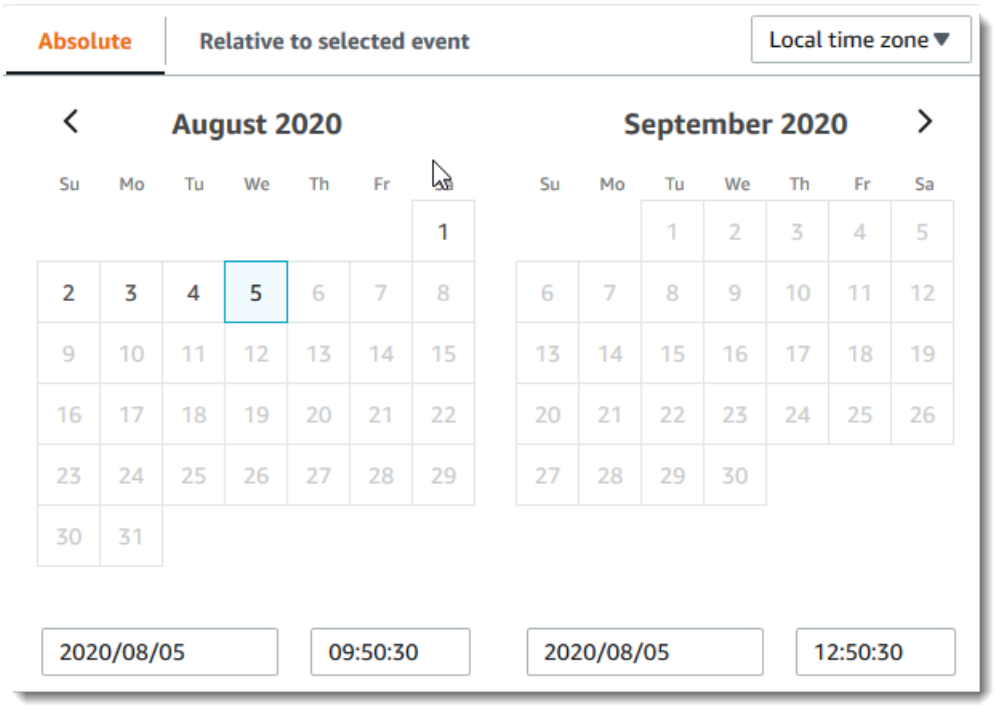
Insights イベントの期間	デフォルトの期間
4 時間未満	3h (3 時間)
4 ~ 12 時間	12h(12 時間)
12 ~ 24 時間	1d (1 日)
24 ~ 72 時間	3d (3 日)
72 時間超	1w (1 週間)

プリセットは、5 分、30 分、1 時間、3 時間、12 時間、または [Custom] から選択できます。次の画像は、選択したイベントの相対期間 ([Custom] で選択できます) を示しています。相対期間は、Insights イベントの詳細ページに表示される、選択した Insights イベントの開始と終了が収まるおおよその期間です。



選択したプリセットをカスタマイズするには、プリセットの下のボックスに数値と時間単位を指定します。

正確な日付と時刻の範囲を指定するには、[絶対] タブを選択します。日付と時刻の絶対範囲を設定する場合は、開始時刻と終了時刻が必要です。時間を設定する方法の詳細については、このトピックのthe section called “Insights イベントのフィルタリング” を参照してください。



Insights イベントのダウンロード

記録された Insights イベント履歴は、CSV または JSON 形式のファイルとしてダウンロードできます。ダウンロードするファイルのサイズを減らすには、フィルタと時間範囲を使用します。

> **Note**
>
> CloudTrail イベント履歴ファイルは、個々のユーザーが設定できる情報 (リソース名など) を含むデータファイルです。一部のデータは、このデータ (CSV インジェクション) の読み取りと分析に使用されるプログラムでコマンドとして解釈される可能性があります。たとえば、 CloudTrail イベントを CSV にエクスポートしてスプレッドシートプログラムにインポートすると、そのプログラムはセキュリティ上の問題について警告することがあります。セキュリティ上のベストプラクティスとして、ダウンロードされたイベント履歴ファイルからリンクまたはマクロを無効にします。

1. ダウンロードするイベントのフィルタと時間範囲を指定します。たとえば、イベント名 `StartInstances` を指定し、過去 3 日間のアクティビティの時間範囲を指定できます。
2. [Download events] (イベントのダウンロード) 選択し、その後 [Download CSV] (CSV のダウンロード) または [Download JSON] (JSON のダウンロード) を選択します。ファイルを保存する場所を選択するプロンプトが表示されます。

> **Note**
>
> ダウンロードが完了するまで時間がかかる場合があります。迅速な結果を得るには、より特定のフィルタまたは短い時間範囲を使って結果を絞り込んでから、ダウンロードプロセスを開始します。

3. ダウンロードが完了したら、ファイルを開いて、指定したイベントを表示します。
4. ダウンロードをキャンセルする場合は、[ダウンロードのキャンセル] を選択します。ダウンロードが完了する前にキャンセルした場合、ローカルコンピューター上の CSV ファイルまたは JSON ファイルにイベントの一部しか含まれていない可能性があります。

CloudTrail でトレイルのインサイトイベントを表示する AWS CLI

コマンドを実行すると、過去 90 CloudTrail 日間のインサイトイベントを検索できます。aws cloudtrail lookup-eventslookup-events コマンドには以下のオプションがあります。

- `--end-time`
- `--event-category`
- `--max-results`
- `--start-time`
- `--lookup-attributes`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

の使用に関する一般的な情報については AWS Command Line Interface、『AWS Command Line Interface ユーザーガイド』を参照してください。

目次

前提条件

- AWS CLI コマンドを実行するには、をインストールする必要があります AWS CLI。詳細については、「はじめに」を参照してください AWS CLI。
- AWS CLI バージョンが 1.6.6 以降であることを確認してください。CLI のバージョンを確認するには、コマンドラインで aws --version を実行します。
- AWS CLI セッションのアカウント、リージョン、デフォルト出力形式を設定するには、コマンドを使用します。aws configure詳細については、「AWS コマンドラインインターフェイスの設定」を参照してください。
- API 呼び出し量に関する Insights イベントを記録するには、証跡が `write` 管理イベントを記録している必要があります。API エラー率に関する Insights イベントを記録するには、証跡が `read` または `write` 管理イベントを記録している必要があります。

> **Note**
>
> CloudTrail AWS CLI コマンドでは大文字と小文字が区別されます。

コマンドラインのヘルプを取得する

`lookup-events` のコマンドライン ヘルプを表示するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events help
```

Insights イベントを参照する

最新 10 件の Insights イベントを表示するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --event-category insight
```

返されるイベントは、次の例のようになります。

```
{
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
    "Events": [
        {
            "eventVersion": "1.07",
            "eventTime": "2019-10-15T21:13:00Z",
            "awsRegion": "us-east-1",
            "eventID": "EXAMPLE-9b6f-45f8-bc6b-9b41c052ebc7",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
            "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
```

```
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                        "average": 0.2
                      },
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                        "average": 0.2
                      }
                    ],
                    "baseline": [
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "userAgent",
                    "insight": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "errorCode",
                    "insight": [
                      {
                        "value": "null",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "null",
```

```
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      },
      {
          "eventVersion": "1.07",
          "eventTime": "2019-10-15T21:14:00Z",
          "awsRegion": "us-east-1",
          "eventID": "EXAMPLEc-9eac-4af6-8e07-26a5ae8786a5",
          "eventType": "AwsCloudTrailInsight",
          "recipientAccountId": "123456789012",
          "sharedEventID": "EXAMPLE8-02b2-4e93-9aab-08ed47ea5fd3",
          "insightDetails": {
          "state": "End",
          "eventSource": "autoscaling.amazonaws.com",
          "eventName": "CompleteLifecycleAction",
          "insightType": "ApiCallRateInsight",
          "insightContext": {
            "statistics": {
              "baseline": {
                "average": 0.0000882145
              },
              "insight": {
                "average": 0.6
              },
              "insightDuration": 5,
              "baselineDuration": 11336
            },
            "attributions": [
              {
                "attribute": "userIdentityArn",
                "insight": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.2
                  },
                  {
```

```
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                        "average": 0.2
                      },
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                        "average": 0.2
                      }
                    ],
                    "baseline": [
                      {
                        "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "userAgent",
                    "insight": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "codedeploy.amazonaws.com",
                        "average": 0.0000882145
                      }
                    ]
                  },
                  {
                    "attribute": "errorCode",
                    "insight": [
                      {
                        "value": "null",
                        "average": 0.6
                      }
                    ],
                    "baseline": [
                      {
                        "value": "null",
```

```
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        },
          "eventCategory": "Insight"
      }
  ]
}
```

出力内の参照関連フィールドの説明については、このトピックの「参照の出力フィールド」を参照してください。Insights イベント内のフィールドの説明については、「CloudTrail レコードの内容」を参照してください。

返す Insights イベント数を指定する

返されるイベントの数を指定するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

<integer> のデフォルト値 (指定されていない場合) は 10 です。有効な値は 1 から 50 です。次の例では、1 件の結果が返されています。

```
aws cloudtrail lookup-events --event-category insight --max-results 1
```

時間範囲により Insights イベントを参照する

Insights イベントは過去 90 日間の記録から参照できます。時間範囲を指定するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --event-category insight --start-time <timestamp> --end-
time <timestamp>
```

`--start-time` *<timestamp>* を UTC で指定すると、指定された時刻かその後に発生した Insights イベントのみが返されます。指定された開始時刻が指定された終了時刻よりも後である場合は、エラーが返されます。

`--end-time` *<timestamp>* を UTC で指定すると、指定された時刻かその前に発生した Insights イベントのみが返されます。指定された終了時刻が指定された開始時刻よりも前である場合は、エラーが返されます。

デフォルトの開始時刻は、過去 90 日間のうち、データが利用できる最も早い日付です。デフォルトの終了時刻は、現在の時刻に最も近いイベント発生時刻です。

すべてのタイムスタンプは UTC で表示されます。

属性により Insights イベントを参照する

属性でフィルタリングするには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=<attribute>,AttributeValue=<string>
```

各 lookup-events コマンドに対し、属性キーと値のペアを 1 つだけ指定できます。以下に、`AttributeKey` の有効な Insights イベント値を示します。値名では大文字と小文字が区別されます。

- `EventId`
- `EventName`
- `EventSource`

の最大長は 2000 `AttributeValue` 文字です。次の文字 ('_', ' ', , \\n ') は 2000 文字の制限に対して 2 文字としてカウントされます。

属性参照の例

次のコマンド例では、`EventName` の値が `PutRule` である Insights イベントが返されます。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

次のコマンド例では、`EventId` の値が `b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002` である Insights イベントが返されます。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventId, AttributeValue=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

次のコマンド例では、EventSource の値が iam.amazonaws.com である Insights イベントが返されます。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventSource, AttributeValue=iam.amazonaws.com
```

次の結果ページを指定する

lookup-events コマンドの次の結果ページを取得するには、次のコマンドを入力します。

```
aws cloudtrail lookup-events --event-category insight <same parameters as previous
 command> --next-token=<token>
```

このコマンドでは、*<token>* の値は、前のコマンドの出力の最初のフィールドから取得されます。

コマンド内で --next-token を使用する場合は、前のコマンドと同じパラメータを使用する必要があります。たとえば、次のコマンドを実行したとします。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName, AttributeValue=PutRule
```

次の結果ページを取得する場合、コマンドは次のようになります。

```
aws cloudtrail lookup-events --event-category insight --lookup-attributes
 AttributeKey=EventName,AttributeValue=PutRule --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

JSON 入力をファイルから取得する

AWS 一部のサービスでは--cli-input-json、--generate-cli-skeletonと 2 つのパラメータを使用して JSON テンプレートを生成できます。このパラメータを変更して、--cli-input-jsonパラメータへの入力として使用できます。 AWS CLI このセクションでは、これらのパラメータを aws cloudtrail lookup-events で使用する方法について説明します。詳細については、「AWS CLI スケルトンと入力ファイル」を参照してください。

JSON 入力をファイルから取得して Insights イベントを参照するには

1. 次の例のように、lookup-events の出力をファイルにリダイレクトして、--generate-cli-skeleton で使用するための入力テンプレートを作成します。

```
aws cloudtrail lookup-events --event-category insight --generate-cli-skeleton >
 LookupEvents.txt
```

生成されたテンプレートファイル (LookupEventsこの場合は.txt) は以下のようになります。

```
{
    "LookupAttributes": [
        {
            "AttributeKey": "",
            "AttributeValue": ""
        }
    ],
    "StartTime": null,
    "EndTime": null,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. テキストエディタを使用し、必要に応じて JSON を変更します。JSON 入力には、指定された値のみが含まれている必要があります。

> **Important**
>
> 空の値や Null 値は、使用する前にテンプレートからすべて削除する必要があります。

次の例では、時間範囲と、返される結果の最大数を指定しています。

```
{
    "StartTime": "2023-11-01",
    "EndTime": "2023-12-12",
    "MaxResults": 10
}
```

3. 編集したファイルを入力として使用するには、次の例のように、構文 `--cli-input-json file://<filename>` を使用します。

```
aws cloudtrail lookup-events --event-category insight --cli-input-json file://
LookupEvents.txt
```

> **Note**
>
> `--cli-input-json` と同じコマンドラインで、他の引数を使用することもできます。

参照の出力フィールド

イベント

指定された参照属性と時間範囲に基づく参照イベントのリストです。イベントリストは時刻でソートされ、最新のイベントが最初に表示されます。各エントリには、検索要求に関する情報と、 CloudTrail 取得されたイベントの文字列表現が含まれます。

以下のエントリは、各参照イベント内のフィールドです。

CloudTrailEvent

返されたイベントのオブジェクト表現を含んだ JSON 文字列です。返される各要素については、「Record Body Contents」を参照してください。

EventId

返されたイベントの GUID を含んだ文字列です。

EventName

返されたイベントの名前を含んだ文字列です。

EventSource

AWS リクエストが行われたサービス。

EventTime

イベントの日時です (UNIX 時刻形式)。

リソース

返されたイベントによって参照されるリソースのリストです。各リソースエントリは、リソースタイプとリソース名を指定します。

ResourceName

イベントによって参照されるリソースの名前を含んだ文字列です。

ResourceType

イベントによって参照されるリソースのタイプを含んだ文字列です。リソースタイプを特定できない場合は、null が返されます。

ユーザー名

返されたイベントに対するアカウントのユーザー名を含んだ文字列です。

NextToken

前の `lookup-events` コマンドから次の結果ページを取得するための文字列です。トークンを使用するには、パラメータが元のコマンドと同じである必要があります。`NextToken` エントリが出力に表示されない場合、返す結果はそれ以上存在しません。

CloudTrail Insights イベントの詳細については、Insights イベントのログ記録本ガイドのを参照してください。

トレイルイベントを CloudTrail Lake にコピーする

既存のトレイルイベントを CloudTrail Lake イベントデータストアにコピーして、 point-in-timeトレイルに記録されたイベントのスナップショットを作成できます。証跡イベントをコピーしても、イベントをログに記録する証跡の機能が損なわれることはなく、証跡が変更されることもありません。

CloudTrail トレイルイベントをイベント用に構成された既存のイベントデータストアにコピーすることも、 CloudTrail 新しいイベントデータストアを作成して、イベントデータストアの作成の一部として [トレイルイベントのコピー] オプションを選択することもできます。証跡イベントを既存のイベントデータストアにコピーする方法の詳細については、「コンソールを使用して、トレイルイベントを既存のイベントデータストアにコピーします。 CloudTrail 」を参照してください。新しいイベントデータストアの作成方法に関する詳細は、「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。

トレイルイベントを CloudTrail Lake イベントデータストアにコピーすると、コピーしたイベントに対してクエリを実行できます。 CloudTrail Lake クエリでは、イベント履歴や実行中の単純なキーや値の検索よりも、より詳細でカスタマイズ可能なイベントを表示できます。`LookupEvents` CloudTrail Lake の詳細については、を参照してください。AWS CloudTrail Lake の使用

証跡イベントを組織のイベントデータストアにコピーするには、組織の管理アカウントを使用する必要があります。組織の委任された管理者アカウントを使用して、証跡イベントをコピーすることはできません。

CloudTrail Lake イベントデータストアには料金が発生します。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。Lake CloudTrail コストの価格設定と管理について詳しくは、「AWS CloudTrail 料金表」と CloudTrail Lake コストの管理「」を参照してください。

トレイルイベントを CloudTrail Lake イベントデータストアにコピーすると、イベントデータストアが取り込む非圧縮データの量に基づいて料金が発生します。

トレイルイベントを CloudTrail Lake にコピーすると、gzip（圧縮）CloudTrail 形式で保存されているログを解凍し、ログに含まれるイベントをイベントデータストアにコピーします。非圧縮データのサイズは、実際の S3 ストレージサイズよりも大きくなる可能性があります。圧縮されていないデータのサイズを概算するには、S3 バケット内のログのサイズに 10 を掛けます。

コピーするイベントの時間範囲を短くすることで、コストを削減できます。コピーしたイベントのクエリにイベントデータストアのみを使用する予定の場合は、イベントの取り込みを無効にして、今後のイベントで料金が発生しないようにすることができます。詳細については、「AWS CloudTrail 料金表」と「CloudTrail Lake コストの管理」を参照してください。

シナリオ

次の表は、証跡イベントのコピーに関する一般的なシナリオと、コンソールを使用して各シナリオを実行する方法について示したものです。

シナリオ	どうすればコンソールでこれを実行できますか?
新しいイベントを取り込むことなく、 CloudTrail Lake の過去のトレイルイベントの分析とクエリを行います。	新しいイベントデータストアを作成し、イベントデータストアを作成する一環として [証跡イベントをコピー] を選択します。イベントデータストアを作成する際には、[イベントを取り込む] (手順のステップ 15) の選択を解除し、イベントデータストアが確実に証跡の過去のイベントのみを含み、未来のイベントは含まれないようにします。
既存のトレイルを CloudTrail Lake イベントデータストアに置き換えます。	証跡と同じイベントセレクターを持つイベントデータストアを作成し、イベントデータストアの対象範囲が証跡と同じであることを確認します。

シナリオ	どうすればコンソールでこれを実行できますか?
	ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成より前の、コピーされたイベントの日付範囲を選択します。 イベントデータストアを作成したら、証跡の ログ記録をオフにします。そうすれば、追加料金の発生を防げます。

トピック

- 証跡イベントのコピーに関する留意事項
- 証跡イベントのコピーに必要な許可
- コンソールを使用して、トレイルイベントを既存のイベントデータストアにコピーします。 CloudTrail

証跡イベントのコピーに関する留意事項

証跡イベントをコピーする場合は、以下の要素を考慮してください。

- トレイルイベントをコピーする場合、S3 `GetObject`API CloudTrail オペレーションを使用してソース S3 バケットのトレイルイベントを取得します。S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Outposts、S3 Intelligent-Tiering Deep Archive 階層など、一部の S3 でアーカイブされたストレージクラスには、`GetObject` を使用してアクセスできません。これらのアーカイブ済みストレージ クラスに保存されている証跡イベントをコピーするには、まず S3 `RestoreObject` オペレーションでコピーを復元する必要があります。アーカイブされたオブジェクトの復元の詳細については、「Amazon S3 ユーザーガイド」の「アーカイブされたオブジェクトの復元」を参照してください。
- トレイルイベントをイベントデータストアにコピーすると、 CloudTrail コピー先のイベントデータストアのイベントタイプ、高度なイベントセレクター、 AWS リージョンまたはの設定に関係なく、すべてのトレイルイベントがコピーされます。
- 証跡イベントを既存のイベントデータストアにコピーする前に、そのイベントデータストアの料金設定オプションと保持期間が、ご自身のユースケースについて適切に設定されていることを確認してください。

  - 料金オプション: 料金オプションによって、イベントの取り込みと保存にかかるコストが決まります。料金オプションの詳細については、「AWS CloudTrail 料金表」および「イベントデータストアの料金オプション」を参照してください。
  - 保存期間:保持期間によって、イベントデータがイベントデータストアに保持される期間が決まります。 CloudTrail `eventTime`イベントデータストアの保持期間内であるトレイルイベントのみをコピーします。適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数 (保持期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。
- 調査のため証跡イベントをイベントデータストアにコピーしており、それ以上のイベントを取り込む必要がない場合は、イベントデータストアへの取り込みを停止できます。イベントデータストアを作成する際に、[イベントを取り込む] オプション (手順のステップ 15) の選択を解除し、イベントデータストアは確実に証跡の過去のイベントのみを含み、未来のイベントは含まれないようにします。
- 証跡イベントをコピーする前に、ソース S3 バケットにアタッチされているアクセスコントロールリスト (ACL) をすべて無効にして、送信先イベントデータストアの S3 バケットポリシーを更新します。S3 バケットとポリシーの更新の詳細については、「証跡イベントのコピー用の Amazon S3 バケットポリシー」を参照してください。ACL の無効化の詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化」を参照してください。
- CloudTrail ソース S3 バケットにある Gzip 圧縮ログファイルからのトレイルイベントのみをコピーします。 CloudTrail 圧縮されていないログファイルや Gzip 以外の形式で圧縮されたログファイルからはトレイルイベントをコピーしません。
- ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の、コピーされたイベントの時間範囲を選択します。
- デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、`CloudTrail`他のサービスのプレフィックスをチェックしません。 AWS CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、トレイルイベントをコピーするときにプレフィックスを選択する必要があります。
- 証跡イベントを組織のイベントデータストアにコピーするには、組織の管理アカウントを使用する必要があります。委任された管理者アカウントを使用して、組織のイベントデータストアに証跡イベントをコピーすることはできません。

証跡イベントのコピーに必要な許可

トレイルイベントをコピーする前に、IAM ロールに必要な権限がすべて揃っていることを確認してください。IAM ロールの許可を更新する必要があるのは、既存の IAM ロールを選択して証跡イベントをコピーする場合だけです。新しい IAM ロールを作成する場合は、 CloudTrail そのロールに必要なすべての権限が付与されます。

ソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでバケット内のデータの復号化が許可されていることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、 CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。

トピック

証跡イベントをコピーするための IAM 許可

証跡イベントをコピーする場合は、新しい IAM ロールを作成するか、既存の IAM ロールを使用するか選択できます。新しい IAM ロールを選択すると、必要な権限を持つ IAM CloudTrail ロールが作成されます。ユーザー側でこれ以上アクションを行う必要はありません。

既存のロールを選択する場合は、IAM ロールのポリシーでソース S3 CloudTrail バケットからトレイルイベントをコピーできることを確認してください。このセクションでは、必要な IAM ロールのアクセス許可と信頼ポリシーの例を示します。

次の例は、ソース S3 CloudTrail バケットからトレイルイベントをコピーすることを許可するアクセス権限ポリシーを示しています。*myAccountId*、*#####*、*#######*、*eventDataStoreId* を、設定に適した値に置き換えます*myBucketName*。*MyAccountId* は CloudTrail Lake AWS に使用されるアカウント ID であり、S3 AWS バケットのアカウント ID とは異なる場合があります。

key-region、*keyAccountID*、*keyID* を、ソース S3 バケットの暗号化に使用する KMS キーの値に置き換えます。送信元 S3 バケットが暗号化に KMS キーを使用しない場合は、`AWSCloudTrailImportKeyAccess` ステートメントを省略できます。

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

```
    {
      "Sid": "AWSCloudTrailImportBucketAccess",
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetBucketAcl"],
      "Resource": [
        "arn:aws:s3:::myBucketName"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportObjectAccess",
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::myBucketName/prefix",
        "arn:aws:s3:::myBucketName/prefix/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
       }
    },
    {
      "Sid": "AWSCloudTrailImportKeyAccess",
      "Effect": "Allow",
      "Action": ["kms:GenerateDataKey","kms:Decrypt"],
      "Resource": [
        "arn:aws:kms:key-region:keyAccountID:key/keyID"
      ]
    }
  ]
}
```

次の例は IAM 信頼ポリシーを示しています。これにより、IAM CloudTrail ロールを引き受け、ソース S3 バケットからトレイルイベントをコピーできます。*myAccountId*、*#### #*、*eventDataStoreID* を設定に適した値に置き換えてください。*MyAccountID* は CloudTrail Lake AWS に使用されるアカウント ID であり、S3 AWS バケットのアカウント ID とは異なる場合があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "myAccountID",
          "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
        }
      }
    }
  ]
}
```

証跡イベントのコピー用の Amazon S3 バケットポリシー

デフォルトでは、Amazon S3 バケットとオブジェクトはプライベートです。リソース所有者 (バケットを作成した AWS アカウント) のみが、バケットとそれに含まれるオブジェクトにアクセスできます。リソース所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

トレイルイベントをコピーする前に、S3 バケットポリシーを更新して、 CloudTrail バケットからトレイルイベントをコピーできるようにする必要があります。

S3 バケットポリシーに次のステートメントを追加して、これらの権限を付与できます。*roleArn* *myBucketName*とを実際の構成に適した値に置き換えてください。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::myBucketName",
    "arn:aws:s3:::myBucketName/*"
  ]
},
```

ソース S3 バケット内のデータを復号化するための KMS キーポリシー

ソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、SSE-KMS 暗号化が有効になっている S3 kms:Decrypt kms:GenerateDataKey バケットからトレイルイベントをコピーするのに必要なおよび権限が KMS キーポリシーに含まれていることを確認してください。 CloudTrail ソース S3 バケットが複数の KMS キーを使用している場合は、各キーポリシーを更新する必要があります。KMS キーポリシーを更新すると CloudTrail 、ソース S3 バケットのデータを復号化し、CloudTrail検証チェックを実行してイベントが標準に準拠していることを確認し、イベントを Lake イベントデータストアにコピーできるようになります。 CloudTrail

次の例は、ソース S3 バケットのデータを復号化できる CloudTrail KMS キーポリシーを示しています。*roleArn myBucketName*、*MyAccountId*、*#####*、*eventDataStoreID* は、構成に適した値に置き換えてください。*MyAccountID* は CloudTrail Lake AWS に使用されるアカウント ID であり、S3 バケットのアカウント ID とは異なる場合があります。 AWS

```
{
  "Sid": "AWSCloudTrailImportDecrypt",
  "Effect": "Allow",
  "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
  ],
  "Principal": {
    "AWS": "roleArn"
```

```
  },
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::myBucketName/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdataStore/eventDataStoreId"
    }
  }
}
```

コンソールを使用して、トレイルイベントを既存のイベントデータストアにコピーします。 CloudTrail

以下の手順を実行し、証跡イベントを既存のイベントデータストアにコピーします。新しいイベントデータストアの作成方法に関する詳細は、「コンソールを使用してイベントのイベントデータストアCloudTrailを作成する」を参照してください。

> **Note**
>
> 証跡イベントを既存のイベントデータストアにコピーする前に、そのイベントデータストアの料金設定オプションと保持期間が、ご自身のユースケースについて適切に設定されていることを確認してください。
>
> - 料金オプション: 料金オプションによって、イベントの取り込みと保存にかかるコストが決まります。料金オプションの詳細については、「AWS CloudTrail 料金表」および「イベントデータストアの料金オプション」を参照してください。
> - 保存期間:保持期間によって、イベントデータがイベントデータストアに保持される期間が決まります。 CloudTrail `eventTime`イベントデータストアの保持期間内であるトレイルイベントのみをコピーします。適切な保存期間を決定するには、コピーする最も古いイベントの日数と、イベントデータストアにイベントを保持したい日数 (保持期間 = *`oldest-event-in-days`*+ *`number-days-to-retain`*) の合計を計算します。例えば、コピーする最も古いイベントが 45 日前のもので、そのイベントをイベントデータストアにさらに 45 日間保持したい場合は、保持期間を 90 日間に設定します。

イベントデータストアに証跡イベントをコピーするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. CloudTrail コンソールの左側のナビゲーションペインで [Trails] を選択します。
3. [Trails] (追跡) ページで、証跡を選択し、次に[Copy events to Lake] (イベントを Lake にコピー) を選択します。トレイルのソース S3 バケットがデータ暗号化に KMS キーを使用している場合は、KMS CloudTrail キーポリシーでバケット内のデータの復号化が許可されていることを確認してください。ソース S3 バケットが複数の KMS キーを使用している場合は、 CloudTrail バケット内のデータの復号を許可するように各キーのポリシーを更新する必要があります。KMS キーポリシーの更新の詳細については、「ソース S3 バケット内のデータを復号化するための KMS キーポリシー」を参照してください。
4. (オプション) デフォルトでは、S3 CloudTrail CloudTrail `CloudTrail` バケットのプレフィックスに含まれるイベントとプレフィックス内のプレフィックスのみをコピーし、`CloudTrail`他のサービスのプレフィックスをチェックしません。 AWS CloudTrail 別のプレフィックスに含まれるイベントをコピーする場合は、[Enter S3 URI] を選択し、[Browse S3] を選択してプレフィックスを参照します。

   S3 バケットポリシーは、 CloudTrail トレイルイベントをコピーするためのアクセス権を付与する必要があります。S3 バケットとポリシーの更新の詳細については、「証跡イベントのコピー用の Amazon S3 バケットポリシー」を参照してください。
5. [イベントの時間範囲を指定] で、イベントをコピーする時間範囲を選択します。 CloudTrail トレイルイベントをコピーする前に、プレフィックスとログファイル名をチェックして、選択した開始日と終了日の間の日付が名前に含まれていることを確認します。[Relative range] (相対範囲) または[Absolute range] (絶対範囲) を選択することができます。ソース証跡と送信先イベントデータストア間でイベントが重複しないようにするには、イベントデータストアの作成よりも前の時間範囲を選択します。

> **Note**
>
> CloudTrail `eventTime`イベントデータストアの保存期間内のトレイルイベントのみをコピーします。たとえば、イベントデータストアの保持期間が 90 日の場合、90 CloudTrail `eventTime` 日以上前のトレイルイベントはコピーされません。

- [相対範囲] を選択すると、過去 6 か月、1 年、2 年、7 年間に記録されたイベントをコピーするか、またはカスタム範囲をコピーするかを選択できます。 CloudTrail 選択した期間内に記録されたイベントをコピーします。
- [絶対範囲] を選択すると、特定の開始日と終了日を選択できます。 CloudTrail 選択した開始日と終了日の間に発生したイベントをコピーします。

6. [Delivery location] (配信場所) で、ドロップダウンリストから配信先イベントデータストアを選択します。
7. [Permissions] (アクセス許可) については、以下の IAM ロールのオプションから選択します。既存の IAM ロールを選択する場合は、IAM ロールポリシーが必要なアクセス許可を提供していることを確認してください。IAM ロールの許可の更新の詳細については、「証跡イベントをコピーするための IAM 許可」を参照してください。

   - [Create a new role (recommended)] (新しいロールの作成 (推奨)) を選択して、新しい IAM ロールを作成します。[Enter IAM role name] (IAM ロール名を入力してください) に、ロールの名前を入力します。 CloudTrail この新しいロールに必要な権限が自動的に作成されます。
   - リストにないカスタム IAM ロールを使用するには、[カスタム IAM ロール ARN を使用] を選択します。[Enter IAM role ARN] (IAM ロールの ARN を入力) で、IAM ARN を入力します。
   - ドロップダウンリストから既存の IAM ロールを選択します。
8. [Copy events] (イベントをコピー) を選択します。
9. コピーの確認を求めるプロンプトが表示されます。確認する準備ができたら、[Copy trail events to Lake] (証跡イベントを Lake にコピー) を選択してから[Copy events] (イベントをコピー) を選択します。
10. [Copy details] (コピーの詳細) ページで、コピーの状態を確認し、エラーを確認できます。証跡イベントのコピーが完了すると、その[Copy status] (コピー ステータス) は、エラーがない場合は[Completed] (完了) に設定され、エラーが発生した場合は[Failed] (失敗) に設定されます。

> **Note**
>
> イベントコピーの詳細ページに表示される詳細は、リアルタイムではありません。[Prefixes copied] (コピーされたプレフィックス) などの詳細の実際の値は、ページに表示される値よりも高くなる場合があります。 CloudTrail イベントコピーの過程で、詳細を段階的に更新します。

11. [Copy status] (コピーのステータス) が[Failed] (失敗) の場合は、[Copy failures] (コピーの失敗) に示されているエラーを修正し、[Retry copy] (コピーの再試行) を選択します。コピーを再試行すると、 CloudTrail 障害が発生した場所でコピーが再開されます。

証跡イベントコピーの詳細を表示する方法については、「イベントコピーの詳細」を参照してください。

CloudTrail ログファイルの取得と表示

証跡を作成して必要なログファイルをキャプチャするように設定した後は、ログファイルを検索し、含まれる情報を解釈できるようにする必要があります。

CloudTrail トレイルを作成するときに指定した Amazon S3 バケットにログファイルを配信します。CloudTrail 通常、API 呼び出しから平均約 5 分以内にログを配信します。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。インサイトイベントは、通常、異常なアクティビティから 30 分以内にバケットに配信されます。インサイトイベントを初めて有効にした後、異常なアクティビティが検出された場合に、最初のインサイトイベントが表示されるまで最大 36 時間かかります。

> **Note**
>
> 証跡の設定を誤ると (S3 バケットにアクセスできないなど)、ログファイルを S3 バケットに 30 日間再配信しようとしますが、 CloudTrail attempted-to-deliver これらのイベントには標準料金が適用されます。 CloudTrail 証跡の不適切な設定による課金を避けるには、その証跡を削除する必要があります。

トピック

- ログファイルを検索する CloudTrail
- CloudTrail ログファイルのダウンロード

ログファイルを検索する CloudTrail

CloudTrail ログファイルを gzip アーカイブで S3 バケットに公開します。S3 バケットでは、ログファイルに次の要素を含む形式の名前が付けられます。

- トレイルを作成したときに指定したバケット名 (コンソールの Trails ページにあります) CloudTrail

- トレイルを作成したときに指定した (オプションの) プレフィックス
- 文字列 "」AWSLogs
- アカウント番号
- 文字列 "CloudTrail」
- リージョン識別子 (us-west-1 など)
- ログファイルが発行された年 (YYYY 形式)
- ログファイルが発行された月 (MM 形式)
- ログファイルが発行された日 (DD 形式)
- 同じ期間をカバーする他のファイルから当該ファイルを区別するための英数字の文字列

次の例は、完全なログファイルオブジェクト名を示しています。

```
bucket_name/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

> **Note**
>
> 組織記録の場合、S3 バケットのログファイルオブジェクト名には、次のようにパスに組織ユニット ID が含まれます。
>
> ```
> bucket_name/prefix_name/AWSLogs/O-ID/Account ID/
> CloudTrail/Region/YYYY/MM/DD/file_name.json.gz
> ```

ログファイルを取得するには、Amazon S3 コンソール、Amazon S3 コマンドラインインターフェイス (CLI)、または API を使用します。

Amazon S3 コンソールでログファイルを検索するには

1. Amazon S3 コンソールを開きます。
2. 指定したバケットを選択します。
3. 必要なログファイルが見つかるまでオブジェクト階層内を移動します。

   ログファイルの拡張子はすべて .gz です。

次の例のように、オブジェクト階層を移動しますが、バケット名、アカウント ID、リージョン、および日付は異なります。

```
All Buckets
    Bucket_Name
        AWSLogs
            123456789012
                CloudTrail
                    us-west-1
                        2014
                            06
                                20
```

先のオブジェクト階層のログファイルは、次のようになります。

```
123456789012_CloudTrail_us-west-1_20140620T1255ZHdkvFTXOA3Vnhbc.json.gz
```

> **Note**
>
> めったに起こることではありませんが、1 つ以上の重複したイベントを含むログファイルを受け取ることがあります。ほとんどの場合、重複するイベントは同じ eventID を持っています。[eventID] フィールドの詳細については、「CloudTrail レコードの内容」を参照してください。

CloudTrail ログファイルのダウンロード

ログファイルは JSON 形式です。JSON ビューアのアドオンがインストールされている場合は、ブラウザで直接ファイルを表示できます。バケットのログファイル名をダブルクリックすると、新しいブラウザウィンドウまたはタブが開きます。JSON は読み取り可能な形式で表示されます。

CloudTrail ログファイルは Amazon S3 オブジェクトです。Amazon S3 コンソール、 AWS Command Line Interface (CLI)、または Amazon S3 API を使用してログファイルを取得できます。

詳細については、Amazon S3 オブジェクトの概要」を参照してください。

次の手順は、 AWS Management Consoleでログファイルをダウンロードする方法を示します。

ログファイルをダウンロードして読み取るには

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. バケットを選択して、ダウンロードするログファイルを選択します。
3. [Download] または [Download as] を選択し、プロンプトに従ってファイルを保存します。この方法では、ファイルが圧縮形式で保存されます。

   > **Note**
   >
   > Chrome などの一部のブラウザでは、ログファイルが自動的に抽出されます。その場合は、ステップ 5 に進みます。

4. 7-Zip のような製品を使用してログファイルを抽出します。
5. Notepad++ などのテキストエディタで、ログファイルを開きます。

ログファイルのエントリで表示できるイベントフィールドの詳細については、「CloudTrail レコードの内容」を参照してください。

AWS は、ログ記録と分析に関するサードパーティーのスペシャリストと提携し、 CloudTrail 出力を使用するソリューションを提供します。詳細については、「 AWS CloudTrail パートナー」を参照してください。

> **Note**
>
> [Event history] 機能を使用して、過去 90 日間の API アクティビティの作成、更新、削除のイベントを検索することもできます。
> 詳細については、「 CloudTrail イベント履歴の操作」を参照してください。

の Amazon SNS 通知の設定 CloudTrail

Amazon S3 CloudTrail バケットに新しいログファイルが公開されると通知を受けることができます。Amazon Simple Notification Service (Amazon SNS) を使用して、通知を管理します。

通知はオプションです。通知が必要な場合は、新しいログファイルが送信されるたびに Amazon SNS CloudTrail トピックに更新情報を送信するように設定します。これらの通知を受け取るには、Amazon SNS を使用してトピックを受信することができます。受信者として、アップデートを

Amazon Simple Queue Service (Amazon SQS) キューに送信できます。これにより、これらの通知をプログラムで処理できます。

トピック

- CloudTrail 通知を送信するように設定します。

CloudTrail 通知を送信するように設定します。

Amazon SNS トピックを使用するように証跡を設定できます。 CloudTrail コンソールまたは aws cloudtrail create-trailCLI コマンドを使用してトピックを作成できます。 CloudTrail Amazon SNS トピックを作成し、適切なポリシーをアタッチします。これにより、 CloudTrail そのトピックに公開する権限が付与されます。

SNS トピック名を作成する際には、名前が次の要件を満たしている必要があります。

- 1 ~ 256 文字
- 大文字および小文字の ASCII 文字、数字、アンダースコア、またはハイフンが含まれている

すべてのリージョンに適用される証跡について通知を設定した場合、すべてのリージョンからの通知は、指定した Amazon SNS トピックに送信されます。リージョン固有の証跡が 1 つ以上ある場合は、リージョンごとに個別のトピックを作成し、各トピックを個別にサブスクライブする必要があります。

通知を受け取るには、Amazon SNS CloudTrail トピックまたはを使用するトピックに登録します。これを行うには、Amazon SNS コンソールまたは Amazon SNS CLI コマンドを使用します。詳細については、「Amazon Simple 通知サービス デベロッパーガイド」の「Amazon SNS トピックのサブスクライブ」を参照してください。

> **Note**
>
> CloudTrail ログファイルが Amazon S3 バケットに書き込まれると通知を送信します。アクティブなアカウントでは、大量の通知が生成されることがあります。E メールまたは SMS を使用してサブスクライブしている場合は、大量のメッセージが受信される可能性があります。そのため、 Amazon Simple Queue Service (Amazon SQS) を使用してサブスクライブすることをお勧めします。これにより、プログラムを使って通知を処理することができます。詳細については、『Amazon Simple Queue Service デベロッパーガイド』の「Amazon SNS トピックへの Amazon SQS キューのサブスクライブ (コンソール)」を参照してください。

Amazon SNS 通知は、Message フィールドを含んだ JSON オブジェクトで構成されます。Message フィールドには、次の例のように、ログファイルへのフルパスがリストされます。

```
{
    "s3Bucket": "your-bucket-name","s3ObjectKey": ["AWSLogs/123456789012/
CloudTrail/us-east-2/2013/12/13/123456789012_CloudTrail_us-
west-2_20131213T1920Z_LnPgDQnpkSKEsppV.json.gz"]
}
```

Amazon S3 バケットに複数のログファイルが配信された場合は、次の例のように、複数のログが通知に含まれている可能性があります。

```
{
    "s3Bucket": "your-bucket-name",
    "s3ObjectKey": [
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2215Z_kpaMYavMQA9Ahp7L.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2210Z_zqDkyQv3TK8ZdLr0.json.gz",
        "AWSLogs/123456789012/CloudTrail/us-
east-2/2016/08/11/123456789012_CloudTrail_us-
east-2_20160811T2205Z_jaMVRa6JfdLCJYHP.json.gz"
    ]
}
```

E メールで通知を受け取る場合、E メールの本文は、Message フィールドの内容で構成されます。JSON 構造については、『Amazon 簡易通知サービス開発者ガイド』の「Amazon SQS キューへのファンアウト」を参照してください。Message情報が表示されるのはフィールドだけです。CloudTrail その他のフィールドには、Amazon SNS サービスからの情報が記載されます。

CloudTrail API を使用して証跡を作成する場合、CreateTrailUpdateTrailまたはオペレーションで通知の送信先となる既存の Amazon SNS トピックを指定できます。 CloudTrail トピックが存在し、 CloudTrail そのトピックに通知を送信できる権限があることを確認する必要があります。「の Amazon SNS トピックポリシー CloudTrail」を参照してください

追加リソース

Amazon SNS トピックおよびそのサブスクライブの詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

証跡を管理するためのヒント

- 2019 年 4 月 12 日以降、 AWS リージョン トレイルはイベントを記録する場所でのみ表示可能になりました。イベントをすべて記録する証跡を作成すると AWS リージョン、 AWS リージョン AWS 作業中のパーティションのすべてのイベントがコンソールに表示されます。1 つのイベントのみを記録する証跡を作成した場合 AWS リージョン、その証跡のみを表示、管理できます AWS リージョン。
- リストの証跡を編集するには、証跡名を選択します。
- AWS 作業しているパーティション内のすべてのリージョンからログファイルを受け取ることができるように、すべてのリージョンに適用されるトレイルを少なくとも 1 つ設定してください。
- 特定のリージョンの、イベントのログ記録を行い、同じリージョンにある S3 バケットにログファイルを配信するときは、証跡を更新することで単一のリージョンに適用できます。これは、ログファイルを分けておきたい場合に役立ちます。たとえば、ユーザーに特定のリージョンのログを自分で管理させたい場合や、 CloudWatch ログアラームをリージョンごとに分けたい場合があります。
- AWS 複数のアカウントからのイベントを 1 つのトレイルに記録するには、 AWS Organizations その中に組織を作成してから、組織トレイルを作成することを検討してください。
- 複数の認跡の作成では、追加コストが発生します。料金の詳細については、「AWS CloudTrail 料金表」を参照してください。

CloudTrail 証跡コストの管理

ベストプラクティスとして、 CloudTrail コスト管理に役立つ AWS サービスとツールを使用することをお勧めします。また、コスト効率を維持しながら、必要なデータをキャプチャする方法で CloudTrail 証跡を設定および管理することもできます。 CloudTrail 料金の詳細については、「 の料金AWS CloudTrail」を参照してください。

コスト管理に役立つツール

AWS の機能である Budgets では AWS Billing and Cost Management、コストまたは使用量が予算額を超えたとき (または超えると予測されるとき) に警告するカスタム予算を設定できます。

複数の証跡を作成する場合、 Budgets CloudTrail を使用して AWS の予算を作成することが推奨されるベストプラクティスであり、 CloudTrail 支出の追跡に役立ちます。コストベースの予算は、CloudTrail 使用量の請求額についての認識を高めるのに役立ちます。 予算アラートは、請求額が定

義したしきい値に達したときに通知します。予算アラートを受け取ったら、請求サイクルの終了前に変更を加えて、コストを管理できます。

予算を作成したら、 AWS Cost Explorer を使用して、 CloudTrail コストが AWS 請求全体にどのような影響を与えているかを確認できます。 AWS Cost Explorer では、 CloudTrail をサービスフィルターに追加した後、リージョンとアカウントの両方で、過去の CloudTrail支出を現在の month-to-date (MTD) 支出の支出と比較できます。この機能は、月 CloudTrail額支出の予期しないコストをモニタリングおよび検出するのに役立ちます。Cost Explorer の追加機能を使用すると、特定のリソースレベルで CloudTrail 支出と月額支出を比較し、コストの増減を促進している要因に関する情報を提供できます。

> **Note**
>
> CloudTrail 証跡にタグを適用することはできますが、 AWS Billing 現在、コスト配分のために証跡に適用されたタグを使用することはできません。Cost Explorer は、 CloudTrail Lake イベントデータストアと CloudTrail サービス全体のコストを表示できます。

AWS Budgets の使用を開始するには、 を開きAWS Billing and Cost Management、左側のナビゲーションバーで Budgets を選択します。 CloudTrail 支出を追跡する予算を作成する際には、予算アラートを設定することをお勧めします。 AWS Budgets の使用方法の詳細については、「 によるコストの管理 AWS Budgets」および「 のベストプラクティス AWS Budgets」を参照してください。

証跡の設定

CloudTrail は、アカウントで証跡を設定する方法に柔軟性を提供します。セットアッププロセス中に行う決定によっては、 CloudTrail 請求書への影響を理解する必要があります。以下は、証跡設定が CloudTrail 請求にどのように影響するかの例です。

複数の証跡の作成

各リージョン内の管理イベントの最初のコピーは無料で配信されます。例えば、アカウントに 2 つの単一リージョンの証跡、 の証跡us-east-1、および の別の証跡がある場合us-west-2、各リージョンに 1 つの証跡ログイベントしかないため、 CloudTrail 料金は発生しません。ただし、アカウントにマルチリージョンの証跡と追加の単一リージョンの証跡がある場合、マルチリージョンの証跡はすでに各リージョンのイベントを口グ記録しているため、単一リージョンの証跡には料金が発生します。

同じ管理イベントを他の送信先に配信する証跡をさらに作成した場合、それ以降の配信には CloudTrail コストが発生します。これにより、異なるユーザーグループ (デベロッパー、セキュリ

ティ担当者、IT 監査人など) が独自のログファイルのコピーを受け取ることができます。データイベントの場合、最初の配信を含むすべての配信に CloudTrail コストが発生します。

証跡をさらに追加するときは、ログに精通し、アカウントのリソースによって生成されるイベントのタイプとボリュームを理解することが特に重要です。これにより、アカウントに関連付けられるイベントの量を予測し、証跡のコストを計画できます。例えば、S3 バケットで AWS KMS マネージドサーバー側の暗号化 (SSE-KMS) を使用すると、 で多数の AWS KMS 管理イベントが発生する可能性があります CloudTrail。複数の証跡にまたがるイベントの量が大きくなった場合も、コストに影響する可能性があります。

証跡に記録されるイベントの数を制限するために、証跡の作成 AWS KMS ページまたは更新ページでイベントを除外または Amazon RDS Data API AWS KMS イベントを除外を選択して、 または Amazon RDS Data API イベントをフィルタリングできます。 基本のイベントセレクターを使用する場合は、管理イベントのみをフィルタリングできます。高度なイベントセレクタを使用すれば、管理イベントとデータイベントの両方をフィルタリングできます。高度なイベントセレクターでは、`resources.type`、`eventName`、`resources.ARN`、および `readOnly` フィールドに基づいてデータイベントを含めたり除外したりできるため、関心のあるデータイベントのみをログ記録できます。これらのフィールドの設定については、「AdvancedFieldSelector」を参照してください。証跡の作成と更新の詳細情報については、本ガイドの「証跡の作成」または「証跡の更新」を参照してください。

AWS Organizations

で Organizations 証跡を設定すると CloudTrail、 は証跡を組織内の各メンバーアカウントに CloudTrail レプリケートします。メンバーアカウントの既存の証跡に加えて、新しい証跡が作成されます。組織の証跡の設定がすべてのアカウントに伝達されるため、組織の証跡の設定が組織内のすべてのアカウントの証跡の設定と一致していることを確認します。

Organizations は各メンバーアカウントに証跡を作成するため、Organizations 証跡と同じ管理イベントを収集する追加の証跡を作成する個々のメンバーアカウントは、イベントの 2 番目のコピーを収集します。アカウントは 2 番目のコピーに対して課金されます。同様に、アカウントにマルチリージョンの証跡があり、単一のリージョンに 2 番目の証跡を作成し、マルチリージョンの証跡と同じ管理イベントを収集する場合、単一リージョンの証跡はイベントの 2 番目のコピーを配信します。2 番目のコピーでは、料金が発生します。

以下も参照してください。

- AWS CloudTrail の料金
- によるコストの管理 AWS Budgets

- Cost Explorer を開始する
- 組織の証跡の作成を準備する

命名の要件

このセクションでは、 CloudTrail リソース、Amazon S3 バケット、および KMS キーの命名要件について説明します。

トピック

- CloudTrail リソース命名要件
- Amazon S3 バケットの命名要件
- AWS KMS エイリアスの命名要件

CloudTrail リソース命名要件

CloudTrail リソース名は以下の要件を満たす必要があります。

- ASCII 文字のみ (a~z、A~Z)、数字 (0~9)、ピリオド (.)、アンダースコア (_)、またはダッシュ (-) を含みます。
- 文字または数字で始まり、文字または数字で終わります。
- 3 ~ 128 文字にしてください。
- 連続するピリオド、アンダースコア、ダッシュはありません。my-_namespace や my-\-namespace のような名前は無効です。
- IP アドレス形式ではありません (たとえば、192.168.5.4)。

Amazon S3 バケットの命名要件

CloudTrail ログファイルの保存に使用する Amazon S3 バケットには、米国標準以外のリージョンの命名要件に準拠した名前を付ける必要があります。Amazon S3 のバケット名は、ピリオドで区切られた 1 つ以上の一連のラベルとして定義されています。命名規則の全一覧については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの名前付けルール」を参照してください。

次のような規則があります。

- バケット名は 3 ~ 63 文字の長さで、小文字、数字、ピリオド、ダッシュのみを使用できます。

- バケット名の各ラベルは、小文字または数字で始まっている必要があります。
- バケット名では、アンダースコア、末尾のダッシュ、連続するピリオド、隣接するピリオドとダッシュは使用できません。
- バケット名を IP アドレス (198.51.100.24) として書式設定することはできません。

> **Warning**
>
> S3 ではバケットをパブリックにアクセス可能な URL として使用できるので、グローバルに一意なバケット名を選択する必要があります。他のアカウントで同じ名前のバケットがすでに作成されている場合は、別の名前を使用する必要があります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの制約と制限」を参照してください。

AWS KMS エイリアスの命名要件

を作成するときは AWS KMS key、エイリアスを選択して識別できます。たとえば、「KMS-CloudTrail-us-west-2」というエイリアスを選択して、特定の記録のログを暗号化できます。

エイリアスは、次の要件を満たしている必要があります。

- 1 ~ 256 文字以内
- 使用できるのは、英数字 (A~Z、a~z、0~9)、ハイフン (-)、スラッシュ (/)、アンダースコア (_) です
- 先頭を aws にすることはできません

詳細については、AWS Key Management Service デベロッパーガイドのキーの作成を参照してください。

証跡を複数作成する

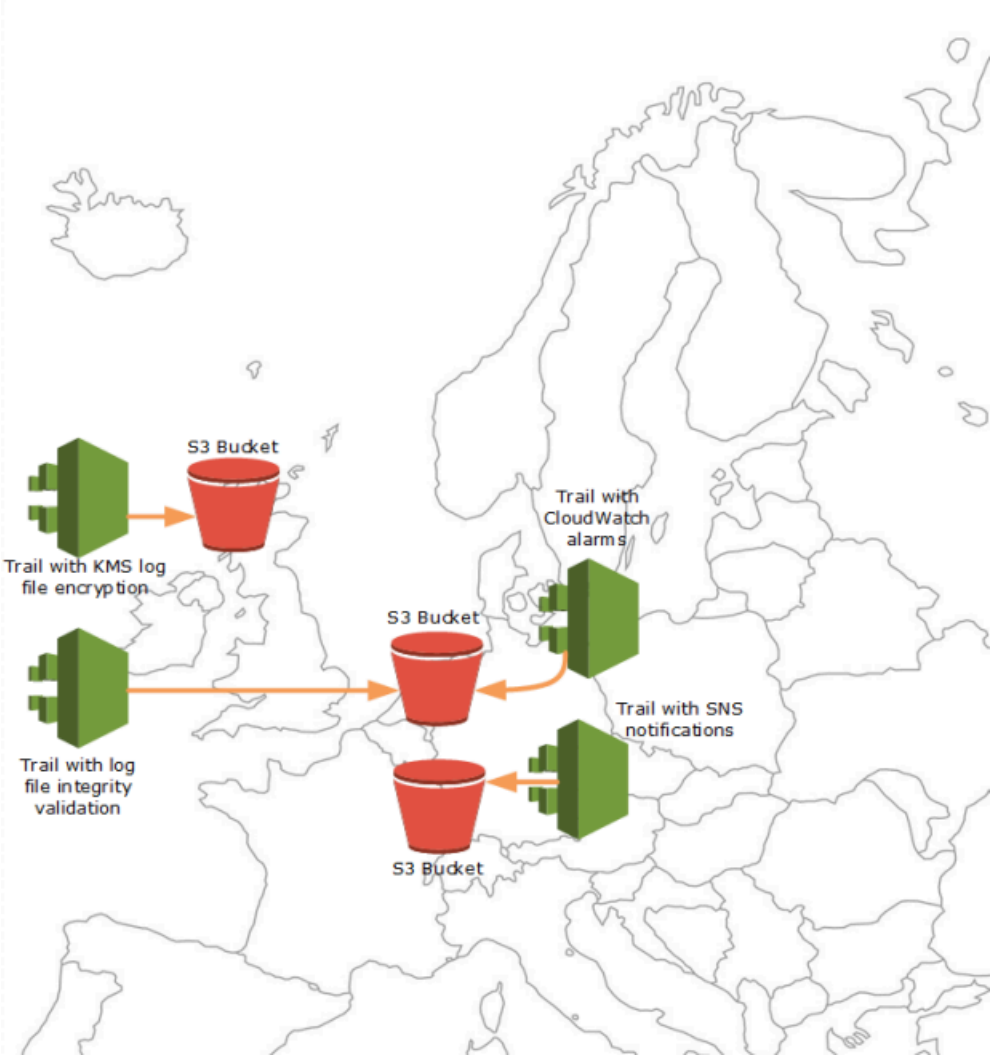
CloudTrail ログファイルを使用して、アカウントの運用上またはセキュリティ上の問題のトラブルシューティングを行うことができます。 AWS ユーザーの種類ごとに複数の証跡を作成すれば、それらのユーザーが独自の証跡を作成し、管理できるようになります。証跡のログファイルの配信先としては、個別の S3 バケットか、共有の S3 バケットを設定できます。

> **Note**
>
> AWS リージョン 各アカウントの管理イベントの最初のコピーは無料です。同じ管理イベントを他の宛先に配信する証跡をさらに作成すると、それ以降の配信にはコストが発生します CloudTrail 。 CloudTrail コストについて詳しくは、「料金表」と「」を参照してください AWS CloudTrail 。 CloudTrail 証跡コストの管理

例えば、次のような要件に応じて、ユーザーごとの証跡を作成できます。

- セキュリティ管理者が欧州 (アイルランド) リージョンの証跡を作成し、KMS のログファイル暗号化を設定できるようにします。この証跡では、欧州 (アイルランド) リージョンの S3 バケットにログファイルを配信します。
- IT 監査人はヨーロッパ (アイルランド) 地域で証跡を作成し、ログファイルの整合性検証を設定して、ログファイルが配信されてから変更されていないことを確認します。 CloudTrail この証跡では、欧州 (フランクフルト) リージョンの S3 バケットにログファイルを配信するよう設定します。
- 開発者はヨーロッパ (フランクフルト) リージョンで証跡を作成し、特定の API CloudWatch アクティビティに関する通知を受け取るようにアラームを設定します。この証跡では、ログファイルの整合性確認用に設定された証跡と同じ S3 バケットを共有します。
- もう 1 人のデベロッパーが欧州 (フランクフルト) リージョンの証跡を作成し、SNS を設定できるようにします。ログファイルは、欧州 (フランクフルト) リージョンの個別の S3 バケットに配信します。

次の図は、この例を説明したものです。



> **Note**
>
> 1 つにつき 5 つまでトレイルを作成できます。 AWS リージョンマルチリージョントレイルは、リージョンごとに 1 つのトレイルとしてカウントされます。

リソースレベルの権限を使用して、特定の操作を実行するユーザーの権限を管理できます。CloudTrail

たとえば、あるユーザーに証跡のアクティビティ表示権限を付与しながらも、ログ記録の開始権限や停止権限は制限するといったことが可能です。また、証跡の作成や削除を行えるフル権限は別のユーザーに付与するといったことも可能です。これにより、証跡とユーザーアクセスを詳細に制御することができます。

リソースレベルのアクセス許可の詳細については、「例: 特定の証跡に対するアクションのポリシーの作成と適用」を参照してください

複数のトレイルについて詳しくは、よくある質問をご覧ください。CloudTrail

CloudTrail トレイルのユーザー権限の制御

AWS CloudTrail AWS Identity and Access Management (IAM) と統合することで、 CloudTrail AWS 必要なリソースやその他のリソースへのアクセスを制御できます。 CloudTrail これらのリソースの例としては、Amazon S3 バケットや Amazon Simple Notification Service (Amazon SNS) のトピックがあります。IAM を使用して、 AWS CloudTrail どのユーザーが証跡の作成、設定、削除、ロギングの開始と停止、ログ情報を含むバケットへのアクセスを許可するかを制御できます。詳細については、「Identity and Access Management AWS CloudTrail」を参照してください。

以下のトピックは、権限、ポリシー、セキュリティを理解するのに役立ちます。 CloudTrail

- CloudTrail 管理権限の付与
- Amazon S3 バケットの命名規則
- の Amazon S3 バケットポリシー CloudTrail
- を使用して組織の証跡を作成する AWS Command Line Interface の組織の証跡に対するバケットポリシーの例。
- の Amazon SNS トピックポリシー CloudTrail
- CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)
- 証跡イベントのコピーに必要な許可
- 委任された管理者を割り当てるために必要な許可
- コンソールで作成されたデフォルト KMS キーポリシー CloudTrail
- AWS Config コンソール上の情報を表示する権限を付与する CloudTrail
- CloudTrail AWS アカウント間でのログファイルの共有
- 組織の証跡を作成するために必要なアクセス許可
- 既存の IAM ロールを使用して組織証跡のモニタリングを Amazon Logs に追加する CloudWatch

インターフェイス VPC AWS CloudTrail エンドポイントでの使用

Amazon Virtual Private Cloud (Amazon VPC) AWS を使用してリソースをホストする場合、VPC との間にプライベート接続を確立できます。 AWS CloudTrailこの接続を使用すると、 CloudTrail パブリックインターネットを経由せずに VPC 上のリソースと通信できるようになります。

Amazon VPC は、 AWS AWS 定義した仮想ネットワークでリソースを起動するために使用できるサービスです。VPC を使用することで、IP アドレス範囲、サブネット、ルートテーブル、ネットワークゲートウェイなどのネットワーク設定を制御できます。VPC エンドポイントでは、VPC AWS AWS とサービス間のルーティングはネットワークによって処理され、IAM ポリシーを使用してサービスリソースへのアクセスを制御できます。

VPC を接続するには CloudTrail、のインターフェイス VPC エンドポイントを定義します。CloudTrailインターフェイスエンドポイントは、 AWS サポートされているサービスを宛先とするトラフィックのエントリポイントとして機能するプライベート IP アドレスを持つelastic network interface です。エンドポイントは、インターネットゲートウェイ、ネットワークアドレス変換 (NAT) インスタンス、または VPN CloudTrail 接続を必要とせずに、信頼性が高くスケーラブルな接続を実現します。詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC とは」を参照してください。

インターフェイス VPC エンドポイントは AWS PrivateLink、プライベート IP アドレスを持つ elastic network interface AWS AWS を使用してサービス間のプライベート通信を可能にするテクノロジーを利用しています。詳細については、「」を参照してください。AWS PrivateLink

以下の手順は、Amazon VPC のユーザー向けです。詳細については、アマゾン VPC ユーザーガイドの「Amazon VPC の使用を開始する」を参照してください。

可用性

CloudTrail 現在、 AWS 以下のリージョンの VPC エンドポイントをサポートしています。

- 米国東部 (オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)

- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- カナダ西部 (カルガリー)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ミラノ)
- 欧州 (パリ)
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

の VPC エンドポイントの作成 CloudTrail

VPC CloudTrail で使用を開始するには、のインターフェイス VPC エンドポイントを作成します。CloudTrail詳細については、Amazon VPC ユーザーガイドの「AWS のサービス インターフェイスを使用して VPC エンドポイントにアクセスする」を参照してください。

の設定を変更する必要はありません。 CloudTrail CloudTrail パブリックエンドポイントまたはプライベートインターフェイスの VPC AWS のサービス エンドポイントのいずれかを使用して他のエンドポイントを呼び出します。

共有サブネット

CloudTrail VPC エンドポイントは、他の VPC エンドポイントと同様に、共有サブネットの所有者アカウントによってのみ作成できます。ただし、参加者アカウントは、参加者アカウントと共有されているサブネットの CloudTrail VPC エンドポイントを使用できます。Amazon VPC 共有の詳細については、「Amazon VPC ユーザーガイド」の「Share your VPC with other accounts」を参照してください。

AWS アカウント クロージャーとトレイル

AWS CloudTrail 任意のユーザー、ロール、 AWS のサービス AWS アカウントまたはユーザーによって生成されたアカウントアクティビティのイベントを継続的に監視して記録します。 CloudTrail ユーザーは証跡を作成して、所有している S3 バケットでこれらのイベントのコピーを受け取ることができます。

CloudTrail は基本的なセキュリティサービスであるため、 AWS アカウント ユーザーが作成した証跡は、閉じる前にユーザーが明示的に証跡を削除しない限り、閉鎖後も存在し続け、イベントを配信します。 AWS アカウント この動作は、管理アカウントまたは委任された管理者によって作成された組織証跡や、組織のメンバーアカウントで作成されたマルチリージョンの組織証跡にも適用されます。これにより、ユーザーがアカウントを再度解説した場合でも、破壊されていないアカウントアクティビティの記録を取得できるようにしています。同時に、残っているアカウントリソースやサービスの削除や終了など、最終的なアカウントアクティビティについての可視性もユーザーに提供しています。

ユーザーは、閉鎖する前に証跡を削除することも AWS アカウント、AWS Support閉鎖後に連絡して記録の削除を依頼することもできます。 AWS アカウント

の閉鎖について詳しくは AWS アカウント、「閉鎖する AWS アカウント」を参照してください。

> **Note**
>
> CloudTrail ログファイルの検証が有効になっている場合、 CloudTrail ユーザーはログが作成されたかどうかを示すダイジェストファイルを 1 時間ごとに受信し続けます。
> CloudTrail Lake イベントデータストア、統合用の CloudTrail Lake チャネル、 CloudTrail サービスにリンクされたチャネル、およびトレイル用に作成されたリソース (たとえば、閉

鎖されたアカウントに存在する Amazon CloudWatch Logs ロググループと Amazon S3 バケット）は、 AWS アカウント閉鎖の標準的な動作に従い、閉鎖後の期間（通常は 90 日）が過ぎると完全に削除されます。

CloudTrail 設定を構成する

CloudTrail コンソールの [設定] ページを使用して、設定を構成および確認できます CloudTrail 。

[設定] ページにアクセスするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. CloudTrailコンソールの左側のナビゲーションペインで [設定] を選択します。
3. 必要に応じて設定を確認して更新します。

   次の設定を使用できます。

   - 組織の委任管理者 — AWS Organizations 組織を運営している場合は、委任された管理者の表示、 CloudTrail 委任された管理者の追加 (最大 3 人)、委任された管理者の削除を行うことができます。委任された管理者を追加または削除できるのは、組織の管理アカウントだけです。

     組織の管理アカウントは、組織内の任意のアカウントに、 CloudTrail 組織に代わって組織のトレイルやイベントデータストアを管理する委任管理者として割り当てることができます。
   - サービスにリンクされたチャネル— 自分のアカウント用に作成されたサービスにリンクされたチャネルはすべて表示できます。

     AWS のサービス CloudTrail ユーザーに代わってイベントを受信するサービス連動チャンネルを作成できます。 AWS サービスにリンクされたチャンネルを作成するサービスは、チャンネルの高度なイベントセレクターを設定し、チャンネルを全員に適用するのか、単一のチャンネルに適用するのかを指定します。 AWS リージョン AWS リージョン

組織の委任された管理者

AWS Organizations 組織 CloudTrail で を使用する場合、組織内の任意のアカウントを割り当てて、組織に代わって組織の証跡とイベントデータストアを管理する CloudTrail 委任管理者として動作させることができます。委任された管理者は、 で CloudTrail 管理アカウントと同じ管理タスク (記載されている を除く) を実行できる組織のメンバーアカウントです。

委任された管理者を選択した場合、このメンバーアカウントには組織内のすべての組織の証跡とイベントデータストアに対する管理許可が付与されます。委任された管理者を追加しても、組織の証跡やイベントデータストアの管理やオペレーションが変更されることはありません。

CloudTrail コンソールで、または AWS CLI または CloudTrail API を使用して、委任された管理者を初めて追加すると、 は組織の管理アカウントにサービスにリンクされたロールがあるかどうか CloudTrail をチェックします。管理アカウントにサービスにリンクされたロールがない場合、 は管理アカウントのサービスにリンクされたロール CloudTrail を作成します。サービスにリンクされたロールの詳細については、「サービスにリンクされたロールを使用する AWS CloudTrail」を参照してください。

> **Note**
>
> AWS Organizations CLI または API オペレーションを使用して委任管理者を追加すると、サービスにリンクされたロールが存在しない場合、作成されません。サービスにリンクされたロールは、コンソール AWS CLI 、または CloudTrail API を使用して委任された管理者を追加したり、組織の証跡やイベントデータストアを作成したりするなど CloudTrail 、管理アカウントから CloudTrail サービスに直接呼び出しを行った場合にのみ作成されます。

委任された管理者が でどのように動作するかを定義する以下の要素に注意してください CloudTrail。

管理アカウントは、委任された管理者が作成する CloudTrail 組織リソースの所有者のままです。

組織の管理アカウントは、証跡やイベントデータストアなど、委任管理者が作成する CloudTrail 組織リソースの所有者のままです。これにより、委任された管理者が変更された場合でも組織の継続性が保たれます。

委任された管理者アカウントを削除しても、作成した CloudTrail 組織リソースは削除されません。

委任された管理者によって作成された組織の証跡とイベントデータストアは、委任された管理者を削除しても削除されません。これは、委任された管理者によって作成されたか管理アカウントによって作成されたかに関係なく、管理アカウントが常に CloudTrail 組織リソースの所有者として機能するためです。

組織には、最大 3 人の CloudTrail 委任された管理者を設定できます。

組織ごとに最大 3 人の CloudTrail 委任管理者を持つことができます。委任された管理者の削除の詳細については、「 CloudTrail 委任された管理者を削除する」を参照してください。

次の表は、管理アカウント、委任管理者アカウント、および AWS Organizations 組織内のメンバーであるアカウントの機能を示しています。

機能	管理アカウント	委任された管理者アカウント	メンバーアカウント
委任された管理者アカウントの追加もしくは削除。	はい	いいえ	いいえ
組織の証跡の作成。	はい	あり [1]	いいえ
組織の証跡の一覧の表示。	はい	はい	はい
組織の証跡の更新。	はい	あり[1、 2]	いいえ
組織の証跡の削除。	はい	はい	いいえ
イベントまたは AWS Config 設定項目の組織 CloudTrail イベントデータストアを作成します。	はい	はい	いいえ
組織のイベントデータストアでの Insights の有効化。	はい	いいえ	いいえ
組織のイベントデータストアの更新。	はい	あり[2]	いいえ
組織イベントデータストアでの Lake クエリフェデレーションの有効化 [3]。	はい	はい	いいえ
組織のイベントデータストアでの Lake クエリフェデレーションの無効化。	はい	はい	いいえ
組織のイベントデータストアの削除。	はい	はい	いいえ
組織のイベントデータストアへの証跡イベントのコピー。	はい	いいえ	いいえ
組織のイベントデータストアでのクエリ実行。	はい	はい	いいえ

機能	管理アカウント	委任された管理者アカウント	メンバーアカウント
組織のイベントデータストアのための Lake ダッシュボードの表示。	はい	はい	いいえ

[1]委任管理者は、 AWS CLI または CloudTrail `CreateTrail` `UpdateTrail` API オペレーションを使用してのみ Logs CloudWatch ロググループを設定できます。Logs CloudWatch ロググループとログロールの両方が呼び出し元のアカウントに存在する必要があります。

[2]組織の証跡またはイベントデータストアをアカウントレベルの証跡またはイベントデータストアに変換したり、アカウントレベルの証跡またはイベントデータストアを組織の証跡またはイベントデータストアに変換したりできるのは、管理アカウントのみです。組織の証跡とイベントデータストアは管理アカウントにのみ存在するため、委任された管理者はこれらのアクションを実行できません。組織の証跡またはイベントデータストアがアカウントレベルの証跡またはイベントデータストアに変換されると、管理アカウントのみが証跡またはイベントデータストアにアクセスできます。

[3]組織のイベントデータストアでフェデレーションを有効にできるのは、委任された管理者アカウントの 1 つ、または管理アカウントだけです。他の委任管理者アカウントは、Lake Formation のデータ共有機能を使用すると、情報をクエリし共有することが可能です。組織の管理アカウントだけでなく委任された管理者アカウントも、フェデレーションを無効化することができます。

トピック

- 委任された管理者を割り当てるために必要な許可
- CloudTrail 委任された管理者を追加する
- CloudTrail 委任された管理者を削除する

委任された管理者を割り当てるために必要な許可

CloudTrail 委任された管理者を割り当てるときは、 で委任された管理者を追加および削除するアクセス許可に加えて CloudTrail、次のポリシーステートメントにリストされている特定の AWS Organizations API アクションと IAM アクセス許可が必要です。

IAM ポリシーの最後に次のステートメントを追加することで、これらの許可を付与できます。

```
{
```

```
    "Sid": "Permissions",
    "Effect": "Allow",
    "Action": [
        "cloudtrail:RegisterOrganizationDelegatedAdmin",
        "cloudtrail:DeregisterOrganizationDelegatedAdmin",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator",
        "organizations:ListAWSServiceAccessForOrganization",
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
    ],
    "Resource": "*"
}
```

CloudTrail 委任された管理者を追加する

委任された管理者を追加して、証跡やイベントデータストアなどの組織の CloudTrail リソースを管理できます。

CloudTrail コンソールまたは を使用して、組織の CloudTrail AWS 委任管理者を追加できます AWS CLI。

委任された管理者を追加するときは、事前に、その管理者がユーザーの組織のアカウントを持っていること、および、ユーザーが、自分の組織にその管理者のアカウントでサインインしていることを確認します。組織の新しい AWS アカウントを作成する方法については、「組織での AWS アカウントの作成」を参照してください。既存の AWS アカウントを組織に招待する方法については、「組織への AWS アカウントの招待」を参照してください。

CloudTrail console

次の手順では、コンソールを使用して CloudTrail 委任管理者を追加する方法を示します CloudTrail 。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. CloudTrail コンソールの左側のナビゲーションペインで 設定 を選択します。
3. [Organization delegated administrators] (組織委任管理者) セクションで、[Register administrator] (管理者を登録) を選択します。
4. 組織の証跡とイベントデータストアの CloudTrail 委任管理者として割り当てる AWS アカウントの 12 桁のアカウント ID を入力します。

5. [Register administrator] (管理者を登録) を選択します。

AWS CLI

次の例では、 CloudTrail 委任された管理者を追加します。

```
aws cloudtrail register-organization-delegated-admin
  --member-account-id="memberAccountId"
```

このコマンドは成功時に出力を生成しません。

CloudTrail 委任された管理者を削除する

CloudTrail コンソールまたは を使用して、 CloudTrail 委任された管理者を削除できます AWS CLI。

CloudTrail console

次の手順では、コンソールを使用して CloudTrail 委任された管理者を削除する方法を示します CloudTrail 。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. CloudTrail コンソールの左側のナビゲーションペインで 設定 を選択します。
3. [Organization delegated administrators] (組織委任管理者) セクションで、削除する委任された管理者を選択します。
4. [Remove administrator] (管理者を削除) を選択します。
5. 委任された管理者を削除することを確認し、[Remove administrator] (管理者を削除) を選択します。

AWS CLI

次のコマンドは、 CloudTrail 委任された管理者を削除します。

```
aws cloudtrail deregister-organization-delegated-admin
  --delegated-admin-account-id="delegatedAdminAccountId"
```

このコマンドは成功時に出力を生成しません。

サービスにリンクされたチャネル

AWS サービスはサービスにリンクされたチャンネルを作成して、 CloudTrail ユーザーに代わってイベントを受信できます。 AWS サービスにリンクされたチャンネルを作成するサービスは、チャンネルの高度なイベントセレクターを設定し、チャンネルを全員に適用するのか、それとも単独に適用するのかを指定します。 AWS リージョン AWS リージョン

トピック

- コンソールを使用してサービスにリンクされたチャネルを表示する
- を使用してサービスにリンクされたチャンネルを視聴する AWS CLI

コンソールを使用してサービスにリンクされたチャネルを表示する

CloudTrail コンソールを使用すると、 CloudTrail サービスによって作成されたサービスにリンクされたチャネルに関する情報を表示できます。 AWS アカウントにサービスにリンクされたチャネルがない場合、テーブルは空です。

サービスにリンクされたチャネルの情報を表示するには、以下の手順に従います。

1. コンソールの左側のナビゲーションペインで [設定] を選択します。 CloudTrail
2. [サービスにリンクされたチャネル] から、サービスにリンクされたチャネルを選択して詳細を表示します。
3. [詳細] ページで、サービスにリンクされたチャネルの設定を確認します。

   [詳細] ページでは、次の情報を表示できます。

   - チャネル名 - チャネルのフルネーム。チャンネル名形式は`aws-service-channel/`*`AWS_service_name`*`/slc`、*`AWS_service_name`* AWS チャンネルを管理するサービスの名前を表します。
   - チャネル ARN - チャネルの ARN。これを API リクエストで使用するとチャネルの詳細を取得できます。
   - すべてのリージョン - チャネルがすべての AWS リージョンに対応するように設定されている場合、値は `Yes` です。
   - AWS service- AWS チャンネルを管理するサービスの名前。
   - 管理イベント - チャネルに設定されている管理イベントをすべて表示します。
   - データイベント - チャネルに設定されているデータイベントをすべて表示します。

を使用してサービスにリンクされたチャンネルを視聴する AWS CLI

を使用すると AWS CLI、 CloudTrail サービスによって作成されたすべてのサービスにリンクされたチャネルに関する情報を表示できます。 AWS

トピック

- サービスにリンクされたチャンネルを取得しましょう。 CloudTrail
- CloudTrail サービスにリンクされたチャンネルをすべて一覧表示します。
- AWS サービスにリンクされたチャネルのサービスイベント

サービスにリンクされたチャンネルを取得しましょう。 CloudTrail

AWS CLI 以下のコマンド例は、宛先サービスの名前、そのチャンネルに設定されているアドバンスセレクター、チャンネルがすべてのリージョンに適用されるのか、単一のリージョンに適用されるのかなど、 CloudTrail AWS 特定のサービスにリンクされたチャンネルに関する情報を返します。

`--channel` には、ARN、または ARN の ID サフィックスを指定する必要があります。

```
aws cloudtrail get-channel --channel EXAMPLE-ee54-4813-92d5-999aeEXAMPLE
```

以下に、応答の例を示します。この例では、`AWS_service_name` AWS はチャネルを作成したサービスの名前を表しています。

```
{
    "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
    "Name": "aws-service-channel/AWS_service_name/slc",
    "Source": "CloudTrail",
    "SourceConfig": {
        "ApplyToAllRegions": false,
        "AdvancedEventSelectors": [
            {
                "Name": "Management Events Only",
                "FieldSelectors": [
                    {
                        "Field": "eventCategory",
                        "Equals": [
                            "Management"
```

```
                        ]
                    }
                ]
            }
        ]
    },
    "Destinations": [
        {
            "Type": "AWS_SERVICE",
            "Location": "AWS_service_name"
        }
    ]
}
```

CloudTrail サービスにリンクされたチャンネルをすべて一覧表示します。

AWS CLI 以下のコマンド例は、 CloudTrail ユーザーに代わって作成されたすべてのサービスにリンクされたチャンネルに関する情報を返します。オプションのパラメータには、コマンドが単一のページに返す結果の最大数を指定する `--max-results` が含まれます。指定した `--max-results` 値よりも多くの結果がある場合は、返された `NextToken` 値を追加してコマンドを再度実行し、結果の次のページを取得します。

```
aws cloudtrail list-channels
```

以下に、応答の例を示します。この例では、`AWS_service_name` AWS はチャンネルを作成したサービスの名前を表しています。

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

AWS サービスにリンクされたチャネルのサービスイベント

AWS サービスにリンクされたチャネルを管理するサービスは、サービスにリンクされたチャネル上でアクション (たとえば、サービスにリンクされたチャネルの作成や更新) を開始できます。CloudTrail AWS これらのアクションをサービスイベントとして記録し、イベント履歴、管理イベント用に設定されたアクティブなトレイル、イベントデータストアに配信します。これらのイベントの場合、eventType フィールドは AwsServiceEvent です。

以下は、 AWS サービスにリンクされたチャネルを作成するためのサービスイベントのログファイルエントリの例です。

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "accountId":"111122223333",
      "invokedBy":"AWS Internal"
   },
   "eventTime":"2022-08-18T17:11:22Z",
   "eventSource":"cloudtrail.amazonaws.com",
   "eventName":"CreateServiceLinkedChannel",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"AWS Internal",
   "requestParameters":null,
   "responseElements":null,
   "requestID":"564f004c-EXAMPLE",
   "eventID":"234f004b-EXAMPLE",
   "readOnly":false,
   "resources":[
      {
         "accountId":"184434908391",
         "type":"AWS::CloudTrail::Channel",
         "ARN":"arn:aws:cloudtrail:us-east-1:111122223333:channel/7944f0ec-EXAMPLE"
      }
   ],
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "recipientAccountId":"111122223333",
   "eventCategory":"Management"
}
```

CloudTrail イベントについて

のイベント CloudTrail は、 AWS アカウント内のアクティビティの記録です。このアクティビティは、IAM アイデンティティによって実行されたアクション、または によってモニタリング可能なサービスにすることができます CloudTrail。 CloudTrail イベントは、、 SDK AWS Management Console、コマンドラインツール、およびその他の を通じて行われた API と非 API アカウントアクティビティの両方の履歴を提供します AWS のサービス。 AWS SDKs

CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序では表示されません。

CloudTrail イベントには 3 つのタイプがあります。

- 管理イベント
- データイベント
- Insights イベント

デフォルトでは、証跡とイベントデータストアは管理イベントをログ記録しますが、データイベントまたは Insights イベントは記録しません。

すべてのイベントタイプは CloudTrail JSON ログ形式を使用します。ログには、リクエストを行った人、使用されたサービス、実行されたアクション、アクションのパラメータなど、アカウントのリソースに対するリクエストに関する情報が含まれています。イベントデータが `Records` の配列で囲まれています。

CloudTrail イベントレコードフィールドの詳細については、「」を参照してくださいCloudTrail レコードの内容。

管理イベント

管理イベントは、 AWS アカウントのリソースで実行される管理オペレーションに関する情報を提供します。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。管理イベントには、次のようなものがあります。

- セキュリティの設定 (API AWS Identity and Access Management `AttachRolePolicy`オペレーションなど) 。

- デバイスの登録 (例: Amazon EC2 `CreateDefaultVpc` API オペレーション)。
- データをルーティングするルールの設定 (例: Amazon EC2 `CreateSubnet` API オペレーション)。
- ログ記録の設定 (API AWS CloudTrail `CreateTrail`オペレーションなど) 。

管理イベントは、アカウントで発生する非 API イベントを含む場合もあります。例えば、ユーザーがアカウントにサインインすると、 はConsoleLoginイベントを CloudTrail ログに記録します。詳細については、「によってキャプチャされた非APIイベント CloudTrail」を参照してください。AWS サービスの CloudTrail ログ記録を行う管理イベントのリストについては、「」を参照してくださいCloudTrail がサポートするサービスと統合。

次の例は、管理イベントの単一のログレコードを示しています。このイベントでは、 という名前の IAM `Mary_Major` ユーザーが aws cloudtrail start-logging コマンドを実行して CloudTrail `StartLogging`アクションを呼び出し、 という名前の証跡でログ記録プロセスを開始しましたmyTrail。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary_Major",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:33:41Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartLogging",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-logging",
    "requestParameters": {
```

```
        "name": "myTrail"
    },
    "responseElements": null,
    "requestID": "9d478fc1-4f10-490f-a26b-EXAMPLE0e932",
    "eventID": "eae87c48-d421-4626-94f5-EXAMPLEac994",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

次の例では、Paulo_Santos という名前の IAM ユーザーが aws cloudtrail start-event-data-store-ingestion コマンドを実行し、StartEventDataStoreIngestion アクションを呼び出し、イベントデータストア上で取り込みを開始しました。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLEPHCNW5EQV7NA54",
        "arn": "arn:aws:iam::123456789012:user/Paulo_Santos",
        "accountId": "123456789012",
        "accessKeyId": "(AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo_Santos",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-21T21:55:30Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-21T21:57:28Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "StartEventDataStoreIngestion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.1 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.start-event-data-
store-ingestion",
    "requestParameters": {
        "eventDataStore": "arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/2a8f2138-0caa-46c8-a194-EXAMPLE87d41"
    },
    "responseElements": null,
    "requestID": "f62a3494-ba4e-49ee-8e27-EXAMPLE4253f",
    "eventID": "d97ca7e2-04fe-45b4-882d-EXAMPLEa9b2c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


データイベント

データイベントでは、リソース上またはリソース内で実行されたリソースオペレーションについての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。

データイベントには、次のようなものがあります。

- S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (GetObject、DeleteObject、および PutObject API オペレーションなど) 。 S3
- AWS Lambda 関数実行アクティビティ (InvokeAPI)。
- CloudTrail PutAuditEvents 外部からのイベントを口グに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。
- トピックに関する Amazon SNS Publish および PublishBatch API オペレーション。

証跡およびイベントデータストアで使用できるデータイベントタイプは、以下の表のとおりです。[データイベントタイプ (コンソール)] 列には、コンソールで有効な選択項目が表示されま

す。resources.type 値列には、 AWS CLI または CloudTrail APIs を使用して証跡またはイベントデータストアにそのタイプのデータイベントを含めるように指定するresources.type値が表示されます。

証跡では、基本イベントセレクタまたはアドバンストイベントセレクタを使用して、Amazon S3 オブジェクト、Lambda 関数、DynamoDB テーブル (テーブルの最初の 3 行に表示) のデータイベントを ログ記録できます。残りの行に表示されるデータイベントタイプを ログに記録するには、高度イベントセレクタのみを使用できます。

イベントデータストアの場合、データイベントを含めるには、詳細イベントセレクタのみを使用できます。

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon DynamoDB	テーブルに対する Amazon DynamoDB 項目レベルの API アクティビティ (、DeleteItem 、および UpdateItem API PutItemオペレーションなど)。 **Note** ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と	DynamoDB	AWS::DynamoDB::Table

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	`AWS::DynamoDB::Table` の両方が含まれます。`resources.type` に `AWS::DynamoDB::Table` を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方がログ記録されます。ストリームイベント を除外するには、`eventName` フィールドにフィルターを追加します。		
AWS Lambda	AWS Lambda 関数実行アクティビティ (InvokeAPI)。	Lambda	`AWS::Lambda::Function`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon S3	S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (GetObject 、DeleteObject 、および PutObject API オペレーションなど)。S3	S3	AWS::S3::Object
AWS AppConfig	StartConfiguration Session および への呼び出しなどの設定オペレーションの AWS AppConfig API アクティビティGetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration
AWS B2B データ交換	GetTransformerJob および StartTransformerJob の呼び出しなど、Transformer 操作用の B2B データ交換 API アクティビティ。	B2B データ交換	AWS::B2BI::Transformer

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Bedrock	エージェントエイリアスでの Amazon Bedrock API アクティビティ。	Bedrock エージェントエイリアス	`AWS::Bedrock::AgentAlias`
	ナレッジベースでの Amazon Bedrock API アクティビティ。	Bedrock ナレッジベース	`AWS::Bedrock::KnowledgeBase`
Amazon CloudFront	CloudFront での API アクティビティKeyValueStore。	CloudFront KeyValueStore	`AWS::CloudFront::KeyValueStore`
AWS Cloud Map	名前空間 での AWS Cloud Map API アクティビティ。	AWS Cloud Map 名前空間	`AWS::ServiceDiscovery::Namespace`
	サービス での AWS Cloud Map API アクティビティ。	AWS Cloud Map service	`AWS::ServiceDiscovery::Service`
AWS CloudTrail	CloudTrail `PutAuditEvents` 外部からのイベントを ログに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。	CloudTrail チャンネル	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	カスタマイズに対する Amazon CodeWhisperer API アクティビティ。	CodeWhisperer カスタマイズ	`AWS::CodeWhisperer::Customization`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	プロファイルの Amazon CodeWhisperer API アクティビティ。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito アイデンティティプール に対する Amazon Cognito API アクティビティ。	Cognito アイデンティティプール	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	ストリームに対する Amazon DynamoDB API アクティビティ	DynamoDB Streams	`AWS::DynamoDB::Stream`
Amazon Elastic Block Store	Amazon EBS スナップショットの `PutSnapshotBlock` 、`GetSnapshotBlock` 、および `ListChangedBlocks` などの Amazon Elastic Block Store (EBS) ダイレクト API。	Amazon EBS ダイレクト API	`AWS::EC2::Snapshot`
Amazon EMR	ログ先行書き込みワークスペースでの Amazon EMR API アクティビティ。	EMR ログ先行書き込みワークスペース	`AWS::EMRWAL::Workspace`
Amazon FinSpace	環境に対する Amazon FinSpace API アクティビティ。	FinSpace	`AWS::FinSpace::Environment`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS Glue	AWS Glue Lake Formation によって作成されたテーブルに対する API アクティビティ。 **Note** AWS Glue テーブルのデータイベントは現在、次のリージョンでのみサポートされています。 • 米国東部 (バージニア北部) • 米国東部 (オハイオ) • 米国西部 (オレゴン) • 欧州 (アイルランド) • アジアパシフィック (東京) リージョン	Lake Formation	`AWS::Glue::Table`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon GuardDuty	ディテクター の Amazon GuardDuty API アクティビティ。https://docs.aws.amazon.com/guardduty/latest/ug/logging-using-cloudtrail.html#guardduty-data-events-in-cloudtrail	GuardDuty ディテクター	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging データストアでの API アクティビティ。	医療用画像データストア	`AWS::MedicalImaging::Datastore`
AWS IoT	証明書 に対する AWS IoT API アクティビティ。	IoT 証明書	`AWS::IoT::Certificate`
	モノに対する AWS IoT API アクティビティ。	IoT モノ	`AWS::IoT::Thing`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS IoT Greengrass Version 2	コンポーネントバージョンの Greengrass コアデバイスからの Greengrass API アクティビティ。 Note Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass コンポーネントバージョン	`AWS::GreengrassV2::ComponentVersion`
	デプロイ上の Greengrass コアデバイスからの Greengrass API アクティビティ。 Note Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass デプロイ	`AWS::GreengrassV2::Deployment`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS IoT SiteWise	アセット での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_CreateAsset.html	IoT SiteWise アセット	`AWS::IoTSiteWise::Asset`
	時系列 での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_DescribeTimeSeries.html	IoT SiteWise 時系列	`AWS::IoTSiteWise::TimeSeries`
AWS IoT TwinMaker	エンティティ での IoT TwinMaker API アクティビティ。 https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateEntity.html	IoT TwinMaker エンティティ	`AWS::IoTTwinMaker::Entity`
	ワークスペース での IoT TwinMaker API アクティビティ。 https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateWorkspace.html	IoT TwinMaker ワークスペース	`AWS::IoTTwinMaker::Workspace`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Kendra インテリジェントランキング	リスコア実行プラン に対する Amazon Kendra Intelligent Ranking API アクティビティ。	Kendra ランキング	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra 向け)	テーブルでの Amazon Keyspaces API アクティビティ。	Cassandra テーブル	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	ストリーム での Kinesis Data Streams API アクティビティ。	Kinesis ストリーム	`AWS::Kinesis::Stream`
	ストリームコンシューマー での Kinesis Data Streams API アクティビティ。	Kinesis ストリームコンシューマー	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	`GetMedia` や への呼び出しなど、ビデオストリーム での Kinesis Video Streams API アクティビティ`PutMedia`。	Kinesis ビデオストリーム	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	ネットワーク上の Amazon Managed Blockchain API アクティビティ。	Managed Blockchain ネットワーク	`AWS::ManagedBlockchain::Network`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	`eth_getBalance` や `eth_getBlockByNumber` などの Ethereum ノードに対する Amazon Managed Blockchain JSON-RPC コール。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune Graph	Neptune Graph でのクエリ、アルゴリズム、ベクトル検索などのデータ API アクティビティ。	Neptune Graph	`AWS::NeptuneGraph::Graph`
AWS Private CA	AWS Private CA Connector for Active Directory API アクティビティ。	AWS Private CA Connector for Active Directory	`AWS::PCAConnectorAD::Connector`
Amazon Q アプリ	Amazon Q Apps での Data API アクティビティ。	Amazon Q アプリ	`AWS::QApps:QApp`
Amazon Q Business	アプリケーション上の Amazon Q Business API アクティビティ。	Amazon Q Business アプリケーション	`AWS::QBusiness::Application`
	データソース上の Amazon Q Business API アクティビティ。	Amazon Q Business データソース	`AWS::QBusiness::DataSource`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	インデックスでの Amazon Q Business API アクティビティ。	Amazon Q Business インデックス	`AWS::QBusiness::Index`
	ウェブエクスペリエンスでの Amazon Q Business API アクティビティ。	Amazon Q Business ウェブエクスペリエンス	`AWS::QBusiness::WebExperience`
Amazon RDS	DB クラスターでの Amazon RDS API アクティビティ。	RDS Data API - DB クラスター	`AWS::RDS::DBCluster`
Amazon S3	アクセスポイントでの Amazon S3 API アクティビティ。	S3 アクセスポイント	`AWS::S3::AccessPoint`
	Amazon S3 Object Lambda アクセスポイント API アクティビティ 、 `CompleteMultipartUpload` や への呼び出しなど`GetObject` 。	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts オブジェクトレベル API アクティビティ。	S3 Outposts	`AWS::S3Outposts::Object`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon SageMaker	エンドポイントでの Amazon SageMaker InvokeEndpointWithResponseStream アクティビティ。	SageMaker エンドポイント	AWS::SageMaker::Endpoint
	特徴量ストアでの Amazon SageMaker API アクティビティ。	SageMaker 特徴量ストア	AWS::SageMaker::FeatureGroup
	実験トライアルコンポーネント での Amazon SageMaker API アクティビティ。https://docs.aws.amazon.com/sagemaker/latest/dg/experiments-monitoring.html	SageMaker メトリクス実験トライアルコンポーネント	AWS::SageMaker::ExperimentTrialComponent
Amazon SNS	プラットフォームエンドポイントでの Amazon SNS Publish API オペレーション。	SNS プラットフォームエンドポイント	AWS::SNS::PlatformEndpoint
	トピックに関する Amazon SNS Publish および PublishBatch API オペレーション。	SNS トピック	AWS::SNS::Topic

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon SQS	メッセージでの Amazon SQS API アクティビティ。	SQS	`AWS::SQS::Queue`
AWS Step Functions	ステートマシンでの Step Functions API アクティビティ。	Step Functions ステートマシン	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain インスタンスでの API アクティビティ。	サプライチェーン	`AWS::SCN::Instance`
Amazon SWF	ドメイン での Amazon SWF API アクティビティ。 https://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dev-domains.html	SWF ドメイン	`AWS::SWF::Domain`
AWS Systems Manager	コントロールチャネルでの Systems Manager API アクティビティ。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	マネージドノードでの Systems Manager API アクティビティ。	Systems Manager マネージドノード	`AWS::SSM::ManagedNode`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Timestream	データベース上の Amazon Timestream Query API アクティビティ。	Timestream データベース	AWS::Timestream::Database
	テーブル上の Amazon Timestream Query API アクティビティ。	Timestream テーブル	AWS::Timestream::Table
Amazon Verified Permissions	ポリシーストア上の Amazon Verified Permissions API アクティビティ。	Amazon Verified Permissions	AWS::VerifiedPermissions::PolicyStore
Amazon WorkSpaces シンクライアント	WorkSpaces デバイス上のシンクライアント API アクティビティ。	シンクライアントデバイス	AWS::ThinClient::Device
	WorkSpaces 環境でのシンクライアント API アクティビティ。	シンクライアント環境	AWS::ThinClient::Environment
AWS X-Ray	トレース での X-Ray API アクティビティ。	X-Ray トレース	AWS::XRay::Trace

証跡またはイベントデータストアの作成時、デフォルトでは、データイベントは記録されません。CloudTrail データイベントを記録するには、アクティビティを収集するサポートされているリソースまたはリソースタイプを明示的に追加する必要があります。詳細については、「証跡の作成」および「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。

データイベントの口グ記録には追加料金が適用されます。 CloudTrail 料金については、「 AWS CloudTrail の料金」を参照してください。

次の例は、Amazon SNS Publishアクションのデータイベントの単一のログレコードを示しています。


```
{
   "eventVersion": "1.09",
   "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Bob",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AKIAIOSFODNN7EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "ExampleUser"
            },
            "attributes": {
                "creationDate": "2023-08-21T16:44:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-08-21T16:48:37Z",
    "eventSource": "sns.amazonaws.com",
    "eventName": "Publish",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/1.29.16 md/Botocore#1.31.16 ua/2.0 os/
linux#5.4.250-173.369.amzn2int.x86_64 md/arch#x86_64 lang/python#3.8.17 md/
pyimpl#CPython cfg/retry-mode#legacy botocore/1.31.16",
    "requestParameters": {
        "topicArn": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic",
        "message": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "subject": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "messageStructure": "json",
        "messageAttributes": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "responseElements": {
        "messageId": "0787cd1e-d92b-521c-a8b4-90434e8ef840"
    },
```

```
    "requestID": "0a8ab208-11bf-5e01-bd2d-ef55861b545d",
    "eventID": "bb3496d4-5252-4660-9c28-3c6aebdb21c0",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::SNS::Topic",
                "ARN": "arn:aws:sns:us-east-1:123456789012:ExampleSNSTopic"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "sns.us-east-1.amazonaws.com"
    }
}
```

次の例は、Amazon Cognito GetCredentialsForIdentityアクションのデータイベントの単一のログレコードを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-01-19T16:55:08Z",
    "eventSource": "cognito-identity.amazonaws.com",
    "eventName": "GetCredentialsForIdentity",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.4",
    "userAgent": "aws-cli/2.7.25 Python/3.9.11 Darwin/21.6.0 exe/x86_64 prompt/off
 command/cognito-identity.get-credentials-for-identity",
    "requestParameters": {
        "logins": {
            "cognito-idp.us-east-1.amazonaws.com/us-east-1_aaaaaaaaa":
 "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "responseElements": {
        "credentials": {
```

```
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "sessionToken": "aAaAaAaAaAaAab1111111111EXAMPLE",
            "expiration": "Jan 19, 2023 5:55:08 PM"
        },
        "identityId": "us-east-1:1cf667a2-49a6-454b-9e45-23199EXAMPLE"
    },
    "requestID": "659dfc23-7c4e-4e7c-858a-1abce884d645",
    "eventID": "6ad1c766-5a41-4b28-b5ca-e223ccb00f0d",
    "readOnly": false,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::Cognito::IdentityPool",
        "ARN": "arn:aws:cognito-identity:us-east-1:111122223333:identitypool/us-
east-1:2dg778b3-50b7-565c-0f56-34200EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111122223333",
    "eventCategory": "Data"
}
```


Insights イベント

CloudTrail Insights イベントは、 CloudTrail 管理アクティビティを分析することで、アカウント内の異常な API コールレートまたはエラーレートのアクティビティをキャプチャします AWS 。Insights イベントは、関連する API、エラーコード、インシデント時間、統計情報などの関連情報を提供し、異常なアクティビティについて理解して対処するのに役立ちます。 CloudTrail 証跡またはイベントデータストアでキャプチャされた他のタイプのイベントとは異なり、Insights イベントは、 がアカウントの API 使用量またはエラー率のログ記録で、アカウントの一般的な使用パターンと大きく異なる変更 CloudTrail を検出した場合にのみログに記録されます。

Insights イベントを生成する可能性のあるアクティビティの例を次に示します。

- 通常、アカウントは Amazon S3 `deleteBucket` API コールを 1 分あたり 20 個までログに記録しますが、アカウントは 1 分あたり平均 100 個の `deleteBucket` API コールを開始しています。異常なアクティビティの開始時に Insights イベントが記録され、異常なアクティビティの終了を示すために別の Insights イベントが記録されます。
- 通常、アカウントは Amazon EC2 `AuthorizeSecurityGroupIngress` API のコールを 1 分あたり 20 個を記録しますが、アカウントは `AuthorizeSecurityGroupIngress` へのコールをまったく記録し始めていません。異常なアクティビティの開始時に Insights イベントが記録さ

れ、10 分後、以上にアクティビティが終了すると、異常なアクティビティの終了を示すために別の Insights イベントが記録されます。

- 通常は、アカウントで AWS Identity and Access Management API `DeleteInstanceProfile` に関する `AccessDeniedException` エラーのログ記録が 7 日間に 1 つもありません。アカウントが `DeleteInstanceProfile` API コールで 1 分あたり平均 12 `AccessDeniedException` エラーのログを記録し始めます。異常なエラーレートのアクティビティが発生した時に Insights イベントが記録されますが、この異常アクティビティの終了を示すために別の Insights イベントも記録されます。

これらの例は、説明のみを目的としています。結果はユースケースによって異なる場合があります。

CloudTrail Insights イベントをログに記録するには、新規または既存の証跡またはイベントデータストアで Insights イベントを明示的に有効にする必要があります。証跡の作成方法の詳細については、「証跡の作成」を参照してください。イベントデータストアの作成方法の詳細については、「コンソールを使用して CloudTrail Insights イベントのイベントデータストアを作成する」を参照してください。

Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail Insights で異常なアクティビティを表示するためにログに記録されるイベントは、開始イベントと終了イベントの 2 つです。次の例は、アプリケーション Auto Scaling API `CompleteLifecycleAction` が異常な回数呼び出されたときに発生した開始インサイトイベントの 1 つのログレコードを示しています。インサイトイベントの場合、`eventCategory` の値は `Insight` です。`insightDetails` ブロックは、イベントの状態、ソース、名前、インサイトのタイプ、および統計情報および属性を含むコンテキストを識別します。`insightDetails` ブロックの詳細については、「CloudTrail `insightDetails`インサイト要素」を参照してください。


```
{
        "eventVersion": "1.08",
        "eventTime": "2023-07-10T01:42:00Z",
        "awsRegion": "us-east-1",
        "eventID": "55ed45c5-0b0c-4228-9fe5-EXAMPLEc3f4d",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "979c82fe-14d4-4e4c-aa01-EXAMPLE3acee",
        "insightDetails": {
            "state": "Start",
```

```
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 9.82222E-5
                    },
                    "insight": {
                        "average": 5.0
                    },
                    "insightDuration": 1,
                    "baselineDuration": 10181
                },
                "attributions": [{
                    "attribute": "userIdentityArn",
                    "insight": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole2",
                        "average": 5.0
                    }, {
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole3",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "arn:aws:sts::123456789012:assumed-role/
CodeDeployRole1",
                        "average": 9.82222E-5
                    }]
                }, {
                    "attribute": "userAgent",
                    "insight": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "codedeploy.amazonaws.com",
                        "average": 9.82222E-5
                    }]
```

```
                }, {
                    "attribute": "errorCode",
                    "insight": [{
                        "value": "null",
                        "average": 5.0
                    }],
                    "baseline": [{
                        "value": "null",
                        "average": 9.82222E-5
                    }]
                }]
            }
        },
        "eventCategory": "Insight"
    }
```

管理イベントのログ記録

デフォルトでは、証跡とイベントデータストアは管理イベントをログ記録し、データイベントや Insights イベントは記録しません。

データイベントや Insights イベントには追加料金が適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

目次

管理イベント

管理イベントは、 AWS アカウント内のリソースに対して実行される管理操作を可視化します。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。管理イベントには、次のようなものがあります。

- セキュリティの設定 (例: IAM `AttachRolePolicy` API オペレーション)。
- デバイスの登録 (例: Amazon EC2 `CreateDefaultVpc` API オペレーション)。
- データをルーティングするルールの設定 (例: Amazon EC2 `CreateSubnet` API オペレーション)。
- ロギングの設定 (AWS CloudTrail `CreateTrail`API 操作など)

管理イベントは、アカウントで発生する非 API イベントを含む場合もあります。たとえば、ユーザーがアカウントにログインすると、 CloudTrail `ConsoleLogin`イベントが記録されます。詳細については、「によってキャプチャされた非APIイベント CloudTrail」を参照してください。

デフォルトでは、証跡とイベントデータストアは管理イベントをログに記録するように設定されます。

> **Note**
>
> CloudTrail イベント履歴機能は管理イベントのみをサポートします。Amazon RDS Data API AWS KMS イベントをイベント履歴から除外したり、Amazon RDS Data API イベントを除外したりすることはできません。トレイルまたはイベントデータストアに適用した設定は、イベント履歴には適用されません。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。

による管理イベントのロギング AWS Management Console

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. 証跡を更新するには、 CloudTrail コンソールの Trails ページを開いて証跡名を選択します。

   イベントデータストアを更新するには、 CloudTrail コンソールのイベントデータストアページを開き、イベントデータストア名を選択します。
3. [Management events] (管理イベント) で、[Edit] (編集) を選択します。

- 証跡またはイベントデータストアで記録する対象を [読み取り] イベント、[書き込み] イベント、またはその両方を選択します。
- [Exclude AWS KMS events] を選択すると、トレイルまたはイベントデータストアからイベントを除外する AWS Key Management Service (AWS KMS) ことができます。デフォルトの設定では、 AWS KMS すべてのイベントが含まれます。

  AWS KMS イベントを口グに記録または除外するオプションは、管理イベントをトレイルまたはイベントデータストアに記録する場合にのみ使用できます。管理イベントを口グに記録しないことを選択した場合、 AWS KMS イベントは記録されず、 AWS KMS イベントログ設定を変更することもできません。

  AWS KMS `Encrypt`、などのアクションでは`Decrypt`、`GenerateDataKey`通常、大量 (99% 以上) のイベントが生成されます。これらのアクションは、[読み取り] イベントとして口グに記録されるようになりました。、**`DisableDelete`**、 AWS KMS などのボリュームの少ない関連アクション**`ScheduleKey`** (通常はイベント量の 0.5% 未満) は、 AWS KMS 書き込みイベントとして記録されます。

  、、などの大量のイベントを除外し**`EncryptDecrypt`**、**`GenerateDataKey`**、などの関連イベントは引き続き記録するには**`Disable`**、**`Delete`**書き込み管理イベントを口グに記録することを選択し、[除外イベント] のチェックボックスをオフにします。**`ScheduleKey`** AWS KMS
- [Amazon RDS Data API イベントを除外する] を選択して、証跡またはイベントデータストアから Amazon Relational Database Service データ API イベントを除外できます。デフォルト設定では、すべての Amazon RDS Data API イベントが含まれています。Amazon RDS Data API イベントの詳細については、「Aurora の　Amazon RDS Amazon RDS ユーザーガイド」の「AWS CloudTrailによる Data API コールの口グ記録」を参照してください。

4. 完了したら、[Save changes] (変更の保存) を選択します。

読み取りおよび書き込みイベント

管理イベントを口グに記録するように証跡またはイベントデータストアを設定するときは、読み取り専用イベントまたは書き込み専用イベントのどちらか一方のみまたは両方を指定できます。

- 読み込み

  読み取り専用イベントには、リソースの読み取りのみ行い、変更を行わない API オペレーションが含まれます。例えば、Amazon EC2 の `DescribeSecurityGroups` および

DescribeSubnets API オペレーションは読み取り専用イベントです。これらのオペレーションは、Amazon EC2 リソースに関する情報のみを返し、設定は変更しません。

- 書き込み

  書き込み専用イベントには、リソースを変更する (または変更する可能性がある) API オペレーションが含まれます。例えば、Amazon EC2 の RunInstances および TerminateInstances API オペレーションはインスタンスを変更します。

例: 読み取りイベントと書き込みイベントを別の証跡に記録する

次の例では、アカウントに対するログアクティビティを異なる S3 バケットに分けるように証跡を設定する方法を示します。1 つのバケットは読み取り専用イベントを受け取り、もう 1 つのバケットは書き込み専用イベントを受け取ります。

1. 証跡を作成し、ログファイルを受け取る read-only-bucket という名前の S3 バケットを選択します。次に、証跡を更新し、[読み取り] 管理イベントを記録するように指定します。
2. 第 2 の証跡を作成し、ログファイルを受け取る write-only-bucket という名前の S3 バケットを選択します。次に、証跡を更新し、書き込み管理イベントを記録するように指定します。
3. Amazon EC2 の DescribeInstances および TerminateInstances API オペレーションがアカウントで発生します。
4. DescribeInstances API オペレーションは読み取り専用イベントであり、1 番目の証跡の設定と一致します。証跡は、イベントをログに記録して read-only-bucket に配信します。
5. TerminateInstances API オペレーションは書き込み専用イベントであり、2 番目の証跡の設定と一致します。証跡は、イベントをログに記録して write-only-bucket に配信します。

AWS Command Line Interfaceを使用してイベントのログを記録する

AWS CLIを使用して、管理イベントのログを記録するように証跡またはイベントデータストアを設定できます。

トピック

- 例 : 証跡での管理イベントの記録
- 例: イベントデータストアの管理イベントのログ記録

例：証跡での管理イベントの記録

証跡が管理イベントをログに記録しているかどうかを確認するには、get-event-selectors コマンドを実行します。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

次の例では、証跡のデフォルト設定が返されます。デフォルトでは、証跡はすべての管理イベントをログに記録して、すべてのイベントソースからイベントをログに記録し、データイベントはログに記録しません。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ]
}
```

基本イベントセレクターと詳細イベントセレクターのどちらかを使用して管理イベントをログに記録できます。イベントセレクタと高度なイベントセレクタの両方を証跡に適用することはできません。高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。以下のセクションでは、高度なイベントセレクターと基本的なイベントセレクターを使用して管理イベントを記録する方法の例を示します。

トピック

- 例:高度なイベントセレクターを使用してトレイルの管理イベントをロギングする
- 例:基本的なイベントセレクターを使用してトレイルの管理イベントをロギングする

例:高度なイベントセレクターを使用してトレイルの管理イベントを口ギングする

次の例では、(セレクターを省略) *TrailName*readOnly読み取り専用および書き込み専用の管理イベントを含めるように名前を付けたトレイル用の高度なイベントセレクターを作成しますが、exclude () イベントは含めません。 AWS Key Management Service AWS KMS AWS KMS イベントは管理イベントとして扱われ、大量に発生する可能性があるため、管理イベントをキャプチャする証跡が複数あると、 CloudTrail 請求額に大きな影響を与える可能性があります。

管理イベントをログに記録しないことを選択した場合、 AWS KMS イベントは記録されず、 AWS KMS イベントログ設定を変更することもできません。

AWS KMS トレイルへのイベントの口ギングを再開するには、eventSourceセレクターを削除してコマンドを再実行してください。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except KMS events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["kms.amazonaws.com"] }
    ]
  }
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except KMS events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "kms.amazonaws.com" ]
        }
      ]
```

```
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

除外されたイベントの証跡へのログ記録を再開するには、次のコマンドに示されるように、eventSource セレクタを削除します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

次の例では、(セレクターを省略) *TrailName*readOnly読み取り専用および書き込み専用の管理イベントを含むように命名されたトレイル用の高度なイベントセレクターを作成しますが、Amazon RDS Data API 管理イベントは除外します。Amazon RDS データ API 管理イベントを除外するには、eventSourceフィールドの文字列値に Amazon RDS データ API イベントソースを指定します。rdsdata.amazonaws.com

管理イベントをログに記録しないことを選択した場合、Amazon RDS データ API 管理イベントは記録されず、Amazon RDS データ API イベントのロギング設定を変更することはできません。

Amazon RDS Data API 管理イベントのトレイルへの記録を再開するには、eventSourceセレクターを削除して、コマンドをもう一度実行します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events except Amazon RDS Data API management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] },
      { "Field": "eventSource", "NotEquals": ["rdsdata.amazonaws.com"] }
    ]
  }
```

```
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log all management events except Amazon RDS Data API management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        },
        {
          "Field": "eventSource",
          "NotEquals": [ "rdsdata.amazonaws.com" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

除外されたイベントの証跡へのログ記録を再開するには、次のコマンドに示されるように、eventSource セレクタを削除します。

```
aws cloudtrail put-event-selectors --trail-name TrailName \
--advanced-event-selectors '
[
  {
    "Name": "Log all management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  }
]'
```

例:基本的なイベントセレクターを使用してトレイルの管理イベントを口ギングする

管理イベントをログに記録するように証跡を設定するには、put-event-selectors コマンドを実行します。次の例では、2 つの S3 オブジェクトに対するすべての管理イベントを含めるように証跡

を設定する方法を示します。1 つの証跡に 1~5 個のイベントセレクタを指定できます。1 つの証跡に 1~250 個のデータリソースを指定できます。

> **Note**
>
> イベントセレクタの数にかかわらず、S3 データリソースの最大数は 250 個です。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

次の例は、証跡に対して設定されているイベントセレクタを返します。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Type": "AWS::S3::Object",
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

証跡のログからイベントを除外 AWS Key Management Service (AWS KMS) するには、put-event-selectorsExcludeManagementEventSourcesコマンドを実行して値がの属性を追加します。kms.amazonaws.com次の例では、読み取り専用と書き込み専用の管理イベントを含むが、*TrailName*イベントは除外するようにという名前のトレイルのイベントセレクターを作成します。 AWS KMS AWS KMS は大量のイベントを生成できるため、この例のユーザーは記録のコストを管理するためにイベントを制限したいと思うかもしれません。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 ["kms.amazonaws.com"],"IncludeManagementEvents": true}]'
```

例では、証跡に対して設定されているイベントセレクタを返します。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "kms.amazonaws.com"
            ]
        }
    ]
}
```

Amazon RDS Data API 管理イベントをトレイルのログから除外するには、put-event-selectorsコマンドを実行して、ExcludeManagementEventSourcesrdsdata.amazonaws.com値がの属性を追加します。次の例では、読み取り専用と書き込み専用の管理イベントを含むが、Amazon RDS Data API TrailName管理イベントは除外するようにという名前のトレイルのイベントセレクターを作成します。Amazon RDS Data API は大量の管理イベントを生成する可能性があるため、この例のユーザーは証跡のコストを管理するためにイベントを制限したいと思うかもしれません。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "EventSelectors": [
        {
            "ReadWriteType": "All",
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ExcludeManagementEventSources": [
                "rdsdata.amazonaws.com"
            ]
        }
    ]
}
```

AWS KMS トレイルへの記録または Amazon RDS Data API 管理イベントの記録を再開するには、次のコマンドに示すようにExcludeManagementEventSources、の値として空の文字列を渡します。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "All","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

AWS KMS 関連イベントをDisable、、Deleteなどのトレイルに記録しScheduleKey、、、AWS KMS などの大量のイベントは除外するにはEncryptDecrypt、次の例に示すようにGenerateDataKey、書き込み専用の管理イベントを記録し、 AWS KMS デフォルト設定のままイベントをログに記録します。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-
selectors '[{"ReadWriteType": "WriteOnly","ExcludeManagementEventSources":
 [],"IncludeManagementEvents": true}]'
```

例: イベントデータストアの管理イベントのログ記録

イベントデータストアに管理イベントが含まれているかどうかを確認するには、get-event-data-store コマンドを実行します。

```
aws cloudtrail get-event-data-store
--event-data-store arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE
```

以下に、応答の例を示します。作成時刻と最終更新時刻は timestamp 形式です。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "myManagementEvents",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "FIXED_RETENTION_PRICING",
    "RetentionPeriod": 2557,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-04T15:56:27.418000+00:00",
    "UpdatedTimestamp": "2023-02-04T15:56:27.544000+00:00"
}
```

すべての管理イベントを含むイベントデータストアを作成するには、create-event-data-store コマンドを実行します。すべての管理イベントを含めるには、高度イベント セレクタを指定する必要はありません。

```
aws cloudtrail create-event-data-store
--name my-event-data-store
--retention-period 90\
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
```

```
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T16:41:57.224000+00:00",
    "UpdatedTimestamp": "2023-11-13T16:41:57.357000+00:00"
}
```

AWS Key Management Service (AWS KMS) イベントを除外するイベントデータストアを作成するには、create-event-data-storeコマンドを実行して the not equal と指定します。eventSource kms.amazonaws.com次の例では、読み取り専用と書き込み専用の管理イベントを含むが、イベントは除外するイベントデータストアを作成します。 AWS KMS

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["kms.amazonaws.com"]}
        ]
    }
]'
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
```

```
                    "Field": "eventSource",
                    "NotEquals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

Amazon RDS Data API 管理イベントを除外するイベントデータストアを作成するには、create-event-data-storeeventSourceコマンドを実行して等しくないことを指定します。rdsdata.amazonaws.com次の例では、読み取り専用管理イベントと書き込み専用管理イベントを含むが、Amazon RDS Data API イベントを除外するイベントデータストアを作成します。

```
aws cloudtrail create-event-data-store --name event-data-store-name --retention-period
 90 --advanced-event-selectors '[
    {
        "Name": "Management events selector",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventSource","NotEquals": ["rdsdata.amazonaws.com"]}
        ]
    }
]'
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "my-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
```

```
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventSource",
                    "NotEquals": [
                        "rdsdata.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2023-11-13T17:02:02.241000+00:00"
}
```

AWS SDK を使用してイベントのログを記録する

GetEventSelectorsオペレーションを使用して、トレイルがトレイルの管理イベントをログに記録しているかどうかを確認してください。PutEventSelectorsオペレーションで管理イベントをログに記録するようにトレイルを設定できます。詳細については、「APIリファレンスAWS CloudTrail」を参照してください。

GetEventDataStore操作を実行して、イベントデータストアに管理イベントが含まれているかどうかを確認します。CreateEventDataStoreUpdateEventDataStoreまたは操作を実行することで、イベントデータストアに管理イベントを含めるように設定できます。詳細については、「を使用して、イベントデータストアを作成、更新、管理します AWS CLI」および AWS CloudTrail API リファレンスを参照してください。

Amazon CloudWatch ログにイベントを送信する

トレイル用に、 CloudTrail CloudWatch ログへのデータおよび管理イベントの送信をサポートします。 CloudWatch Logs ロググループにイベントを送信するようにトレイルを設定すると、CloudTrail トレイルで指定したイベントのみが送信されます。たとえば、管理イベントのみを記録するようにトレイルを設定した場合、 CloudWatch トレイルは管理イベントをログロググループにのみ配信します。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

データイベントをログ記録する

このセクションでは、 CloudTrail コンソールと を使用してデータイベントをログに記録する方法について説明しますAWS CLI。

デフォルトでは、証跡とイベントデータストアはデータイベントを記録しません。追加の変更がイベントデータに適用されます。詳細については、「AWS CloudTrail の料金」を参照してください。

データイベントでは、リソース上またはリソース内で実行されたリソースオペレーションについて知ることができます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。

データイベントには、次のようなものがあります。

- S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (`GetObject`、`DeleteObject`、および `PutObject` API オペレーションなど)。 S3
- AWS Lambda 関数実行アクティビティ (`Invoke`API)。
- CloudTrail `PutAuditEvents` 外部からのイベントをログに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。
- トピックに関する Amazon SNS `Publish` および `PublishBatch` API オペレーション。

高度なイベントセレクタを使用してきめ細かなセレクタを作成できます。これにより、ユースケースの特定のイベントのみをログに記録することでコストを制御できます。例えば、高度なイベントセレクタを使用して、 `eventName`フィールドにフィルターを追加することで、特定の API コールをログに記録できます。詳細については、「高度なイベントセレクタを使用したデータイベントのフィルタリング」を参照してください。

> **Note**
>
> 証跡によってログに記録されるイベントは、Amazon で利用できます EventBridge。たとえば、管理イベントではなく、S3 オブジェクトのデータイベントを口グ記録するように選択した場合、証跡は指定された S3 オブジェクトのデータイベントのみを処理して記録します。これらの S3 オブジェクトのデータイベントは、Amazon で利用できます EventBridge。詳細については、「Amazon ユーザーガイド」の「 AWS のサービスからのイベント」を参照してください。 EventBridge

目次

データイベント

証跡およびイベントデータストアで使用できるデータイベントタイプは、以下の表のとおりです。[データイベントタイプ (コンソール)] 列には、コンソールで有効な選択項目が表示されます。resources.type 値列には、 AWS CLI または CloudTrail APIs を使用して証跡またはイベントデータストアにそのタイプのデータイベントを含めるように指定するresources.type値が表示されます。

証跡では、基本イベントセレクタまたはアドバンストイベントセレクタを使用して、Amazon S3 オブジェクト、Lambda 関数、DynamoDB テーブル (テーブルの最初の 3 行に表示) のデータイベントをログ記録できます。残りの行に表示されるデータイベントタイプをログに記録するには、高度イベントセレクタのみを使用できます。

イベントデータストアの場合、データイベントを含めるには、詳細イベントセレクタのみを使用できます。

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon DynamoDB	テーブルに対する Amazon DynamoDB 項目レベルの API アクティビティ (、DeleteItem 、および UpdateItem API PutItemオペレーションなど) 。	DynamoDB	AWS::DynamoDB::Table

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	Note ストリームが有効になっているテーブルの場合、データイベントの `resources` フィールドには `AWS::DynamoDB::Stream` と `AWS::DynamoDB::Table` の両方が含まれます。`resources.type` に `AWS::DynamoDB::Table` を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方がログ記録されます。ストリームイベント を除外		

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	するには、eventName フィールドにフィルターを追加します。		
AWS Lambda	AWS Lambda 関数実行アクティビティ (InvokeAPI)。	Lambda	AWS::Lambda::Function
Amazon S3	S3 バケット内のオブジェクトに対する Amazon S3 オブジェクトレベルの API アクティビティ (GetObject 、DeleteObject 、および PutObject API オペレーションなど)。 S3	S3	AWS::S3::Object
AWS AppConfig	StartConfiguration Session および への呼び出しなどの設定オペレーションの AWS AppConfig API アクティビティGetLatestConfiguration 。	AWS AppConfig	AWS::AppConfig::Configuration

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS B2B データ交換	GetTransformerJob および StartTransformerJob の呼び出しなど、Transformer 操作用の B2B データ交換 API アクティビティ。	B2B データ交換	AWS::B2BI::Transformer
Amazon Bedrock	エージェントエイリアスでの Amazon Bedrock API アクティビティ。	Bedrock エージェントエイリアス	AWS::Bedrock::AgentAlias
	ナレッジベースでの Amazon Bedrock API アクティビティ。	Bedrock ナレッジベース	AWS::Bedrock::KnowledgeBase
Amazon CloudFront	CloudFront での API アクティビティKeyValueStore。	CloudFront KeyValueStore	AWS::CloudFront::KeyValueStore
AWS Cloud Map	名前空間 での AWS Cloud Map API アクティビティ。	AWS Cloud Map 名前空間	AWS::ServiceDiscovery::Namespace
	サービス での AWS Cloud Map API アクティビティ。	AWS Cloud Map service	AWS::ServiceDiscovery::Service

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS CloudTrail	CloudTrail PutAuditEvents 外部からのイベントをログに記録するために使用される CloudTrail Lake チャネルでの アクティビティ AWS。	CloudTrail チャンネル	`AWS::CloudTrail::Channel`
Amazon CodeWhisperer	カスタマイズに対する Amazon CodeWhisperer API アクティビティ。	CodeWhisperer カスタマイズ	`AWS::CodeWhisperer::Customization`
	プロファイルの Amazon CodeWhisperer API アクティビティ。	CodeWhisperer	`AWS::CodeWhisperer::Profile`
Amazon Cognito	Amazon Cognito アイデンティティプール に対する Amazon Cognito API アクティビティ。	Cognito アイデンティティプール	`AWS::Cognito::IdentityPool`
Amazon DynamoDB	ストリームに対する Amazon DynamoDB API アクティビティ	DynamoDB Streams	`AWS::DynamoDB::Stream`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon Elastic Block Store	Amazon EBS スナップショットの `PutSnapshotBlock` 、`GetSnapshotBlock` 、および `ListChangedBlocks` などの Amazon Elastic Block Store (EBS) ダイレクト API。	Amazon EBS ダイレクト API	`AWS::EC2::Snapshot`
Amazon EMR	ログ先行書き込みワークスペースでの Amazon EMR API アクティビティ。	EMR ログ先行書き込みワークスペース	`AWS::EMRWAL::Workspace`
Amazon FinSpace	環境に対する Amazon FinSpace API アクティビティ。	FinSpace	`AWS::FinSpace::Environment`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS Glue	AWS Glue Lake Formation によって作成されたテーブルに対する API アクティビティ。 **Note** AWS Glue テーブルのデータイベントは現在、次のリージョンでのみサポートされています。 • 米国東部 (バージニア北部) • 米国東部 (オハイオ) • 米国西部 (オレゴン) • 欧州 (アイルランド) • アジアパシフィック (東京) リージョン	Lake Formation	`AWS::Glue::Table`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon GuardDuty	ディテクター の Amazon GuardDuty API アクティビティ。https://docs.aws.amazon.com/guardduty/latest/ug/logging-using-cloudtrail.html#guardduty-data-events-in-cloudtrail	GuardDuty ディテクター	`AWS::GuardDuty::Detector`
AWS HealthImaging	AWS HealthImaging データストアでの API アクティビティ。	医療用画像データストア	`AWS::MedicalImaging::Datastore`
AWS IoT	証明書の AWS IoT API アクティビティ。	IoT 証明書	`AWS::IoT::Certificate`
	モノの AWS IoT API アクティビティ。	IoT モノ	`AWS::IoT::Thing`
AWS IoT Greengrass Version 2	コンポーネントバージョンの Greengrass コアデバイスからの Greengrass API アクティビティ。 **Note** Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass コンポーネントバージョン	`AWS::GreengrassV2::ComponentVersion`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	デプロイ上の Greengrass コアデバイスからの Greengrass API アクティビティ。 **Note** Greengrass はアクセス拒否イベントを記録しません。	IoT Greengrass デプロイ	`AWS::GreengrassV2::Deployment`
AWS IoT SiteWise	アセット での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_CreateAsset.html	IoT SiteWise アセット	`AWS::IoTSiteWise::Asset`
	時系列 での IoT SiteWise API アクティビティ。 https://docs.aws.amazon.com/iot-sitewise/latest/APIReference/API_DescribeTimeSeries.html	IoT SiteWise 時系列	`AWS::IoTSiteWise::TimeSeries`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS IoT TwinMaker	エンティティ での IoT TwinMaker API アクティビティ。https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateEntity.html	IoT TwinMaker エンティティ	`AWS::IoTTwinMaker::Entity`
	ワークスペース での IoT TwinMaker API アクティビティ。https://docs.aws.amazon.com/iot-twinmaker/latest/apireference/API_CreateWorkspace.html	IoT TwinMaker ワークスペース	`AWS::IoTTwinMaker::Workspace`
Amazon Kendra インテリジェントランキング	リスコア実行プラン に対する Amazon Kendra Intelligent Ranking API アクティビティ。	Kendra ランキング	`AWS::KendraRanking::ExecutionPlan`
Amazon Keyspaces (Apache Cassandra 向け)	テーブルでの Amazon Keyspaces API アクティビティ。	Cassandra テーブル	`AWS::Cassandra::Table`
Amazon Kinesis Data Streams	ストリーム での Kinesis Data Streams API アクティビティ。	Kinesis ストリーム	`AWS::Kinesis::Stream`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	ストリームコンシューマー での Kinesis Data Streams API アクティビティ。	Kinesis ストリームコンシューマー	`AWS::Kinesis::StreamConsumer`
Amazon Kinesis Video Streams	`GetMedia` および の呼び出しなど、ビデオストリームでの Kinesis Video Streams API アクティビティ`PutMedia`。	Kinesis ビデオストリーム	`AWS::KinesisVideo::Stream`
Amazon Managed Blockchain	ネットワーク上の Amazon Managed Blockchain API アクティビティ。	Managed Blockchain ネットワーク	`AWS::ManagedBlockchain::Network`
	`eth_getBalance` や `eth_getBlockByNumber` などの Ethereum ノードに対する Amazon Managed Blockchain JSON-RPC コール。	Managed Blockchain	`AWS::ManagedBlockchain::Node`
Amazon Neptune Graph	Neptune Graph でのクエリ、アルゴリズム、ベクトル検索などのデータ API アクティビティ。	Neptune Graph	`AWS::NeptuneGraph::Graph`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
AWS Private CA	AWS Private CA Connector for Active Directory API アクティビティ。	AWS Private CA Connector for Active Directory	`AWS::PCAConnectorAD::Connector`
Amazon Q アプリ	Amazon Q Apps での Data API アクティビティ。	Amazon Q アプリ	`AWS::QApps:QApp`
Amazon Q Business	アプリケーション上の Amazon Q Business API アクティビティ。	Amazon Q Business アプリケーション	`AWS::QBusiness::Application`
	データソース上の Amazon Q Business API アクティビティ。	Amazon Q Business データソース	`AWS::QBusiness::DataSource`
	インデックスでの Amazon Q Business API アクティビティ。	Amazon Q Business インデックス	`AWS::QBusiness::Index`
	ウェブエクスペリエンスでの Amazon Q Business API アクティビティ。	Amazon Q Business ウェブエクスペリエンス	`AWS::QBusiness::WebExperience`
Amazon RDS	DB クラスターでの Amazon RDS API アクティビティ。	RDS Data API - DB クラスター	`AWS::RDS::DBCluster`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon S3	アクセスポイントでの Amazon S3 API アクティビティ。	S3 アクセスポイント	`AWS::S3::AccessPoint`
	Amazon S3 Object Lambda アクセスポイント API アクティビティ、`CompleteMultipartUpload` や への呼び出しなど`GetObject`。	S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`
Amazon S3 on Outposts	Amazon S3 on Outposts オブジェクトレベル API アクティビティ。	S3 Outposts	`AWS::S3Outposts::Object`
Amazon SageMaker	エンドポイントでの Amazon SageMaker `InvokeEndpointWithResponseStream` アクティビティ。	SageMaker エンドポイント	`AWS::SageMaker::Endpoint`
	特徴量ストアでの Amazon SageMaker API アクティビティ。	SageMaker 特徴量ストア	`AWS::SageMaker::FeatureGroup`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
	実験トライアルコンポーネント での Amazon SageMaker API アクティビティ。 https://docs.aws.amazon.com/sagemaker/latest/dg/experiments-monitoring.html	SageMaker メトリクス実験トライアルコンポーネント	`AWS::SageMaker::ExperimentTrialComponent`
Amazon SNS	プラットフォームエンドポイントでの Amazon SNS `Publish` API オペレーション。	SNS プラットフォームエンドポイント	`AWS::SNS::PlatformEndpoint`
	トピックに関する Amazon SNS `Publish` および `PublishBatch` API オペレーション。	SNS トピック	`AWS::SNS::Topic`
Amazon SQS	メッセージでの Amazon SQS API アクティビティ。	SQS	`AWS::SQS::Queue`
AWS Step Functions	ステートマシンでの Step Functions API アクティビティ。	Step Functions ステートマシン	`AWS::StepFunctions::StateMachine`
AWS Supply Chain	AWS Supply Chain インスタンスでの API アクティビティ。	サプライチェーン	`AWS::SCN::Instance`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon SWF	ドメイン での Amazon SWF API アクティビティ。 https://docs.aws.amazon.com/amazonswf/latest/developerguide/swf-dev-domains.html	SWF ドメイン	`AWS::SWF::Domain`
AWS Systems Manager	コントロールチャネルでの Systems Manager API アクティビティ。	Systems Manager	`AWS::SSMMessages::ControlChannel`
	マネージドノードでの Systems Manager API アクティビティ。	Systems Manager マネージドノード	`AWS::SSM::ManagedNode`
Amazon Timestream	データベース上の Amazon Timestream `Query` API アクティビティ。	Timestream データベース	`AWS::Timestream::Database`
	テーブル上の Amazon Timestream `Query` API アクティビティ。	Timestream テーブル	`AWS::Timestream::Table`
Amazon Verified Permissions	ポリシーストア上の Amazon Verified Permissions API アクティビティ。	Amazon Verified Permissions	`AWS::VerifiedPermissions::PolicyStore`

AWS のサービス	説明	データイベントタイプ (コンソール)	resources.type 値
Amazon WorkSpaces シンクライアント	WorkSpaces デバイス上のシンクライアント API アクティビティ。	シンクライアントデバイス	`AWS::ThinClient::Device`
	WorkSpaces 環境上のシンクライアント API アクティビティ。	シンクライアント環境	`AWS::ThinClient::Environment`
AWS X-Ray	トレース での X-Ray API アクティビティ。	X-Ray トレース	`AWS::XRay::Trace`

CloudTrail データイベントを記録するには、アクティビティを収集する各リソースタイプを明示的に追加する必要があります。詳細については、「証跡の作成」および「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。

単一リージョンの証跡またはイベントデータストアでは、そのリージョンでアクセスできるリソースのデータイベントのみを記録できます。S3 バケットはグローバルですが、 AWS Lambda 関数と DynamoDB テーブルはリージョン別です。

データイベントのログ記録には追加料金が適用されます。 CloudTrail 料金については、「 AWS CloudTrail の料金」を参照してください。

例: Amazon S3 オブジェクトのデータイベントのログ記録

S3 バケットのすべての S3 オブジェクトに対するデータイベントのログ記録

次の例では、*`bucket-1`* という名前の S3 バケットにすべてのデータイベントのログ記録を設定する時の、ログ記録のしくみを示します。この例では、 CloudTrail ユーザーは空のプレフィックスと、読み取りと書き込みの両方のデータイベントをログに記録するオプションを指定しました。

1. ユーザーがオブジェクトを `bucket-1` にアップロードします。
2. `PutObject` API オペレーションは Amazon S3 オブジェクトレベルの API です。これは にデータイベントとして記録されます CloudTrail。 CloudTrail ユーザーが空のプレフィックスを持つ

S3 バケットを指定しているため、そのバケット内の任意のオブジェクトで発生したイベントがログに記録されます。証跡はイベントを処理してログに記録します。

3. 別のユーザーがオブジェクトを bucket-2 にアップロードします。
4. 証跡またはイベントデータストアに指定されなかった S3 バケット内のオブジェクトで PutObject API オペレーションが発生しました。証跡またはイベントデータストアがイベントをログに記録しません。

特定の S3 オブジェクトのデータイベントをログに記録する

次の例では、証跡またはイベントデータストアを構成し、特定の S3 オブジェクトのイベントをログに記録する際に、ログ機能がどのように動作するかを示します。この例では、 CloudTrail ユーザーは bucket-3 という名前の S3 バケットに、プレフィックス *my-images* と、書き込みデータイベントのみをログに記録するオプションを指定しました。

1. ユーザーは、バケットの my-images プレフィックスで始まるオブジェクト (arn:aws:s3:::bucket-3/my-images/example.jpg など) を削除します。
2. DeleteObject API オペレーションは Amazon S3 オブジェクトレベルの API です。これは、書き込みデータイベントとして に記録されます CloudTrail。証跡またはイベントデータストアで指定した S3 バケットとプレフィックスに一致するオブジェクトでイベントが発生しました。証跡またはイベントデータストアはイベントを処理してログに記録します。
3. 別のユーザーが S3 バケットで異なるプレフィックスのオブジェクト (arn:aws:s3:::bucket-3/my-videos/example.avi など) を削除します。
4. 証跡またはイベントデートストアで指定したプレフィックスに一致しないオブジェクトでイベントが発生しました。証跡またはイベントデータストアがイベントをログに記録しません。
5. ユーザーはオブジェクト arn:aws:s3:::bucket-3/my-images/example.jpg に対して GetObject API オペレーションを呼び出します。
6. 証跡またはイベントデータストアで指定したバケットとプレフィックスでイベントが発生しましたが、GetObject は読み取りタイプの Amazon S3 オブジェクトレベルの API です。これはで読み取りデータイベントとして記録され CloudTrail、証跡またはイベントデータストアは読み取りイベントをログ記録するように設定されていません。証跡またはイベントデータストアがイベントをログに記録しません。

> **Note**
>
> 特定の Amazon S3 バケットのデータイベントを口グ記録する場合は、証跡のデータイベントセクションで指定したログファイルの受け取り用に、データイベントをログに記録する Amazon S3 バケットを使用しないことをお勧めします。同じ Amazon S3バケットを使用すると、証跡は、口グファイルが Amazon S3 バケットに配信されるたびにデータイベントをログに記録します。ログファイルは、間隔で配信される集約イベントのため、イベントと口グファイルの比率は 1:1 になりません。イベントは、次回のログファイルに記録されます。例えば、 がログを CloudTrail 配信すると、PutObjectイベントは S3 バケットで発生します。S3 バケットがデータイベントセクションでも指定されていると、証跡は PutObject イベントをデータイベントとして処理して記録します。このアクションは別の PutObject イベントであり、証跡はイベントを再び処理して記録します。
> AWS アカウントのすべての Amazon S3 データイベントをログに記録するように証跡を設定する場合、ログファイルを受信する Amazon S3 バケットのデータイベントをログに記録しないようにするには、別の AWS アカウントに属する Amazon S3 バケットへのログファイルの配信を設定することを検討してください。詳細については、「CloudTrail 複数のアカウントからのログファイルの受信」を参照してください。

他の AWS アカウントの S3 オブジェクトのデータイベントの口グ記録

データイベントをログに記録するように証跡を設定するときに、他の AWS アカウントに属する S3 オブジェクトを指定することもできます。指定されたオブジェクトでイベントが発生すると、 はイベントが各アカウントの証跡と一致するかどうか CloudTrail を評価します。イベントが証跡の設定と一致する場合、証跡はそのアカウントのイベントを処理してログに記録します。一般的に、API の呼び出し元とリソース所有者の両方がイベントを受け取ることができます。

自分が所有する S3 オブジェクトを証跡で指定すると、自分のアカウントのオブジェクトで発生したイベントが証跡によって記録されます。オブジェクトを所有しているため、他のアカウントがオブジェクトを呼び出したときも証跡はイベントを記録します。

あるアカウントのユーザーが自分の証跡で S3 オブジェクトを指定し、別のアカウントがそのオブジェクトを所有している場合は、自分のアカウントのそのオブジェクトで発生したイベントのみが記録されます。他のアカウントで発生したイベントは記録されません。

例: 2 つの AWS アカウントの Amazon S3 オブジェクトのデータイベントの口グ記録

次の例は、2 つの AWS アカウントが同じ S3 オブジェクトのイベントを口グ CloudTrail に記録するように を設定する方法を示しています。

1. ユーザー A は、owner-bucket という名前の S3 バケットのすべてのオブジェクトに対するデータイベントを記録します。A は S3 バケットと空のオブジェクトプレフィックスを指定して証跡を設定します。
2. ユーザー B は、S3 バケットへのアクセスを許可されている別のアカウントを持っています。B も、同じ S3 バケット内のすべてのオブジェクトのデータイベントを記録しようとします。B は、自分の証跡を設定し、同じ S3 バケットと空のオブジェクトプレフィックスを指定します。
3. B は、PutObject API オペレーションで S3 バケットにオブジェクトをアップロードします。
4. このイベントは、B のアカウントで発生し、B の証跡の設定に一致します。B の証跡はイベントを処理してログに記録します。
5. ユーザー A は S3 バケットを所有しており、イベントは A の証跡の設定と一致するので、A の証跡も同じイベントを処理して記録します。イベントの 2 つのコピー (1 つは Bob の証跡にログインし、もう 1 つは自分の証跡にログインした) が存在するため、 はデータイベントの 2 つのコピーに対して CloudTrail 課金します。
6. A が S3 バケットにオブジェクトをアップロードします。
7. このイベントは A のアカウントで発生し、A の証跡の設定と一致します。A の証跡はイベントを処理してログに記録します。
8. イベントは Bob のアカウントで発生せず、S3 バケットを所有していないため、Bob の証跡はイベントを記録しません。 はこのデータイベントの 1 つのコピーに対してのみ CloudTrail 課金します。

例: 2 つの AWS アカウントで使用される S3 バケットを含む、すべてのバケットのデータイベントのログ記録

次の例は、アカウントでデータイベントを収集する証跡に対してアカウント内のすべての S3 バケットの選択が有効になっている場合のログ記録動作を示しています AWS 。

1. ユーザー A は、アカウントですべての S3 バケットに対するデータイベントを記録します。証跡を設定するには、[読み取り] イベント、[書き込み] イベント、または両方の [データイベント] の [All current and future S3 buckets] を選択します。
2. ユーザー B は、アカウントの S3 バケットへのアクセスを許可されている別のアカウントを持っています。B は、B がアクセス権を持っているバケットのデータイベントを記録します。B は、すべての S3 バケットのデータイベントを取得するように証跡を設定します。
3. B は、PutObject API オペレーションで S3 バケットにオブジェクトをアップロードします。
4. このイベントは、B のアカウントで発生し、B の証跡の設定に一致します。B の証跡はイベントを処理してログに記録します。

5. ユーザー A は S3 バケットを所有しており、イベントは A の証跡の設定と一致するので、A の証跡もそのイベントを処理して記録します。イベントのコピーが 2 つ (1 つは Bob の証跡にログインし、もう 1 つは自分の証跡にログインしている) になったため、 はデータイベントのコピーに対して各アカウントに CloudTrail 課金します。
6. A が S3 バケットにオブジェクトをアップロードします。
7. このイベントは A のアカウントで発生し、A の証跡の設定と一致します。A の証跡はイベントを処理してログに記録します。
8. イベントは Bob のアカウントで発生せず、S3 バケットを所有していないため、Bob の証跡はイベントを記録しません。 は、アカウント内のこのデータイベントのコピーを 1 つだけ CloudTrail 課金します。
9. 3 番目のユーザー C は S3 バケットへのアクセス権を持ち、そのバケットで `GetObject` オペレーションを実行します。C は自分のアカウントのすべての S3 バケットでデータイベントを記録するように証跡を設定しています。API 発信者であるため、 は証跡にデータイベント CloudTrail を記録します。B はバケットへのアクセス権を持っていますが、リソース所有者ではないため、今回は B の証跡にイベントは記録されません。リソース所有者は、Mary が呼び出した`GetObject`オペレーションに関するイベントを証跡で受け取ります。 CloudTrail は、データイベントのコピーごとにアカウントと Mary のアカウントに課金します。1 つは Mary の証跡で、もう 1 つは です。

読み取り専用イベントと書き込み専用イベント

データイベントと管理イベントを口グに記録するように証跡またはイベントデータストアを設定するときは、読み取り専用イベントまたは書き込み専用イベントのどちらか一方のみまたは両方を指定できます。

- 読み取り

  [読み取り] イベントには、リソースの読み取りのみ行い、変更を行わない API オペレーションが含まれます。例えば、Amazon EC2 の `DescribeSecurityGroups` および `DescribeSubnets` API オペレーションは読み取り専用イベントです。これらのオペレーションは、Amazon EC2 リソースに関する情報のみを返し、設定は変更しません。

- 書き込み

  [Write] イベントには、リソースを変更する (または変更する可能性がある) API オペレーションが含まれます。例えば、Amazon EC2 の `RunInstances` および `TerminateInstances` API オペレーションはインスタンスを変更します。

例: 読み取りイベントと書き込みイベントを別の証跡に記録する

次の例では、アカウントに対するログアクティビティを異なる S3 バケットに分けるように証跡を設定する方法を示します。1 つのバケットは読み取り専用イベントを受け取り、もう 1 つのバケットは書き込み専用イベントを受け取ります。

1. 証跡を作成し、ログファイルを受け取る `read-only-bucket` という名前の S3 バケットを選択します。次に、証跡を更新し、[読み取り] の管理イベントとデータイベントを記録するように指定します。
2. 第 2 の証跡を作成し、ログファイルを受け取る `write-only-bucket` という名前の S3 バケットを選択します。次に、証跡を更新し、[Write] の管理イベントとデータイベントを記録するように指定します。
3. Amazon EC2 の `DescribeInstances` および `TerminateInstances` API オペレーションがアカウントで発生します。
4. `DescribeInstances` API オペレーションは読み取り専用イベントであり、1 番目の証跡の設定と一致します。証跡は、イベントをログに記録して `read-only-bucket` に配信します。
5. `TerminateInstances` API オペレーションは書き込み専用イベントであり、2 番目の証跡の設定と一致します。証跡は、イベントをログに記録して `write-only-bucket` に配信します。

を使用したデータイベントのログ記録 AWS Management Console

以下の手順では、 AWS Management Consoleを使用して既存のイベントデータストアまたは証跡を更新し、データイベントのログ記録を行う方法について説明します。データイベントをログ記録するために、イベントデータストアを作成する方法の詳細については、「コンソールを使用してイベントのイベントデータストア CloudTrailを作成する」を参照してください。データイベントをログ記録するために、証跡を作成する方法の詳細については、「コンソールで証跡を作成する」を参照してください。

証跡の場合、データイベントのログ記録手順は、高度なイベントセレクタを使用しているか、基本的なイベントセレクタを使用しているかによって異なります。高度なイベントセレクタを使用してすべてのデータイベントタイプのデータイベントをログ記録できますが、基本的なイベントセレクタを使用する場合、Amazon S3 バケットとバケットオブジェクト、 AWS Lambda 関数、および Amazon DynamoDB テーブルのデータイベントのログ記録に制限されます。

内のデータイベントをログに記録するための既存のイベントデータストアの更新 AWS Management Console

以下の手順を実行し、既存の証跡を更新し、データイベントをログに記録します。高度なイベントセレクタの使用の詳細については、このトピック高度なイベントセレクタを使用したデータイベントのフィルタリングの「」を参照してください。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. ナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
3. [イベントデータストア] ページで、更新するイベントデータストアを選択します。

   > **Note**
   >
   > データイベントは、イベントを含むイベントデータストアでのみ有効にできます CloudTrail 。 AWS Config 設定項目、 CloudTrail Insights イベント、またはイベント以外の CloudTrail イベントデータストアでデータイベントを有効にすることはできません AWS 。

4. 詳細ページの [データイベント] で、[編集] を選択します。
5. まだデータイベントのログを記録していない場合は、[データイベント] チェックボックスをオンにします。
6. [データイベントタイプ] で、データイベントをログ記録するリソースのタイプを選択します。
7. ログセレクタテンプレートを選択します。 には、リソースタイプのすべてのデータイベントをログに記録する事前定義されたテンプレート CloudTrail が含まれています。カスタムログセレクタテンプレートを構築するには、[Custom] を選択します。
8. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。
9. [Advanced event selectors] で、データイベントをログに記録する特定のリソースの式を作成します。事前定義済みのログテンプレートを使用している場合は、このステップをスキップできます。

   a. 次のフィールドから選択します。

- **readOnly** - readOnly は、 または の値と等しくなるように設定できますfalse。true読み取り専用データイベントは、Get* または Describe* イベントなどのリソースの状態を変更しないイベントです。書き込みイベントは、Put*、Delete*、または Write* イベントなどのリソース、属性、またはアーティファクトを追加、変更、または削除します。read および write イベントの両方を記録するには、readOnly セレクタを追加しないでください。
- **eventName** - eventName は任意の演算子を使用できます。これを使用して、、、 などCloudTrail、 に口グ記録されたデータイベントを含めたり除外PutBucketGetItemしたりできますGetSnapshotBlock。
- **resources.ARN** - 任意の演算子を で使用できますがresources.ARN、等号または不等号を使用する場合、値はテンプレートで の値として指定したタイプの有効なリソースの ARN と完全に一致する必要がありますresources.type。

  以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

  > **Note**
  >
  > resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方がログ記録されます。ストリームイベント を除外するには、 eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントをログ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントをログ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

データイベントリソースの ARN 形式の詳細については、AWS Identity and Access Management ユーザーガイドの「アクション、リソース、条件キー」を参照してください。

b. 各フィールドについて、[条件の追加] を選択して、必要な条件をすべて追加します。すべての条件に対して最大 500 個の指定値を設定できます。例えば、2 つの S3 バケットのデータイベントをイベントデータストアに記録されたデータイベントから除外するには、 フィールドを resources.ARN に設定し、 の演算子を で始まらないように設定して、S3 バケット ARN に貼り付けるか、イベントをログに記録したくない S3 バケットを参照します。

2 番目の S3 バケットを追加するには、[条件の追加] を選択した後に上記の手順を繰り返し、ARN に貼り付けるか、別のバケットをブラウズします。

> **Note**
>
> イベントデータストア上のすべてのセレクターに対して、最大 500 の値を設定できます。これには、`eventName` などのセレクタの複数の値の配列が含まれます。すべてのセレクタに単一の値がある場合、セレクタに最大 500 個の条件を追加できます。

c. [+ Field] を選択し、必要に応じてフィールドを追加します。エラーを回避するには、フィールドに競合する値や重複する値を設定しないでください。例えば、あるセレクタで ARN を値と等しく指定せず、次に、別のセレクタで同じ値に等しくない ARN を指定します。

10. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。ステップ 6 からこのステップまで繰り返し、データイベントタイプの高度なイベントセレクターを設定します。
11. 選択内容をレビューして確認が完了したらしたら、[変更を保存] を選択します。

の高度なイベントセレクタを使用してデータイベントをログに記録するための既存の証跡の更新 AWS Management Console

で AWS Management Console、証跡が高度なイベントセレクタを使用している場合は、選択したリソースのすべてのデータイベントをログに記録する事前定義されたテンプレートから選択できます。ログセレクタテンプレートを選択したら、最も表示したいデータイベントのみを含めるようにテンプレートをカスタマイズできます。高度なイベントセレクタの使用の詳細については、このトピック高度なイベントセレクタを使用したデータイベントのフィルタリングの「」を参照してください。

1. CloudTrail コンソールのダッシュボードまたは証跡ページで、更新する証跡を選択します。
2. 詳細ページの [データイベント] で、[編集] を選択します。
3. まだデータイベントのログを記録していない場合は、[データイベント] チェックボックスをオンにします。

4. [データイベントタイプ] で、データイベントをログ記録するリソースのタイプを選択します。
5. ログセレクタテンプレートを選択します。 には、リソースタイプのすべてのデータイベントをログに記録する事前定義されたテンプレート CloudTrail が含まれています。カスタムログセレクタテンプレートを構築するには、[Custom] を選択します。

> **Note**
>
> S3 バケットの事前定義されたテンプレートを選択すると、 AWS 現在アカウントにあるすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティのログ記録も有効にします。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。
> 証跡が 1 つのリージョンのみに適用される場合、すべての S3 バケットをログ記録する事前定義済みテンプレートを選択すると、同じリージョン内のすべてのバケット、およびそのリージョンで後に作成するバケットに対して、データイベントのログ記録が可能になります。 AWS アカウント内の他のリージョンの Amazon S3 バケットのデータイベントはログに記録されません。
> すべてのリージョンの証跡を作成する場合、Lambda 関数の事前定義されたテンプレートを選択すると、 AWS アカウントで現在使用しているすべての関数と、証跡の作成後に任意のリージョンで作成できるすべての Lambda 関数のデータイベントログ記録が有効になります。1 つのリージョンの証跡を作成する場合 (証跡の場合、これは を使用してのみ実行できます AWS CLI) 、この選択により、 AWS アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベントログ記録が有効になります。他のリージョンで作成された Lambda 関数のデータイベントのログ記録は有効になりません。
> すべての関数のデータイベントをログに記録すると、そのアクティビティが別の AWS アカウントに属する関数で実行されている場合でも、アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティのログ記録も可能になります AWS 。

6. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。
7. [Advanced event selectors] で、データイベントをログに記録する特定のリソースの式を作成します。事前定義済みのログテンプレートを使用している場合は、このステップをスキップできます。

a. 次のフィールドから選択します。

- **readOnly** - readOnly は、 または の値と等しくなるように設定できますfalse。true読み取り専用データイベントは、Get* または Describe* イベントなどのリソースの状態を変更しないイベントです。書き込みイベントは、Put*、Delete*、または Write* イベントなどのリソース、属性、またはアーティファクトを追加、変更、または削除します。read および write イベントの両方を記録するには、readOnly セレクタを追加しないでください。
- **eventName** - eventName は任意の演算子を使用できます。これを使用して、、、 などCloudTrail、 に口グ記録されたデータイベントを含めたり除外PutBucketGetItemしたりできますGetSnapshotBlock。
- **resources.ARN** - 任意の演算子を で使用できますがresources.ARN、等号または不等号を使用する場合、値はテンプレートで の値として指定したタイプの有効なリソースの ARN と完全に一致する必要がありますresources.type。

  以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

  > **Note**
  >
  > resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /

resources.type	resources.ARN
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*

resources.type	resources.ARN
AWS::CodeWhisperer::Profile	arn:*partition* :codewhis perer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identity pool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name* / stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapsho t/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_I D* :workspace/ *workspace_name*
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*

resources.type	resources.ARN
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinm aker: *region*:*account_ID* :workspac e/ *workspace_ID*
AWS::KendraRanking::Executi onPlan	arn:*partition* :kendra-r anking: *region*:*account_ID* :rescore- execution-plan/ *rescore_execution_ plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*

resources.type	resources.ARN
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* /qapp/*qapp_UUID*

resources.type	resources.ARN
AWS::QBusiness::Application	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*/ data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusines s: *region*:*account_ID* :applicat ion/ *application_ID* /web-expe rience/ *web_experienc_ID*
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_I D* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_I D* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspo int/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outpo sts: *region*:*account_ID* :*object_path*

resources.type	resources.ARN
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*

resources.type	resources.ARN
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*

resources.type	resources.ARN
AWS::ThinClient::Environment	arn:*partition* :thinclie nt: *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name*
AWS::Timestream::Table	arn:*partition* :timestre am: *region*:*account_ID* :database / *database_name* /table/*table_name*
AWS::VerifiedPermissions::P olicyStore	arn:*partition* :verifiedpermissio ns: *region*:*account_ID* :policy-s tore/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方が口グ記録されます。ストリームイベント を除外するには、 eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントを口グ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

データイベントリソースの ARN 形式の詳細については、AWS Identity and Access Management ユーザーガイドの「アクション、リソース、条件キー」を参照してください。

b. 各フィールドについて、[条件の追加] を選択して、必要な条件をすべて追加します。すべての条件に対して最大 500 個の指定値を設定できます。例えば、証跡に記録されたデータイベントから 2 つの S3 バケットのデータイベントを除外するには、 フィールドを resources.ARN に設定し、 の演算子を で始まらないように設定して、S3 バケット ARN に貼り付けるか、イベントをログに記録したくない S3 バケットを参照します。

2 番目の S3 バケットを追加するには、[条件の追加] を選択した後に上記の手順を繰り返し、ARN に貼り付けるか、別のバケットをブラウズします。

> **Note**
>
> 証跡上のすべてのセレクタに対して、最大 500 の値を設定できます。これには、`eventName` などのセレクタの複数の値の配列が含まれます。すべてのセレクタに単一の値がある場合、セレクタに最大 500 個の条件を追加できます。

c. [+ Field] を選択し、必要に応じてフィールドを追加します。エラーを回避するには、フィールドに競合する値や重複する値を設定しないでください。例えば、あるセレクタで ARN を値と等しく指定せず、次に、別のセレクタで同じ値に等しくない ARN を指定します。

8. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。ステップ 4 からこのステップを繰り返し、データイベントタイプのアドバンストイベントセレクタを設定します。
9. 選択内容をレビューして確認が完了したらしたら、[変更を保存] を選択します。

既存の証跡を更新して、 の基本的なイベントセレクタを使用してデータイベントを ログに記録する AWS Management Console

以下の手順で、基本的なイベントセレクターを使用してデータイベントをログに記録するために既存の証跡を更新します。

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/cloudtrail/ で CloudTrail コンソールを開きます。
2. CloudTrail コンソールの証跡ページを開き、証跡名を選択します。

> **Note**
>
> 既存の証跡を編集してデータイベントをログ記録することもできますが、ベストプラクティスとして、ログ記録データイベント専用に別の証跡を作成することを検討してください。

3. [Data events] で、[編集] を選択します。
4. Amazon S3 バケット:

   a. [Data source] で、[S3] を選択します。

   b. すべての現在および将来の S3 バケットを記録することを選択するか、バケットまたは関数を個々に指定することができます。デフォルトでは、現在および将来のすべての S3 バケットのデータイベントが記録されます。

   > **Note**
   >
   > デフォルトの「現在および将来のすべての S3 バケット」オプションを保持すると、 AWS 現在アカウント内のすべてのバケットと、証跡の作成後に作成するバケットのデータイベントログ記録が有効になります。また、 AWS アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティのログ記録も有効にします。これは、そのアクティビティが別の AWS アカウントに属するバケットで実行された場合でも同様です。
   > 1 つのリージョンの証跡を作成する場合 (を使用 AWS CLI) 、アカウント内のすべての S3 バケットを選択 オプションを選択すると、証跡と同じリージョン内のすべてのバケットと、そのリージョンで後から作成するバケットのデータイベントログ記録が有効になります。 AWS アカウントの他のリージョンの Amazon S3 バケットのデータイベントはログに記録されません。

   c. デフォルトの [All current and future S3 buckets] で、[読み取り] イベント、[書き込み] イベント、またはその両方をログ記録することを選択します。

   d. 個々のバケットを選択するには、[All current and future S3 buckets] の [読み取り] および [書き込み] のチェックボックスをオフにします。[Individual bucket selection] で、データイベントをログ記録するバケットを参照します。特定のバケットを検索するには、目的のバケットのバケットプレフィックスを入力します。このウィンドウで、複数のバケットを選択できます。[Add bucket] を選択してより多くのバケットのデータイベントをログ記録します。

[読み取り] イベント (例: GetObject) か、[書き込み] イベント (例: PutObject)、または両方を選択します。

この設定は、個別のバケットに設定した個々の設定よりも優先されます。たとえば、すべての S3 バケットにログ記録 [読み取り] イベントを指定し、データイベントログ記録に特定のバケットの追加を選択した場合、追加したバケットには既に [読み取り] が設定されています。選択を解除することはできません。[書き込み] のオプションしか設定することができません。

ログ記録からバケットを削除するには、[X] を選択します。

5. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。
6. Lambda 関数の場合

   a. [Data source] で、[Lambda] を選択します。

   b. [Lambda 関数] で、[All regions] を選択してすべての Lambda 関数を口グ記録するか、[Input function as ARN] を使用して、特定の関数のデータイベントを口グ記録します。

   AWS アカウントのすべての Lambda 関数に対するデータイベントを記録するには、[現在および将来の関数をすべて記録する] を選択します。この設定は、関数に個々に設定した各設定よりも優先されます。すべての関数が表示されていなくても、関数はすべて口グ記録されます。

   > **Note**
   >
   > すべてのリージョンで証跡を作成している場合は、この選択によって、 AWS アカウントの現時点のすべての関数や、証跡作成後に任意のリージョンに作成する可能性のある Lambda 関数のデータイベントの口グ記録が有効になります。1 つのリージョンの証跡を作成する場合 (を使用して作成 AWS CLI) 、この選択により AWS 、アカウントのそのリージョンで現在使用しているすべての関数と、証跡の作成後にそのリージョンで作成する可能性のある Lambda 関数のデータイベント口グ記録が有効になります。他のリージョンで作成された Lambda 関数のデータイベントの口グ記録は有効になりません。
   > すべての関数のデータイベントを口グに記録すると、そのアクティビティが別の AWS アカウントに属する関数で実行されている場合でも、アカウント内の任意のユーザーまたはロールによって実行されたデータイベントアクティビティの口グ記録も可能になります AWS 。

c. [Input function as ARN] を選択した場合、Lambda 関数の ARN を入力します。

> **Note**
>
> アカウントに 15,000 を超える Lambda 関数がある場合、証跡の作成時にコンソールで CloudTrailすべての関数を表示または選択することはできません。表示されていない場合でも、すべての関数をログ記録するオプションを選択することができます。特定の関数のデータイベントをログ記録する場合、ARN が分かれば、関数を手動で追加することができます。コンソールで証跡の作成を終了し、 AWS CLI および put-event-selectors コマンドを使用して、特定の Lambda 関数のデータイベントログ記録を設定することもできます。詳細については、「を使用した証跡の管理 AWS CLI」を参照してください。

7. データイベントをログに記録する別のデータタイプを追加するには、[Add data event type] を選択します。
8. DynamoDB テーブルの場合

   a. [Data event source] で、[DynamoDB] を選択します。

   b. [DynamoDB table selection] で、[Browse] を選択してテーブルを選択するか、アクセス許可を持つ DynamoDB テーブルの ARN に貼り付けます。DynamoDB テーブルの ARN は次の形式です。

   ```
   arn:partition:dynamodb:region:account_ID:table/table_name
   ```

   別のテーブルを追加するには、[Add row] を選択し、テーブルを参照するか、アクセス許可のあるテーブルの ARN に貼り付けます。
9. [変更を保存] を選択します。

を使用したデータイベントのログ記録 AWS Command Line Interface

AWS CLIを使用して、データイベントのログを記録するように証跡を設定できます。

トピック

- を使用した証跡のデータイベントのログ記録 AWS CLI
- を使用したイベントデータストアのデータイベントのログ記録 AWS CLI

を使用した証跡のデータイベントのログ記録 AWS CLI

AWS CLIを使用して、管理イベントとデータイベントのログを記録するように証跡を設定できます。

> **Note**
>
> - アカウントが管理イベントのコピーを複数記録している場合は、料金が発生することに注意してください。データイベントのログ記録には常に料金が発生します。詳細については、「AWS CloudTrail の料金」を参照してください。
> - 高度なイベントセレクターまたは基本的なイベントセレクターのいずれかを使用できますが、両方を使用することはできません。高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。
> - 証跡で基本イベントセレクターを使用している場合、ログ記録できるのは以下のリソースタイプのみです。
>   - `AWS::DynamoDB::Table`
>   - `AWS::Lambda::Function`
>   - `AWS::S3::Object`
>
>   この他のリソースタイプをログ記録するには、高度なイベントセレクタを使用します。証跡で高度なイベントセレクターが使用されるようにするには、get-event-selectors コマンドを実行して現在のイベントセレクターを確認し、以前のイベントセレクターの対象範囲と一致するように高度なイベントセレクターを設定してから、そのセレクターをデータイベントをログ記録したい任意のリソースタイプに追加します。
> - 高度なイベントセレクターを使用すると `eventName`、`resources.ARN`、および `readOnly` フィールドの値に基づくフィルタリングが実行できるため、関心のあるデータイベントのみをログ記録できるようになります。これらのフィールドの設定の詳細については、 AWS CloudTrail API リファレンスAdvancedFieldSelectorの「」およびこのトピック高度なイベントセレクタを使用したデータイベントのフィルタリングの「」を参照してください。

証跡が管理イベントとデータイベントをログに記録しているかどうかを確認するには、`get-event-selectors` コマンドを実行します。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

コマンドは、証跡のイベントセレクタを返します。

トピック

- アドバンストイベントセレクタを使用してイベントを口グに記録する
- 高度なイベントセレクタを使用して Amazon S3 バケットのすべての Amazon S3 イベントを口グに記録する
- アドバンストイベントセレクタを使用して AWS Outposts イベントの Amazon S3 を口グに記録する
- 基本的なイベントセレクタを使用してイベントを口グに記録する

アドバンストイベントセレクタを使用してイベントを口グに記録する

> **Note**
>
> 高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。高度なイベントセレクターを設定する前に、get-event-selectors コマンドを実行して現在のイベントセレクターを確認してから、以前のイベントセレクターの対象範囲と一致するように高度なイベントセレクターを設定し、そのセレクターを口グ記録を行いたい追加のデータイベントのいずれかに追加します。

次の例では、 という名前の証跡のカスタムアドバンストイベントセレクタを作成し*TrailName*、読み取り/書き込み管理イベント (readOnlyセレクタを省略) PutObjectと、 という名前のバケットsample_bucket_nameと という名前の AWS Lambda 関数DeleteObjectのデータイベントを除くすべての Amazon S3 バケット/プレフィックスの組み合わせのデータイベントを含めますMyLambdaFunction。これらはカスタムアドバンストイベントセレクタであるため、セレクタの各セットにはわかりやすい名前をつけます。末尾のスラッシュは S3 バケットの ARN 値の一部であることに注意してください。

```
aws cloudtrail put-event-selectors --trail-name TrailName --advanced-event-selectors
'[
  {
    "Name": "Log readOnly and writeOnly management events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Management"] }
    ]
  },
  {
```

```
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  },
  {
    "Name": "Log data plane actions on MyLambdaFunction",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::Lambda::Function"] },
      { "Field": "resources.ARN", "Equals": ["arn:aws:lambda:us-
east-2:111122223333:function/MyLambdaFunction"] }
    ]
  }
]'
```

例は、証跡用に設定されたアドバンストイベントセレクタを返します。

```
{
  "AdvancedEventSelectors": [
    {
      "Name": "Log readOnly and writeOnly management events",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Management" ]
        }
      ]
    },
    {
      "Name": "Log PutObject and DeleteObject events for all but one bucket",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::S3::Object" ]
```

```
        },
        {
          "Field": "resources.ARN",
          "NotStartsWith": [ "arn:aws:s3:::sample_bucket_name/" ]
        },
      ]
    },
{
      "Name": "Log data plane actions on MyLambdaFunction",
      "FieldSelectors": [
        {
          "Field": "eventCategory",
          "Equals": [ "Data" ]
        },
        {
          "Field": "resources.type",
          "Equals": [ "AWS::Lambda::Function" ]
        },
        {
          "Field": "eventName",
          "Equals": [ "Invoke" ]
        },
        {
          "Field": "resources.ARN",
          "Equals": [ "arn:aws:lambda:us-east-2:111122223333:function/
MyLambdaFunction" ]
        }
      ]
    }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

高度なイベントセレクタを使用して Amazon S3 バケットのすべての Amazon S3 イベントをログに記録する

> **Note**
>
> 高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。

次の例では、特定の S3 バケットのすべての Amazon S3 オブジェクトのデータイベントを含めるように証跡を設定する方法を示します。resources.type の S3 イベントの値フィールドは AWS::S3::Object です。S3 オブジェクトと S3 バケットの ARN 値はわずかに異なるため、resources.ARN の StartsWith 演算子を追加してすべてのイベントをキャプチャする必要があります。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

コマンドは、次の出力例を返します。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "resources.ARN",
```

```
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                }
            ]
        }
    ]
}
```

アドバンストイベントセレクタを使用して AWS Outposts イベントの Amazon S3 を ログに記録する

> **Note**
>
> 高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。

次の例では、アウトポストの Outopost オブジェクト上のすべての Amazon S3 のすべてのデータイベントを含めるよう、証跡を設定する方法を示します。

```
aws cloudtrail put-event-selectors --trail-name TrailName --region region \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
    }
]'
```

コマンドは、次の出力例を返します。

```
{
    "TrailARN": "arn:aws:cloudtrail:region:account_ID:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
```

```
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ]
}
```

基本的なイベントセレクタを使用してイベントをログに記録する

以下に、基本的なイベントセレクタを示す get-event-selectors コマンドの結果の例を示します。デフォルトでは、 を使用して証跡を作成すると AWS CLI、証跡はすべての管理イベントを記録します。デフォルトでは、証跡はデータイベントを記録しません。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [],
            "ReadWriteType": "All"
        }
    ]
}
```

管理イベントとデータイベントをログに記録するように証跡を設定するには、put-event-selectors コマンドを実行します。

次の例は、基本のイベントセレクターを使用して、すべての管理イベントと S3 オブジェクトのデータイベントを、2 つの S3 バケットのプレフィクスに含めるよう、証跡を設定する方法について示したものです。1 つの証跡に 1~5 個のイベントセレクタを指定できます。1 つの証跡に 1~250 個のデータリソースを指定できます。

> **Note**
>
> 基本イベントセレクタを使用してデータイベントを制限する場合は、S3 データリソースの最大数は 250 個です。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{ "ReadWriteType": "All", "IncludeManagementEvents":true, "DataResources":
 [{ "Type": "AWS::S3::Object", "Values": ["arn:aws:s3:::mybucket/prefix",
 "arn:aws:s3:::mybucket2/prefix2"] }] }]'
```

このコマンドは、証跡に対して設定されているイベントセレクタを返します。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "EventSelectors": [
        {
            "IncludeManagementEvents": true,
            "DataResources": [
                {
                    "Values": [
                        "arn:aws:s3:::mybucket/prefix",
                        "arn:aws:s3:::mybucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
}
```

を使用したイベントデータストアのデータイベントのログ記録 AWS CLI

AWS CLIを使用して、データイベントを記録するようにイベントデータストアを設定できます。create-event-data-store コマンドを使用して、データイベントをログに記録する新しいイベントデータストアを作成します。update-event-data-store コマンドを使用して、既存のイベントデータストアに関する高度イベントセレクターを更新します。

イベントデータストアにデータイベントが含まれているかどうかを確認するには、get-event-data-store コマンドを実行します。

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

コマンドは、イベントデータストアの設定を返します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE6441aa",
    "Name": "ebs-data-events",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all EBS direct APIs on EBS snapshots",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::EC2::Snapshot"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:37:34.228000+00:00"
}
```

トピック

- バケットのすべての Amazon S3 イベントを含める
- Amazon S3 on AWS Outposts イベントを含める

バケットのすべての Amazon S3 イベントを含める

次の例では、特定の S3 バケットのすべての Amazon S3 オブジェクトのデータイベントを口グ含めるようにイベントデータストアを作成する方法を示します。resources.type の S3 イベントの値フィールドは AWS::S3::Object です。S3 オブジェクトと S3 バケットの ARN 値はわずかに異なるため、resources.ARN の StartsWith 演算子を追加してすべてのイベントをキャプチャする必要があります。

```
aws cloudtrail create-event-data-store --name "EventDataStoreName" --multi-region-
enabled \
--advanced-event-selectors \
'[
    {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:partition:s3:::bucket_name/"] }
            ]
        }
]'
```

コマンドは、次の出力例を返します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE492-301f-4053-ac5e-EXAMPLE441aa",
    "Name": "EventDataStoreName",
    "Status": "ENABLED",
    "AdvancedEventSelectors": [
        {
            "Name": "S3EventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.ARN",
```

```
                    "StartsWith": [
                        "arn:partition:s3:::bucket_name/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2023-11-20T20:49:21.766000+00:00"
}
```

Amazon S3 on AWS Outposts イベントを含める

次の例では、アウトポストの Outopost オブジェクト上のすべての Amazon S3 のすべてのデータイベントを含めるよう、イベントデータストアを作成する方法を示します。

```
aws cloudtrail create-event-data-store --name EventDataStoreName \
--advanced-event-selectors \
'[
    {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3Outposts::Object"] }
            ]
        }
]'
```

コマンドは、次の出力例を返します。

```
{
```

```
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEb4a8-99b1-4ec2-9258-EXAMPLEc890",
    "Name": "EventDataStoreName",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "OutpostsEventSelector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Data"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3Outposts::Object"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-02-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2023-02-20T21:00:17.820000+00:00"
}
```

高度なイベントセレクタを使用したデータイベントのフィルタリング

このセクションでは、高度なイベントセレクタを使用してきめ細かなセレクタを作成する方法について説明します。これにより、対象となる特定のデータイベントのみをログに記録することでコストを制御できます。

例:

- eventName フィールドにフィルターを追加することで、特定の API コールを含めたり除外したりできます。

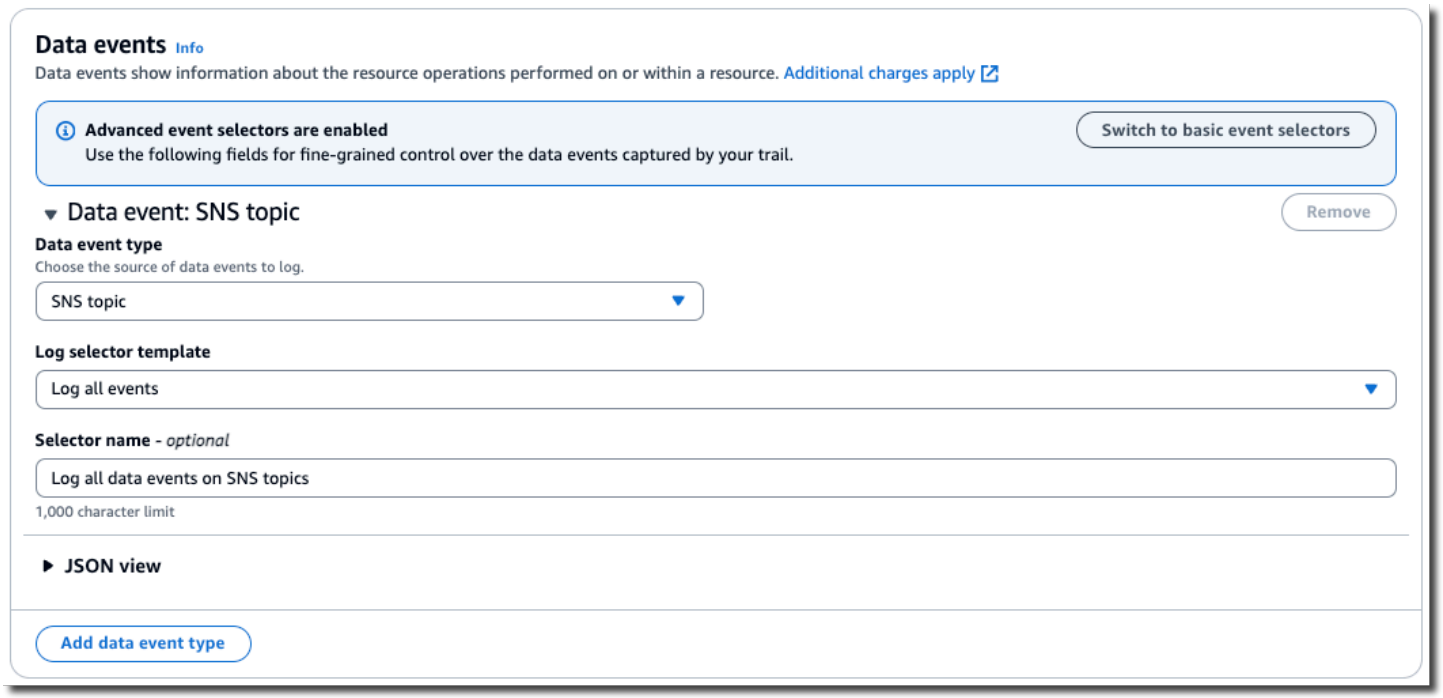
- resources.ARN フィールドにフィルターを追加することで、特定のリソースのログ記録を含めたり除外したりできます。例えば、S3 データイベントをログに記録していた場合は、証跡の S3 バケットのログ記録を除外できます。
- readOnly フィールドにフィルターを追加することで、書き込み専用イベントまたは読み取り専用イベントのみをログに記録するように選択できます。

次の表は、高度なイベントセレクタの設定可能なフィールドに関する追加情報を示しています。

フィールド	必要	有効な演算子	[Description] (説明)
eventCategory	はい	Equals	このフィールドは、データイベントをログに記録するDataように に設定されます。
resources.type	はい	Equals	このフィールドは、データイベントをログに記録するリソースタイプを選択するために使用されます。データイベントテーブルには、可能な値が表示されます。
readOnly	いいえ	Equals	これは、 readOnly値に基づいてデータイベントを含めたり除外したりするために使用されるオプションのフィールドです。の値は、読み込みイベントのみをtrueログに記録します。の値は、イベントfalseのみを書き込みます。このフィールドを追加しない場合、 は読み取りイベントと書き込みイベントの両方を CloudTrail ログに記録します。
eventName	いいえ	すべて	これは、 や など CloudTrail、 に記録されたデータイベントをフィルタリングまたは除外するために使用されるオプションのファイルですPutBucket GetSnapshotBlock 。 を使用している場合は AWS CLI、各値をカンマで区切ることで、複数の値を指定できます。

フィールド	必要	有効な演算子	[Description] (説明)
			コンソールを使用している場合は、フィルタリング`eventName` する各 の条件を作成して、複数の値を指定できます。
`resources.ARN`	いいえ	すべて	これは、 を指定して特定のリソースのデータイベントを除外または含めるために使用されるオプションのフィールドです`resources.ARN` 。で任意の演算子を使用できますが`resources.ARN` 、 `Equals`または を使用する場合`NotEquals` 、値は`resources.type` 指定した の有効なリソースの ARN と完全に一致する必要があります。 を使用している場合は AWS CLI、各値をカンマで区切ることで、複数の値を指定できます。 コンソールを使用している場合は、フィルタリング`resources.ARN` する各 の条件を作成して、複数の値を指定できます。

CloudTrail コンソールを使用してデータイベントを口グ記録するには、証跡またはイベントデータストアを作成または更新するときに、データイベントオプションを選択し、対象のデータイベントタイプを選択します。データイベントテーブルには、 CloudTrail コンソールで選択できるデータイベントタイプが表示されます。



でデータイベントを ログ記録するには AWS CLI、 `--advanced-event-selector`パラメータを設定して、データイベントを ログに記録するリソースタイプ`resources.type`値`eventCategory`と等しい `Data`と の値を設定します。データイベントテーブルには、使用可能なリソースタイプが一覧表示されます。

例えば、すべての Cognito ID プールのデータイベントを ログに記録する場合は、 `--advanced-event-selectors`パラメータを次のように設定します。

```
--advanced-event-selectors '[
    {
       "Name": "Log Cognito data events on Identity pools",
       "FieldSelectors": [
         { "Field": "eventCategory", "Equals": ["Data"] },
         { "Field": "resources.type", "Equals": ["AWS::Cognito::IdentityPool"] }
       ]
     }
]'
```

前述の例では、ID プール上のすべての Cognito データイベントを ログに記録します。高度なイベントセレクタをさらに絞り込んで、`eventName`、、および `resources.ARN`フィールドでフィルタリングして、特定の関心のあるイベントを ログに記録したり`readOnly`、関心のないイベントを除外したりできます。

高度なイベントセレクタを設定して、複数の条件に基づいてデータイベントをフィルタリングできます。例えば、次の例に示すように、すべての Amazon S3 および API コールをログに記録するように高度なイベントセレクタを設定できます。ただし、特定の S3 バケットのイベントログを除外できます。 `PutObject` `DeleteObject`

```
--advanced-event-selectors
'[
  {
    "Name": "Log PutObject and DeleteObject events for all but one bucket",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["PutObject","DeleteObject"] },
      { "Field": "resources.ARN", "NotStartsWith":
 ["arn:aws:s3:::sample_bucket_name/"] }
    ]
  }
]'
```

アドバンストイベントセレクタを使用して、管理イベントとデータイベントの両方をログに記録できます。複数のリソースタイプのデータイベントをログに記録するには、データイベントをログに記録するリソースタイプごとにフィールドセレクタステートメントを追加します。

> **Note**
>
> 証跡は、基本的なイベントセレクタまたは高度なイベントセレクタのいずれかを使用できますが、両方を使用することはできません。高度なイベントセレクターを証跡に適用すると、既存の基本的なイベントセレクターは上書きされます。

トピック

- によるデータイベントのフィルタリング eventName
- によるデータイベントのフィルタリング resources.ARN
- readOnly 値によるデータイベントのフィルタリング

によるデータイベントのフィルタリング `eventName`

高度なイベントセレクタを使用すると、 `eventName` フィールドの値に基づいてイベントを含めたり除外したりできます。でフィルタリング`eventName`すると、 のデータイベントをログに記録すると

きにコストが発生しないように、新しいデータ APIs のサポートが追加されるため、 AWS のサービス コストの制御に役立ちます。

eventName フィールドでは任意の演算子を使用できます。これを使用して、 や など CloudTrail、 に記録されたデータイベントをフィルタリングPutBucketまたは除外できますGetSnapshotBlock。

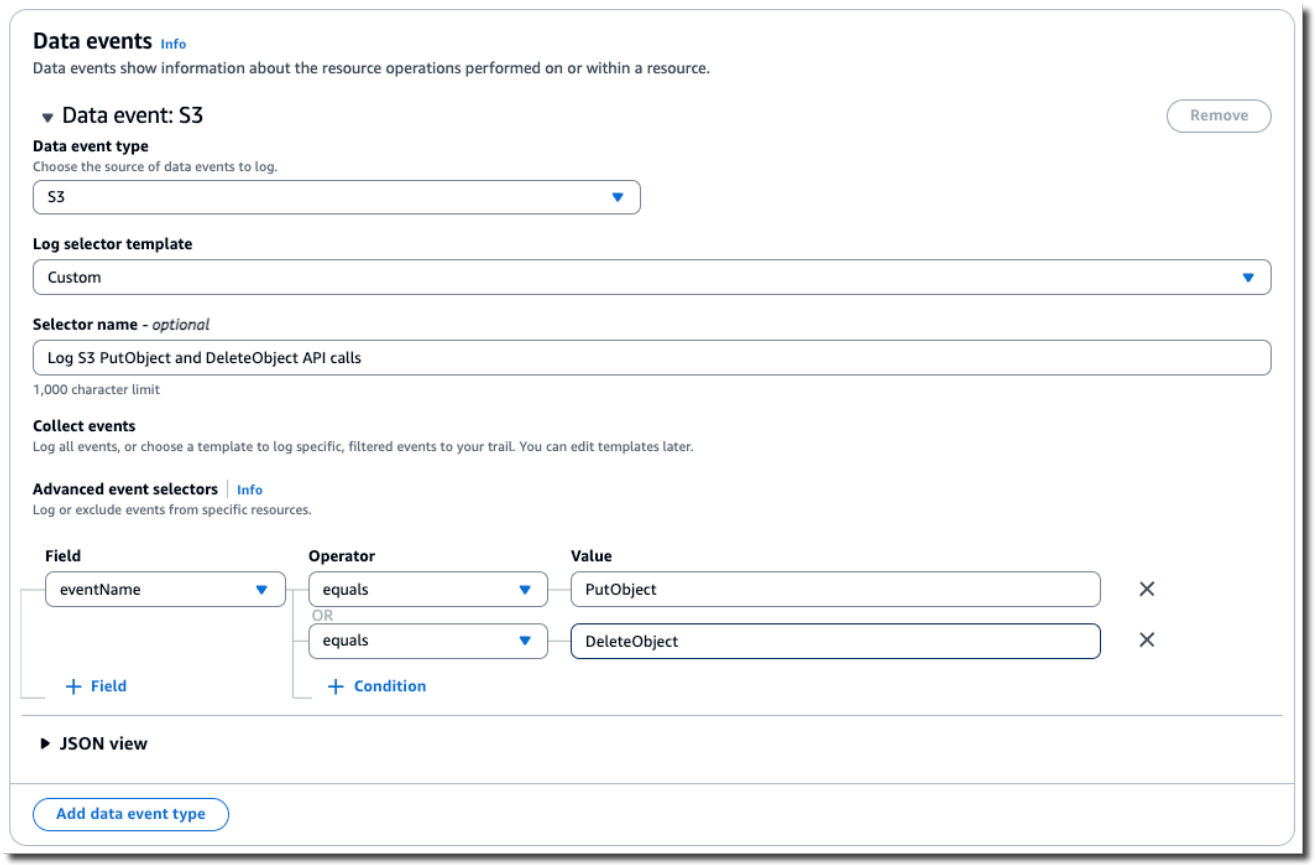
トピック

- eventName を使用したデータイベントのフィルタリング AWS Management Console
- eventName を使用したデータイベントのフィルタリング AWS CLI

eventName を使用したデータイベントのフィルタリング AWS Management Console

CloudTrail コンソールを使用して eventNameフィールドでフィルタリングするには、次の手順を実行します。

1. 証跡の作成手順のステップに従うか、イベントデータストアの作成手順のステップに従います。
2. 証跡またはイベントデータストアを作成するステップに従って、次の選択を行います。
    a. データイベント を選択します。
    b. データイベントをログに記録するデータイベントタイプを選択します。
    c. ログセレクタテンプレート で、カスタム を選択します。
    d. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。
    e. アドバンストイベントセレクタ で、次の操作を実行して をフィルタリングしますeventName。
        i. フィールド で eventNameを選択します。
        ii. 演算子 で、条件演算子を選択します。この例では、特定の API コールをログに記録するため、等号を選択します。
        iii. 値 に、フィルタリングするイベントの名前を入力します。
        iv. 別の でフィルタリングするにはeventName、 + 条件 を選択します。



f. +Field を選択して、他のフィールドにフィルターを追加します。

eventName を使用したデータイベントのフィルタリング AWS CLI

を使用すると AWS CLI、 eventNameフィールドでフィルタリングして、特定のイベントを含めたり除外したりできます。

次の例では、証跡の S3 データイベントをログに記録します。--advanced-event-selectors は、、GetObject、PutObjectおよび DeleteObject API コールのデータイベントのみをログに記録するように設定されています。

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors '[
  {
    "Name": "Log GetObject, PutObject and DeleteObject S3 data events",
    "FieldSelectors": [
      { "Field": "eventCategory", "Equals": ["Data"] },
```

```
      { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
      { "Field": "eventName", "Equals": ["GetObject","PutObject","DeleteObject"] }
    ]
  }
]'
```

次の例では、EBS Direct APIsが、ListChangedBlocksAPI コールは除外します。update-event-data-store コマンドを使用して、既存のイベントデータストアを更新できます。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName"
--advanced-event-selectors '[
    {
        "Name": "Log all EBS Direct API data events except ListChangedBlocks",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
            { "Field": "eventName", "NotEquals": ["ListChangedBlocks"] }
         ]
    }
]'
```

によるデータイベントのフィルタリング **resources.ARN**

高度なイベントセレクタを使用すると、 resources.ARNフィールドの値でフィルタリングできます。

で任意の演算子を使用できますがresources.ARN、 Equalsまたは を使用する場合NotEquals、値はresources.type指定した値の有効なリソースの ARN と完全に一致する必要があります。特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、一致する値としてバケット ARN のみを含めます。

以下の表は、それぞれの resources.type に有効な ARN フォーマットを示しています。

> **Note**
>
> resources.ARN フィールドを使用して、ARN ARNs を持たないリソースタイプをフィルタリングすることはできません。

resources.type	resources.ARN
AWS::DynamoDB::Table [1]	arn:*partition* :dynamodb : *region*:*account_ID* :table/*table_name*
AWS::Lambda::Function	arn:*partition* :lambda:*region*:*account_ID* :function: *function_name*
AWS::S3::Object [2]	arn:*partition* :s3:::*bucket_name* / arn:*partition* :s3:::*bucket_name* /*object_or_file_name* /
AWS::AppConfig::Configuration	arn:*partition* :appconfig: *region*:*account_ID* :application/ *application_ID* /environment/ *environment_ID* /configuration/ *configuration_profile_ID*
AWS::B2BI::Transformer	arn:*partition* :b2bi:*region*:*account_ID* :transformer/ *transformer_ID*
AWS::Bedrock::AgentAlias	arn:*partition* :bedrock: *region*:*account_ID* :agent-alias/ *agent_ID*/*alias_ID*
AWS::Bedrock::KnowledgeBase	arn:*partition* :bedrock: *region*:*account_ID* :knowledge-base/*knowledge_base_ID*
AWS::Cassandra::Table	arn:*partition* :cassandra: *region*:*account_ID* :keyspace/ *keyspace_name* /table/*table_name*

resources.type	resources.ARN
AWS::CloudFront::KeyValueStore	arn:*partition* :cloudfront: *region*:*account_ID* :key-value-store/*KVS_name*
AWS::CloudTrail::Channel	arn:*partition* :cloudtrail: *region*:*account_ID* :channel/ *channel_UUID*
AWS::CodeWhisperer::Customization	arn:*partition* :codewhisperer: *region*:*account_ID* :customization/ *customization_ID*
AWS::CodeWhisperer::Profile	arn:*partition* :codewhisperer: *region*:*account_ID* :profile/ *profile_ID*
AWS::Cognito::IdentityPool	arn:*partition* :cognito-identity: *region*:*account_ID* :identitypool/ *identity_pool_ID*
AWS::DynamoDB::Stream	arn:*partition* :dynamodb: *region*:*account_ID* :table/*table_name* /stream/*date_time*
AWS::EC2::Snapshot	arn:*partition* :ec2:*region*::snapshot/ *snapshot_ID*
AWS::EMRWAL::Workspace	arn:*partition* :emrwal:*region*:*account_ID* :workspace/ *workspace_name*

resources.type	resources.ARN
AWS::FinSpace::Environment	arn:*partition* :finspace : *region*:*account_ID* :environm ent/ *environment_ID*
AWS::Glue::Table	arn:*partition* :glue:*region*:*account_I D* :table/*database_name* /*table_name*
AWS::GreengrassV2::Componen tVersion	arn:*partition* :greengra ss: *region*:*account_ID* :componen ts/ *component_name*
AWS::GreengrassV2::Deployment	arn:*partition* :greengra ss: *region*:*account_ID* :deployme nts/ *deployment_ID*
AWS::GuardDuty::Detector	arn:*partition* :guarddut y: *region*:*account_ID* :detector / *detector_ID*
AWS::IoT::Certificate	arn:*partition* :iot:*region*:*account_I D* :cert/*certificate_ID*
AWS::IoT::Thing	arn:*partition* :iot:*region*:*account_I D* :thing/*thing_ID*
AWS::IoTSiteWise::Asset	arn:*partition* :iotsitew ise: *region*:*account_ID* :asset/*asset_ID*
AWS::IoTSiteWise::TimeSeries	arn:*partition* :iotsitew ise: *region*:*account_ID* :timeseri es/ *timeseries_ID*

resources.type	resources.ARN
AWS::IoTTwinMaker::Entity	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID* /entity/*entity_ID*
AWS::IoTTwinMaker::Workspace	arn:*partition* :iottwinmaker: *region*:*account_ID* :workspace/ *workspace_ID*
AWS::KendraRanking::ExecutionPlan	arn:*partition* :kendra-ranking: *region*:*account_ID* :rescore-execution-plan/ *rescore_execution_plan_ID*
AWS::Kinesis::Stream	arn:*partition* :kinesis: *region*:*account_ID* :stream/*stream_name*
AWS::Kinesis::StreamConsumer	arn:*partition* :kinesis: *region*:*account_ID* :*stream_type* /*stream_name* /consumer/ *consumer_name* :*consumer_creation_timestamp*
AWS::KinesisVideo::Stream	arn:*partition* :kinesisvideo: *region*:*account_ID* :stream/*stream_name* /*creation_time*
AWS::ManagedBlockchain::Network	arn:*partition* :managedblockchain:::networks/ *network_name*
AWS::ManagedBlockchain::Node	arn:*partition* :managedblockchain: *region*:*account_ID* :nodes/*node_ID*

resources.type	resources.ARN
AWS::MedicalImaging::Datastore	arn:*partition* :medical-imaging: *region*:*account_ID* :datastore/ *data_store_ID*
AWS::NeptuneGraph::Graph	arn:*partition* :neptune-graph: *region*:*account_ID* :graph/*graph_ID*
AWS::PCAConnectorAD::Connector	arn:*partition* :pca-connector-ad: *region*:*account_ID* :connector/ *connector_ID*
AWS::QApps:QApp	arn:*partition* :qapps:*region*:*account_ID* :application/ *application_UUID* / qapp/*qapp_UUID*
AWS::QBusiness::Application	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID*
AWS::QBusiness::DataSource	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*/data-source/ *datasource_ID*
AWS::QBusiness::Index	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /index/*index_ID*
AWS::QBusiness::WebExperience	arn:*partition* :qbusiness: *region*:*account_ID* :application/ *application_ID* /web-experience/ *web_experienc_ID*

resources.type	resources.ARN
AWS::RDS::DBCluster	arn:*partition* :rds:*region*:*account_ID* :cluster/ *cluster_name*
AWS::S3::AccessPoint [3]	arn:*partition* :s3:*region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3ObjectLambda::AccessPoint	arn:*partition* :s3-object-lambda: *region*:*account_ID* :accesspoint/ *access_point_name*
AWS::S3Outposts::Object	arn:*partition* :s3-outposts: *region*:*account_ID* :*object_path*
AWS::SageMaker::Endpoint	arn:*partition* :sagemaker: *region*:*account_ID* :endpoint/ *endpoint_name*
AWS::SageMaker::ExperimentTrialComponent	arn:*partition* :sagemaker: *region*:*account_ID* :experiment-trial-component/ *experiment_trial_component_name*
AWS::SageMaker::FeatureGroup	arn:*partition* :sagemaker: *region*:*account_ID* :feature-group/ *feature_group_name*
AWS::SCN::Instance	arn:*partition* :scn:*region*:*account_ID* :instance/ *instance_ID*
AWS::ServiceDiscovery::Namespace	arn:*partition* :servicediscovery: *region*:*account_ID* :namespace/ *namespace_ID*

resources.type	resources.ARN
AWS::ServiceDiscovery::Service	arn:*partition* :servicediscovery: *region*:*account_ID* :service/ *service_ID*
AWS::SNS::PlatformEndpoint	arn:*partition* :sns:*region*:*account_ID* :endpoint/ *endpoint_type* /*endpoint_name* /*endpoint_ID*
AWS::SNS::Topic	arn:*partition* :sns:*region*:*account_ID* :*topic_name*
AWS::SQS::Queue	arn:*partition* :sqs:*region*:*account_ID* :*queue_name*
AWS::SSM::ManagedNode	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :ssm:*region*:*account_ID* :managed-instance/ *instance_ID* • arn:*partition* :ec2:*region*:*account_ID* :instance/ *instance_ID*
AWS::SSMMessages::ControlChannel	arn:*partition* :ssmmessages: *region*:*account_ID* :control-channel/ *control_channel_ID*

resources.type	resources.ARN
AWS::StepFunctions::StateMachine	ARN は次のいずれかの形式である必要があります。 • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* • arn:*partition* :states:*region*:*account_ID* :stateMachine: *stateMachine_name* /*label_name*
AWS::SWF::Domain	arn:*partition* :swf:*region*:*account_ID* :/domain/ *domain_name*
AWS::ThinClient::Device	arn:*partition* :thinclient: *region*:*account_ID* :device/*device_ID*
AWS::ThinClient::Environment	arn:*partition* :thinclient: *region*:*account_ID* :environment/ *environment_ID*
AWS::Timestream::Database	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name*
AWS::Timestream::Table	arn:*partition* :timestream: *region*:*account_ID* :database/ *database_name* /table/*table_name*

resources.type	resources.ARN
AWS::VerifiedPermissions::PolicyStore	arn:*partition* :verifiedpermissions: *region*:*account_ID* :policy-store/ *policy_store_ID*

[1] ストリームが有効になっているテーブルの場合、データイベントの resources フィールドには AWS::DynamoDB::Stream と AWS::DynamoDB::Table の両方が含まれます。resources.type に AWS::DynamoDB::Table を指定すると、デフォルトで DynamoDB テーブルと DynamoDB ストリームイベントの両方が口グ記録されます。ストリームイベント を除外するには、eventNameフィールドにフィルターを追加します。

[2] 特定の S3 バケット内のすべてのオブジェクトのすべてのデータイベントを口グ記録するには、StartsWith 演算子を使用し、値の一致するバケット ARN のみを含めます。末尾のスラッシュは意図的です。除外しないでください。

[3] S3 アクセスポイントのすべてのオブジェクトでイベントを口グ記録するには、アクセスポイント ARN のみを使用し、オブジェクトパスを含めず、StartsWith または NotStartsWith 演算子を使用することを推奨します。

トピック

- resources.ARN を使用したデータイベントのフィルタリング AWS Management Console
- resources.ARN を使用したデータイベントのフィルタリング AWS CLI

resources.ARN を使用したデータイベントのフィルタリング AWS Management Console

CloudTrail コンソールを使用して resources.ARNフィールドでフィルタリングするには、次の手順に従います。

1. 証跡の作成手順のステップに従うか、イベントデータストアの作成手順のステップに従います。
2. 証跡またはイベントデータストアを作成するステップに従って、次の選択を行います。
    a. データイベント を選択します。
    b. データイベントを口グに記録するデータイベントタイプを選択します。
    c. 口グセレクタテンプレート で、カスタム を選択します。

d. (オプション) [セレクタ名] に、セレクタを識別する名前を入力します。セレクタ名は、「2 つの S3 バケットだけのデータイベントを記録する」など、高度なイベントセレクタに関する説明的な名前です。セレクタ名は、拡張イベントセレクタに「Name」と表示され、[JSON ビュー] を展開すると表示されます。

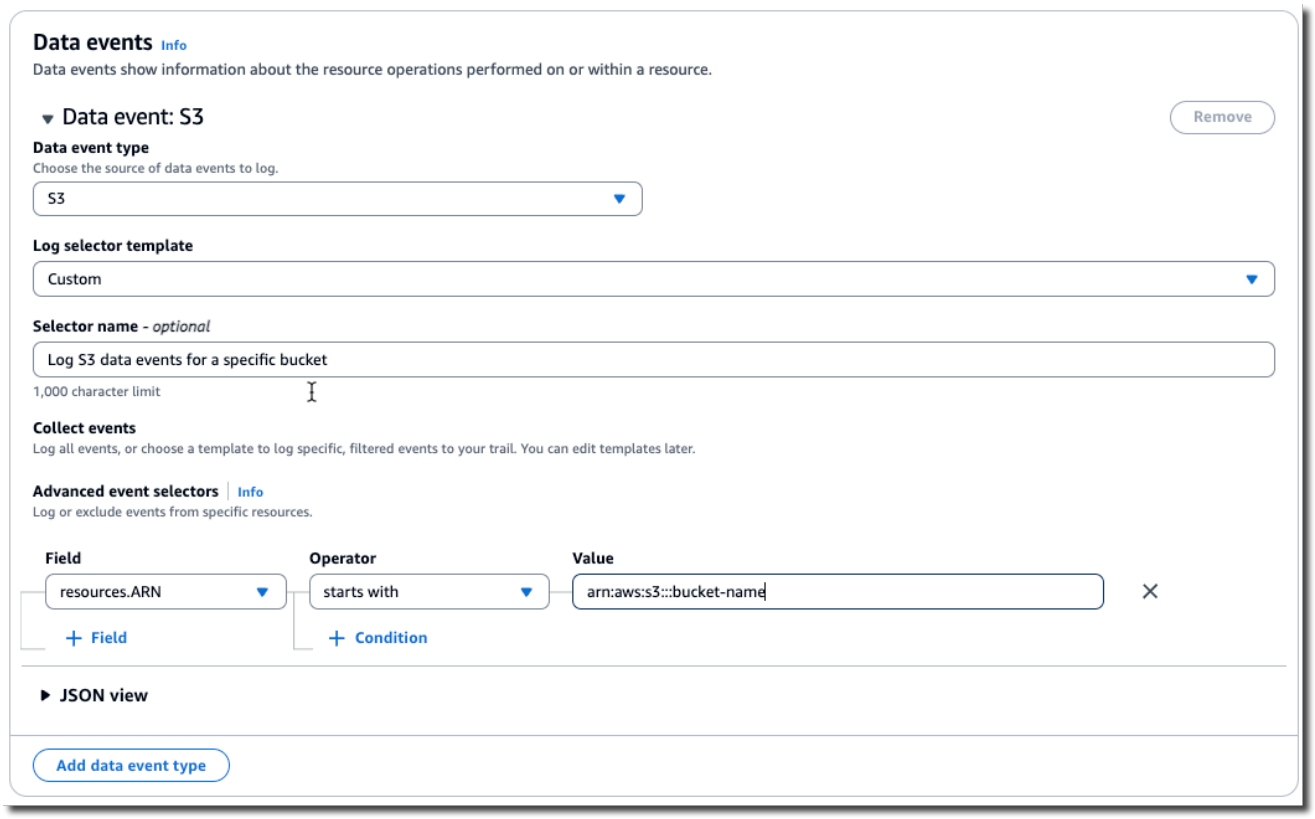
e. アドバンストイベントセレクタ で、次の操作を実行して をフィルタリングしますresources.ARN。

   i. [フィールド]に、[resources.ARN] を選択します。

   ii. 演算子 で、条件演算子を選択します。この例では、特定の S3 バケットのデータイベントを口グに記録するため、 で始まる を選択します。

   iii. 値 には、リソースタイプの ARN を入力します (例: *arn:aws:s3::bucket-name*)。

   iv. 別の をフィルタリングするにはresources.ARN、 + 条件 を選択します。



f. +Field を選択して、他のフィールドにフィルターを追加します。

`resources.ARN` を使用したデータイベントのフィルタリング AWS CLI

を使用すると AWS CLI、 `resources.ARN`フィールドでフィルタリングして、特定の ARN のイベントをログに記録したり、特定の ARN のログ記録を除外したりできます。

次の例では、特定の S3 バケットのすべての Amazon S3 オブジェクトのデータイベントをログ含めるように証跡を設定する方法を示します。`resources.type` の S3 イベントの値フィールドは `AWS::S3::Object` です。S3 オブジェクトと S3 バケットの ARN 値はわずかに異なるため、`resources.ARN` の `StartsWith` 演算子を追加してすべてのイベントをキャプチャする必要があります。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "resources.ARN", "StartsWith":
 ["arn:aws:s3:::bucket_name/"] }
            ]
    }
]'
```

`readOnly` 値によるデータイベントのフィルタリング

高度なイベントセレクタを使用すると、 `readOnly` フィールドの値に基づいてフィルタリングできます。

`Equals` 演算子は `readOnly`フィールドでのみ使用できます。`readOnly` 値は `true`または に設定できます`false`。このフィールドを追加しない場合、 は読み取りイベントと書き込みイベントの両方を CloudTrail ログに記録します。の値は、読み込みイベントのみを`true`ログに記録します。の値は、イベント`false`のみを書き込みます。

トピック

- を使用したreadOnly値によるデータイベントのフィルタリング AWS Management Console
- を使用したreadOnly値によるデータイベントのフィルタリング AWS CLI

を使用した**readOnly**値によるデータイベントのフィルタリング AWS Management Console

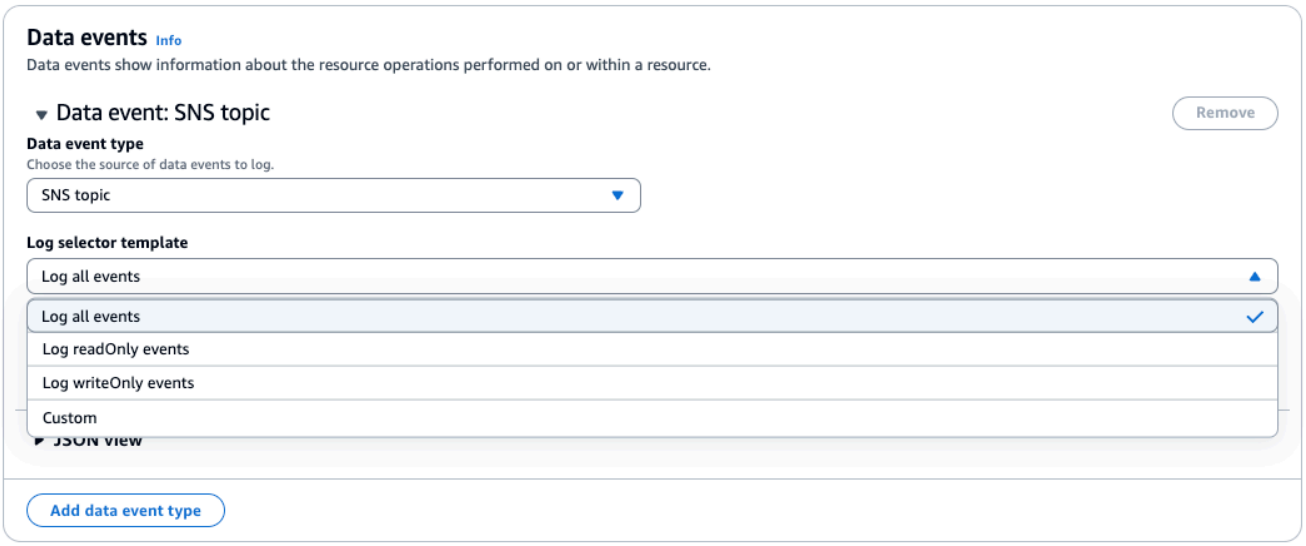
CloudTrail コンソールを使用して readOnlyフィールドでフィルタリングするには、次の手順を実行します。

1. 証跡の作成手順のステップに従うか、イベントデータストアの作成手順のステップに従います。
2. 証跡またはイベントデータストアを作成するステップに従って、次の選択を行います。

   a. データイベント を選択します。

   b. データイベントをログに記録するデータイベントタイプを選択します。

   c. ログセレクタテンプレート で、ユースケースに適したテンプレートを選択します。



これを行う予定がある場合	このログセレクタテンプレートを選択する
読み取りイベントのみをログに記録し、他のフィルター (resources.ARN 値など) を適用しません。	readOnly イベントのログ記録
書き込みイベントのみをログに記録し、他のフィルター (resources.ARN 値など) は適用しません。	writeOnly イベントのログ記録
readOnly 値をフィルタリングし、追加のフィルター (resources.ARN 値など) を適用します。	カスタム

これを行う予定がある場合	このログセレクタテンプレートを選択する
	アドバンストイベントセレクタ で、次の操作を実行してreadOnly値をフィルタリングします。 書き込みイベントをログに記録するには a. [フィールド]に、[readOnly] を選択します。 b. [オペレーター]に、[equals] を選択します。 c. [値] に「**false**」と入力します。 d. +Field を選択して、他のフィールドにフィルターを追加します。 読み取りイベントをログに記録するには a. [フィールド]に、[readOnly] を選択します。 b. [オペレーター]に、[equals] を選択します。 c. [値] に「**true**」と入力します。 d. +Field を選択して、他のフィールドにフィルターを追加します。

を使用した**readOnly**値によるデータイベントのフィルタリング AWS CLI

を使用すると AWS CLI、 readOnlyフィールドでフィルタリングできます。

Equals 演算子は readOnlyフィールドでのみ使用できます。readOnly 値は trueまたは に設定できますfalse。このフィールドを追加しない場合、 CloudTrail は読み取りイベントと書き込みイベントの両方を記録します。の値は、読み込みイベントのみをtrueログに記録します。の値は、イベントfalseのみを書き込みます。

次の例は、すべての Amazon S3 オブジェクトの読み取り専用データイベントを口グに記録するように証跡を設定する方法を示しています。

```
aws cloudtrail put-event-selectors \
--trail-name TrailName \
--region region \
--advanced-event-selectors '[
    {
            "Name": "Log read-only S3 data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
                { "Field": "readOnly", "Equals": ["true"] }
            ]
    }
]'
```

次の例では、APIs の書き込み専用データイベントのみをログに記録する新しいイベントデータストアを作成します。update-event-data-store コマンドを使用して、既存のイベントデータストアを更新できます。

```
aws cloudtrail create-event-data-store \
--name "eventDataStoreName" \
--advanced-event-selectors \
'[
    {
            "Name": "Log write-only EBS Direct API data events",
            "FieldSelectors": [
                { "Field": "eventCategory", "Equals": ["Data"] },
                { "Field": "resources.type", "Equals": ["AWS::EC2::Snapshot"] },
                { "Field": "readOnly", "Equals": ["false"] }
            ]
     }
]'
```

AWS Config コンプライアンスのデータイベントをログに記録する

コン AWS Config フォーマンスパックを使用して、企業が連邦リスク認可管理プログラム (FedRAMP) や米国国立標準技術研究所 (NIST) で必要とされるような形式化された標準への準拠を維持する場合、コンプライアンスフレームワークのコンフォーマンスパックでは、少なくとも Amazon S3 バケットのデータイベントをログに記録する必要があります。コンプライアンスフレームワークの適合パックには、アカウントの S3 データイベントのログ記録をチェックする、cloudtrail-s3-dataevents-enabled と呼ばれるマネージドルールが含まれます。コンプ

ライアンスフレームワークに関連付けられていない多くの適合パックも、S3 データイベントログ記録を必要とします。次に、このルールを含む適合パックの例を示します。

- AWS Well-Architected フレームワークのセキュリティの柱に関する運用上のベストプラクティス
- FDA Title 21 CFR Part 11 の運用のベストプラクティス
- FFIEC に関する運用上のベストプラクティス
- FedRAMP(Moderate) に関する運用上のベストプラクティス
- HIPAA Security の運用のベストプラクティス
- K-ISMS の運用のベストプラクティス
- ログ記録に関する運用上のベストプラクティス

で利用可能なサンプルコンフォーマンスパックの完全なリストについては AWS Config、「 デベロッパーガイド」の「コンフォーマンスパックのサンプルテンプレート」を参照してください。 AWS Config

SDKs を使用した AWS データイベントのログ記録

GetEventSelectors オペレーションを実行して、証跡がデータイベントをログに記録しているかどうかを確認します。PutEventSelectors オペレーションを実行することで、データイベントをログに記録するように証跡を設定できます。詳細については、「 APIリファレンスAWS CloudTrail」を参照してください。

GetEventDataStore オペレーションを実行して、イベントデータストアがデータイベントをログに記録しているかどうかを確認します。CreateEventDataStore または UpdateEventDataStoreオペレーションを実行し、高度なイベントセレクタを指定することで、データイベントを含めるようにイベントデータストアを設定できます。詳細については、「を使用して、イベントデータストアを作成、更新、管理します AWS CLI」および AWS CloudTrail API リファレンスを参照してください。

Amazon CloudWatch Logs へのイベントの送信

CloudTrail は、 CloudWatch ログへのデータイベントの送信をサポートします。Logs ロググループにイベントを送信するように証跡を設定すると、 CloudWatch CloudTrail は証跡で指定したイベントのみを送信します。例えば、データイベントのみをログ記録するように証跡を設定すると、証跡はデータイベントのみを Logs CloudWatch ロググループに配信します。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

Insights イベントのログ記録

AWS CloudTrail インサイトは、 CloudTrail 管理イベントを継続的に分析することで、 AWS ユーザーが API 呼び出しや API エラー率に関連する異常なアクティビティを特定して対応するのに役立ちます。 CloudTrail Insights は、API 呼び出し量と API エラー率の通常のパターン (ベースラインとも呼ばれる) を分析し、呼び出し量またはエラー率が通常のパターンから外れると Insights イベントを生成します。API コール量に関する Insights イベントは、`write` 管理 API に対して生成されます。一方、API エラー率に関する Insights イベントは、`read` と `write` の両方の管理 API に対して生成されます。

> **Note**
>
> API コールのボリュームで Insights イベントをログ記録するには、証跡またはイベントデータストアで `write` 管理イベントがログ記録されている必要があります。API エラー率に関する Insights イベントをログ記録するには、証跡またはイベントデータストアで `read` または `write` の管理イベントがログ記録されている必要があります。

CloudTrail Insights は、グローバルではなく 1 つのリージョンで発生する管理イベントを分析します。 CloudTrail インサイトイベントは、それをサポートする管理イベントが生成されるのと同じリージョンで生成されます。

Insights イベントには追加料金が適用されます。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。詳細については、「AWS CloudTrail の料金」を参照してください。

目次

Insights イベントの配信を理解する

CloudTrail キャプチャする他の種類のイベントとは異なり、Insights イベントは、アカウントの API CloudTrail 使用状況の変化がアカウントの一般的な使用パターンと大きく異なることを検出した場合にのみ記録されます。

CloudTrail イベントを配信する場所と Insights イベントの受信にかかる時間は、トレイルとイベントデータストアによって異なります。

証跡の Insights イベントの配信

トレイルで Insights イベントを有効にしていて、 CloudTrail 異常なアクティビティを検出すると、トレイル用に選択した送信先 S3 `/CloudTrail-Insight` バケットのフォルダーに Insights CloudTrail イベントが配信されます。トレイルで初めて CloudTrail Insights を有効にしてから、異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントが配信されるまでに最大 36 時間かかることがあります。

トレイルの Insights イベントのロギングをオフにしてから Insights イベントを再度有効にするか、トレイルのロギングを停止して再開した場合、異常なアクティビティが検出された場合に Insights イベントの配信が再開されるまでに最大 36 時間かかることがあります。 CloudTrail

イベントデータストアの Insights イベントの配信

ソースイベントデータストアで Insights イベントを有効にしている場合、Insights CloudTrail イベントは送信先のイベントデータストアに配信されます。ソースイベントデータストアで初めて CloudTrail Insights を有効にした後、異常なアクティビティが検出された場合、最初の Insights CloudTrail イベントが宛先イベントデータストアに配信されるまでに最大 7 日かかることがあります。

ソースイベントデータストアの Insights イベントログをオフにしてから Insights イベントを再度有効にするか、ソースイベントデータストアでのイベントの取り込みを停止して再開した場合、異常なアクティビティが検出された場合、Insights イベントの配信が再開されるまでに最大 7 日かかることがあります。 CloudTrail Lake でインサイトイベントを取り込むには追加料金がかかります。 CloudTrail 証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。 CloudTrail 料金について詳しくは、「料金表」を参照してくださいAWS CloudTrail 。

でインサイトイベントをロギングする AWS Management Console

証跡またはイベントデータストアでの Insights イベントは、コンソールを使用して有効化できます。

トピック

- 既存のトレイルでの CloudTrail Insights イベントの有効化
- 既存のイベントデータストアで CloudTrail Insights イベントを有効にする

既存のトレイルでの CloudTrail Insights イベントの有効化

以下の手順に従って、既存のトレイルで CloudTrail Insights イベントを有効にします。デフォルトでは、Insights イベントは有効になっていません。

1. CloudTrail コンソールの左側のナビゲーションペインで Trails ページを開き、トレイル名を選択します。
2. [Insights events] で、[編集] を選択します。

> **Note**
>
> Insights イベントの記録には追加料金が適用されます。 CloudTrail 料金については、「AWS CloudTrail 料金表」を参照してください。

3. [Event type] (イベントタイプ) で、[Insights events] (Insights イベント) を選択します。
4. [Insights events] (Insights イベント) の [Choose Insights types] (Insights の種類を選択) で、[API call rate] (API コールレート) と [API error rate] (API エラー率) のどちらか一方、または両方を選択選択します。[API コール率] の Insights イベントをログに記録するには、証跡が [Write] 管理イベントをログ記録している必要があります。[API エラー率] の Insights イベントをログに記録するには、証跡が [Read] または [Write] 管理イベントをログ記録している必要があります。
5. [変更を保存] を選択して、変更を保存します。

異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントが配信されるまでに最大 36 時間かかることがあります。

既存のイベントデータストアで CloudTrail Insights イベントを有効にする

以下の手順を使用して、既存のイベントデータストアで CloudTrail Insights イベントを有効にします。デフォルトでは、Insights イベントは有効になっていません。

Lake に Insights CloudTrail イベントを取り込むには追加料金がかかります。証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。 CloudTrail 料金について詳しくは、「料金表」を参照してくださいAWS CloudTrail 。

> **Note**
>
> CloudTrail Insights イベントは、 CloudTrail 管理イベントを含むイベントデータストアでのみ有効にできます。他の種類のイベントデータストアでは CloudTrail Insights イベントを有効にすることはできません。

1. CloudTrail コンソールの左側のナビゲーションペインの [Lake] で、[イベントデータストア] を選択します。
2. イベントデータストアの名前を選択します。
3. [管理イベント] で、[編集] を選択します。
4. [Insights を有効にする] を選択します。
5. Insights CloudTrail イベントの配信先となるイベントデータストアを選択します。送信先イベントデータストアは、このイベントデータストア内の管理イベントアクティビティに基づいて Insights イベントを収集します。送信先イベントデータストアの作成方法については、「Insights イベントを口グに記録する送信先イベントデータストアを作成するには」を参照してください。
6. [Insights タイプを選択] で、[API コールレート] と [API エラー率] のどちらか一方、または両方を選択します。[API コールレート] の Insights イベントを口グ記録するには、イベントデータストアが [書き込み] 管理イベントを記録している必要があります。[API エラー率] の Insights イベントを口グ記録するには、イベントデータストアが [読み出し] または [書き込み] の管理イベントを記録している必要があります。
7. [変更を保存] を選択して、変更を保存します。

異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントの配信には最大 7 日かかることがあります。

を使用してインサイトイベントを口ギングする AWS Command Line Interface

AWS CLIを使用すると、Insights イベントを口グ記録するように、証跡とイベントデータストアを設定できます。

> **Note**
>
> API コールのボリュームで Insights イベントを口グ記録するには、証跡またはイベントデータストアで `write` 管理イベントが口グ記録されている必要があります。API エラー率に関する Insights イベントを口グ記録するには、証跡またはイベントデータストアで `read` または `write` の管理イベントが口グ記録されている必要があります。

トピック

- を使用するトレイルの口ギングインサイトイベント AWS CLI
- を使用してイベントデータストアの Insights イベントを口ギングする AWS CLI

を使用するトレイルの口ギングインサイトイベント AWS CLI

証跡が Insights イベントを口グに記録しているかどうかを確認するには、`get-insight-selectors` コマンドを実行します。

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

次の結果は、証跡に対するデフォルト設定を示しています。デフォルトでは、証跡は Insights イベントを記録しません。Insights イベントコレクションが有効になっていないため、`InsightType` 属性値が空になっていて、Insights イベントセレクタが指定されていません。

Insights セレクターを追加しない場合、get-insight-selectorsコマンドは次のエラーメッセージを返します。「 GetInsightSelectors 操作の呼び出し時にエラーが発生しました (InsightNotEnabledException): ######################。証跡の設定を編集して Insights を有効にしてから、もう一度操作を試してください。

```
{
  "InsightSelectors": [ ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

Insights イベントをログに記録するように証跡を設定するには、put-insight-selectors コマンドを実行します。次に、 を含むように証跡を設定する方法の例を示します。Insights セレクターの値は、ApiCallRateInsight、ApiErrorRateInsight、または両方になります。

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

次の結果は、証跡用に設定された Insights イベントセレクタを示しています。

```
{
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ],
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName"
}
```

を使用してイベントデータストアの Insights イベントをロギングする AWS CLI

イベントデータストアで Insights を有効にするには、管理イベントをログ記録するソースイベントデータストアと、Insights イベントをログ記録する送信先イベントデータストアが必要です。

イベントデータストアで Insights イベントが有効になっているかどうかを表示するには、get-insight-selectors コマンドを実行します。

```
aws cloudtrail get-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
```

イベントデータストアで、Insights イベントまたは管理イベントのどちらを受信するように構成されているかを表示するには、get-event-data-store コマンドを実行します。

```
aws cloudtrail get-event-data-store --event-data-store arn:aws:cloudtrail:us-
east-1:123456789012:eventdatastore/EXAMPLE-d483-5c7d-4ac2-adb5dEXAMPLE
```

次の手順で、宛先とソースイベントデータストアを作成し、Insights イベントを有効にする方法を示します。

1. aws cloudtrail create-event-data-store コマンドを実行して、Insights イベントを収集する送信先イベントデータストアを作成します。eventCategory の値は Insight にする必要があります。*retention-period-days*イベントデータストアにイベントを保持したい日数に置き換えてください。

   AWS Organizations 組織の管理アカウントでサインインしている場合、--organization-enabled委任管理者にイベントデータストアへのアクセス権を付与する場合はパラメータを含めてください。

   ```
   aws cloudtrail create-event-data-store \
   --name insights-event-data-store \
   --no-multi-region-enabled \
   --retention-period retention-period-days \
   --advanced-event-selectors '[
       {
         "Name": "Select Insights events",
         "FieldSelectors": [
             { "Field": "eventCategory", "Equals": ["Insight"] }
           ]
       }
     ]'
   ```

   以下に、応答の例を示します。

   ```
   {
       "Name": "insights-event-data-store",
       "ARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
   EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
       "AdvancedEventSelectors": [
           {
              "Name": "Select Insights events",
              "FieldSelectors": [
                 {
                     "Field": "eventCategory",
   ```

```
                "Equals": [
                    "Insight"
                ]
            }
        ]
    }
    ],
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": "90",
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:22:33.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:22:33.714000+00:00"
}
```

この応答の ARN (または ARN の ID サフィックス) は、ステップ 3 で --insights-destination パラメータの値として使用します。

2. 管理イベントを口グ記録するソースイベントデータストアを作成するには、aws cloudtrail create-event-data-store コマンドを実行します。イベントデータストアのデフォルトでは、すべての口グ管理イベントを口グ記録します。すべての管理イベントを口グ記録するのであれば、高度なイベントセレクタを指定する必要はありません。*retention-period-days*イベントデータストアにイベントを保存したい日数に置き換えてください。組織のイベントデータストアを作成する場合は、--organization-enabled パラメータを含めます。

```
aws cloudtrail create-event-data-store --name source-event-data-store --retention-
period retention-period-days
```

以下に、応答の例を示します。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
    "Name": "source-event-data-store",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Default management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
```

```
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 90,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2023-11-08T15:25:35.578000+00:00",
    "UpdatedTimestamp": "2023-11-08T15:25:35.714000+00:00"
}
```

この応答の ARN (または ARN の ID サフィックス) は、ステップ 3 で `--event-data-store` パラメータの値として使用します。

3. put-insight-selectors コマンドを実行して Insights イベントを有効にします。Insights セレクターの値は、`ApiCallRateInsight`、`ApiErrorRateInsight`、または両方になります。`--event-data-store` パラメータには、管理イベントをログに記録して Insights を有効にするソースイベントデータストアの ARN (または ARN の ID サフィックス) を指定します。`--insights-destination` パラメータには、Insights イベントをログ記録する送信先イベントデータストアの ARN (または ARN の ID サフィックス) を指定します。

```
aws cloudtrail put-insight-selectors --event-data-store arn:aws:cloudtrail:us-
east-1:111122223333:eventdatastore/EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE --
insights-destination arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE --insight-selectors '[{"InsightType":
 "ApiCallRateInsight"},{"InsightType": "ApiErrorRateInsight"}]'
```

次の結果は、イベントデータストア用に設定された Insights イベントセレクタを表示しています。

```
{
  "EventDataStoreARN": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLE9952-4ab9-49c0-b788-f4f3EXAMPLE",
  "InsightsDestination": "arn:aws:cloudtrail:us-east-1:111122223333:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
  "InsightSelectors":
```

```
      [
         {
            "InsightType": "ApiErrorRateInsight"
         },
         {
            "InsightType": "ApiCallRateInsight"
         }
      ]
}
```

CloudTrail イベントデータストアで初めてインサイトを有効にした後、異常なアクティビティが検出された場合、最初の CloudTrail Insights イベントが配信されるまでに最大 7 日かかることがあります。

CloudTrail Insights は、グローバルではなく 1 つのリージョンで発生する管理イベントを分析します。 CloudTrail インサイトイベントは、それをサポートする管理イベントが生成されるのと同じリージョンで生成されます。

組織イベントデータストアでは、 CloudTrail 組織のすべての管理イベントの集計を分析する代わりに、各メンバーのアカウントからの管理イベントを分析します。

Lake で Insights イベントを取り込むには追加料金がかかります。 CloudTrail 証跡とイベントデータストアの両方で Insights を有効にすると、それぞれ個別に課金されます。 CloudTrail 料金について詳しくは、「料金表」を参照してくださいAWS CloudTrail 。

AWS SDK によるイベントのロギング

GetInsightSelectors操作を実行して、トレイルまたはイベントデータストアで Insights イベントが有効になっているかどうかを確認します。PutInsightSelectorsオペレーションで Insights イベントが有効になるように、トレイルまたはイベントデータストアを設定できます。詳細については、「 APIリファレンスAWS CloudTrail」を参照してください。

証跡に関する追加情報

このセクションでは、証跡に固有の追加情報を提供します。このセクションでは、 CloudTrail 登録したトレイルのイベントをコンソールのインサイトページから表示する方法と、 CloudWatch オプションでこれらのイベントをログに送信してモニタリングする方法について説明します。

トピック

- コンソールでの証跡の Insights イベントの表示

- Amazon CloudWatch ログへのトレイルイベントの送信

コンソールでの証跡の Insights イベントの表示

トレイルについては、コンソールの Insights ページから Insights イベントにアクセスして表示することもできます。 CloudTrail コンソールで Insights イベントにアクセスして表示する方法と、を使用する方法について詳しくは AWS CLI、 CloudTrail トレイルのインサイトイベントの表示このガイドのを参照してください。

証跡での Insights イベントの例を次の画像に示します。Insights イベントの詳細ページを開くには、[ダッシュボード] ページまたは [Insights] ページから Insights イベント名を選択します。

CloudTrail トレイルでインサイトを無効にしたり、トレイルへのロギングを停止したりすると（ CloudTrail インサイトが無効になる ）、インサイトイベントが宛先の S3 バケットに保存されるか、コンソールのインサイトページに、インサイトが以前にインサイトを有効にした日付で表示される可能性があります。

フィルター列

左側の列には、サブジェクト API に関連し、同じ Insights イベントタイプを持つ Insights イベントのリストが表示されます。この列では、詳細情報が必要な Insights イベントを選択できます。この列でイベントを選択すると、そのイベントが [Insights graph] タブのグラフで強調表示されます。デフォルトでは、[イベント] タブに表示されるイベントを、CloudTrailインサイトイベントをトリガーした異常なアクティビティが発生した期間に呼び出された特定の API CloudTrail に関するイベントに限定するフィルターを適用します。Insights CloudTrail イベントとは関係のないイベントを含め、異常なアクティビティの期間中に呼び出されたイベントをすべて表示するには、フィルターをオフにしてください。

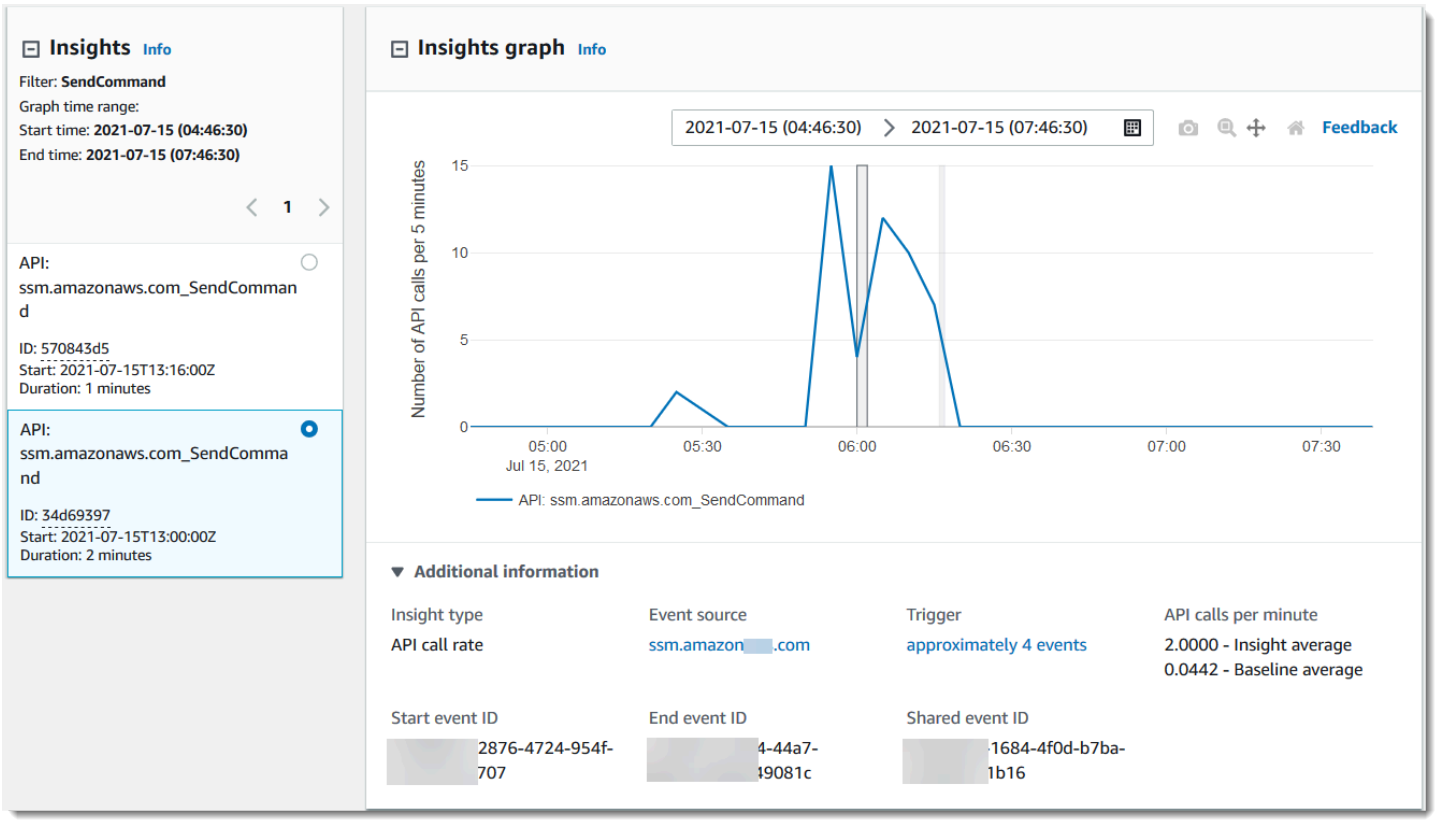
[Insights graph] タブ

[Insights graph] タブでは、Insights イベントの詳細ページには、1 つ以上の Insights イベントがログに記録される前後の期間に発生した API コールボリュームまたはエラーレートのグラフが表示されます。グラフでは、Insights イベントは縦棒で強調表示され、棒の幅は Insights イベントの開始時刻と終了時刻を示します。

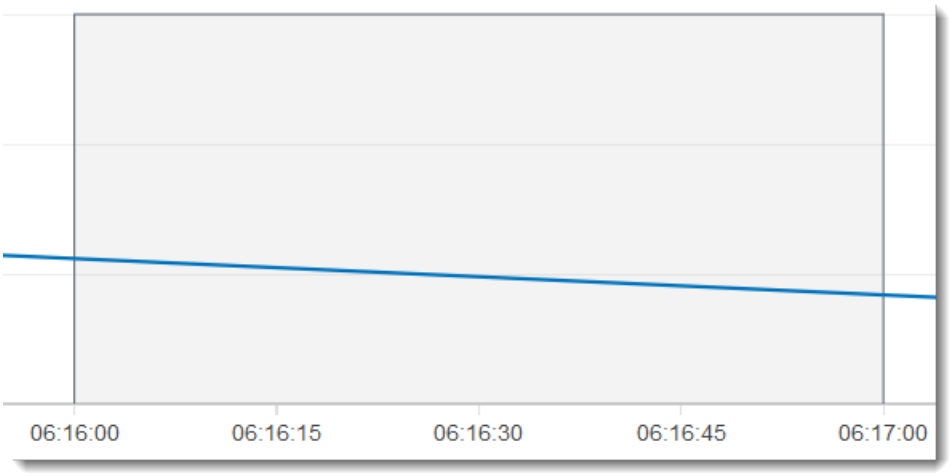
この例では、縦方向の強調表示帯に、アカウント内の異常な数の AWS Systems Manager SendCommand API 呼び出しが表示されています。強調表示された領域では、SendCommand呼び出し数がアカウントのベースライン平均である 1 分あたりの 0.0442 呼び出しを上回ったため、異常なアクティビティを検出したときに Insights CloudTrail イベントが記録されました。Insights イベ

ントでは、午前 5 時 50 分から午前 5 時 55 分までの 5 分間に 15 件の SendCommand の呼び出しがあったことが記録されています。これは、アカウントに対して予想されるよりも毎分約 2 回多い API コールです。この例では、グラフの期間は 3 時間です。つまり、太平洋夏時間 2021年7月15日 午前 4 時 30 分から 2021 年 7 月 15 日 午前 7:30 までです。このイベントの開始時刻は、太平洋夏時間 2021 年 7月 15 日 午前 6:00で、終了時刻はその 2 分後です。終了 Insights イベント (強調表示されていない) は、異常なアクティビティが 午前 6 時 16 分頃に終了したことを示しています。

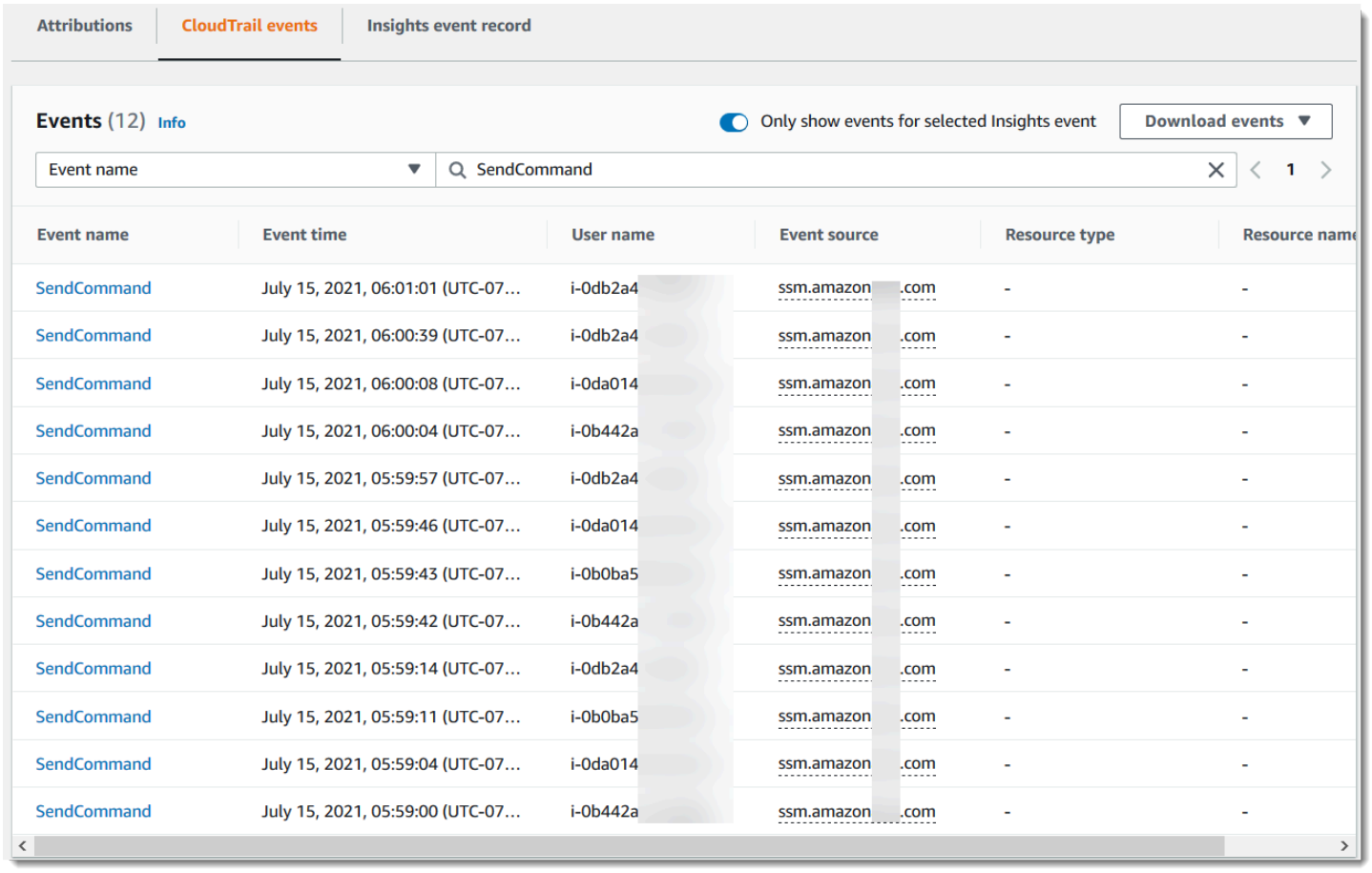
ベースラインは、Insights イベントの開始前の 7 日間にわたって計算されます。ベースライン期間 (API CloudTrail での正常なアクティビティを分析する期間) の値は約 7 日間ですが、ベースライン期間を整数 1 CloudTrail 日に四捨五入するため、正確なベースライン期間は異なる場合があります。



ツールバーにある Zoom コマンドを使って終了 Insights イベントを拡大すると、開始時刻と終了時刻を表示できます。この例は、[Zoom] (ズーム) を選択し、強調表示された Insights イベントの一方の端をズームカーソルで少しドラッグすると、Insights イベントが展開され、タイムラインの詳細が表示されることを示しています。

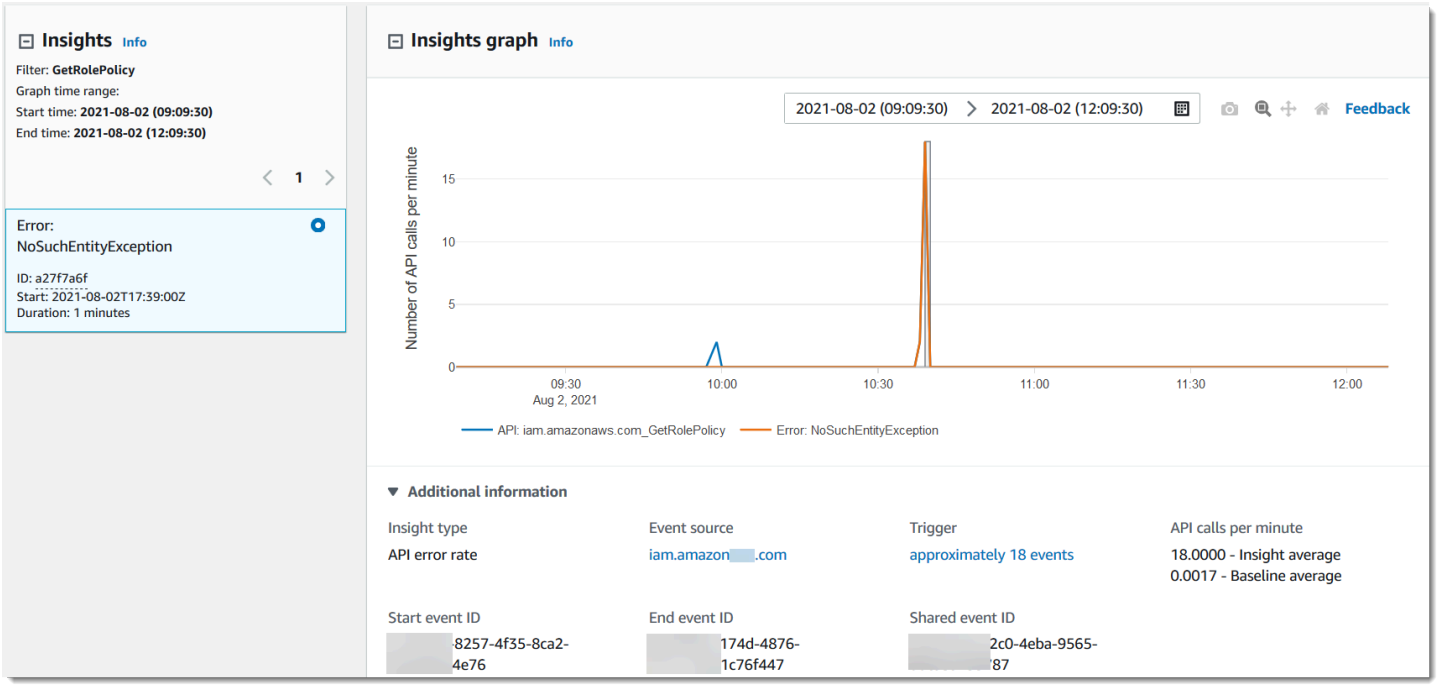


CloudTrail 分析されて異常なアクティビティが特定されたイベントを表示するには、CloudTrail イベントタブを開きます。この例では、12 CloudTrail 件のイベントを分析し、そのうちの 4 件が Insights イベントをトリガーしました。



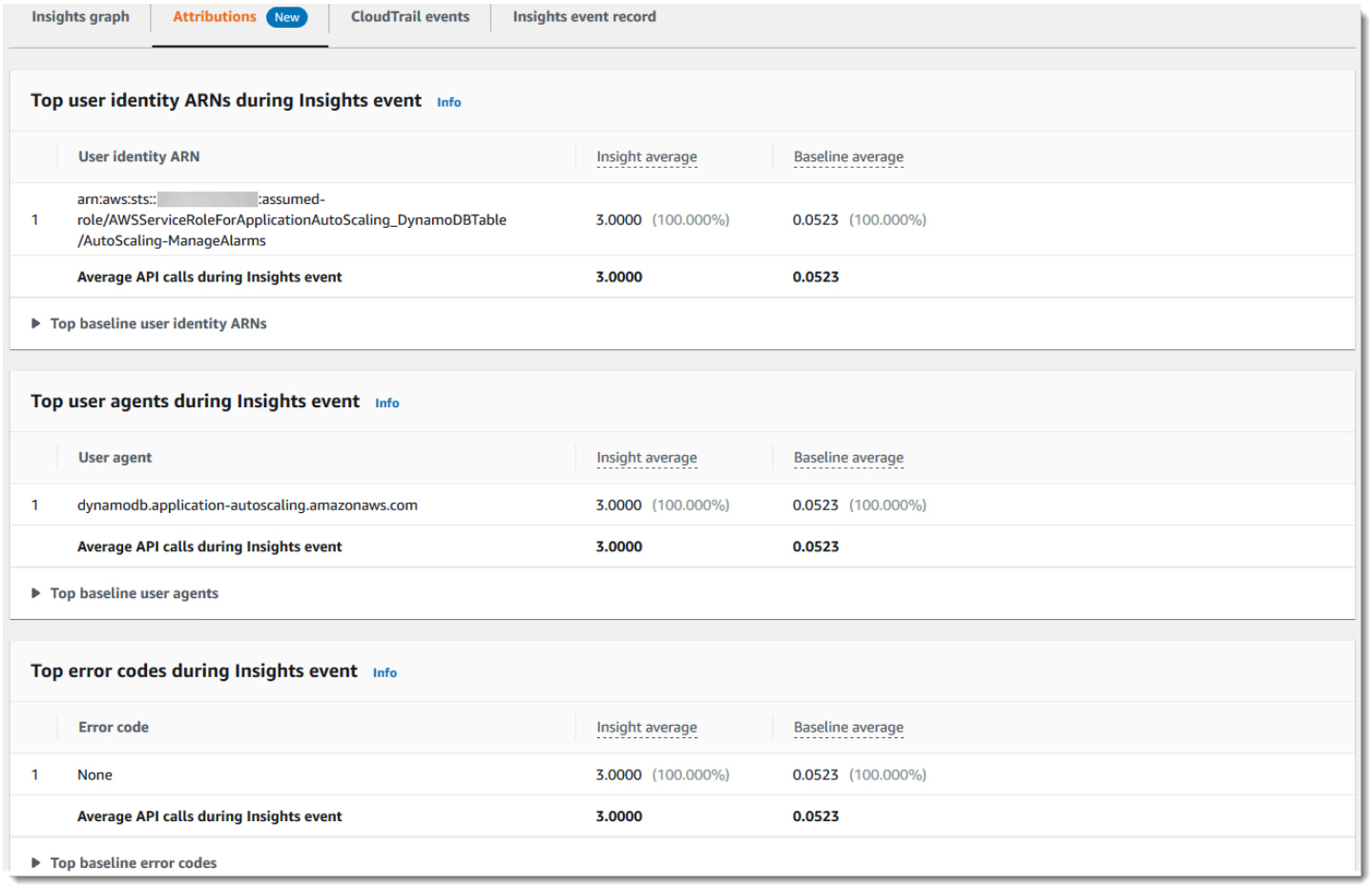
API エラー率 Insights イベントのための Insights グラフタブを次の画像に示します。強調表示されている領域では、`GetRolePolicy` IAM API コールでの `NoSuchEntityException` エラーの発生

が、API コールの 1 分あたりのベースライン平均 0.0017 NoSuchEntityException エラーを上回ったため (インサイト期間中に 1 分あたり平均 18 個のエラーが発生)、Insights イベントがログに記録されています。この例では、 CloudTrail インサイトイベントをトリガーしたイベントの数は、インサイトの 1 NoSuchEntityException 分間の平均エラー数 18 件と一致します。API コールレートのグラフとは異なり、API エラーレートは 2 本の線を対照的な色で示しています。片方は異常な数のエラーが発生した IAM API GetRolePolicy の呼び出しを測定する線で、もう片方は異常なアクティビティがログに記録されたエラー NoSuchEntityException を測定する線です。

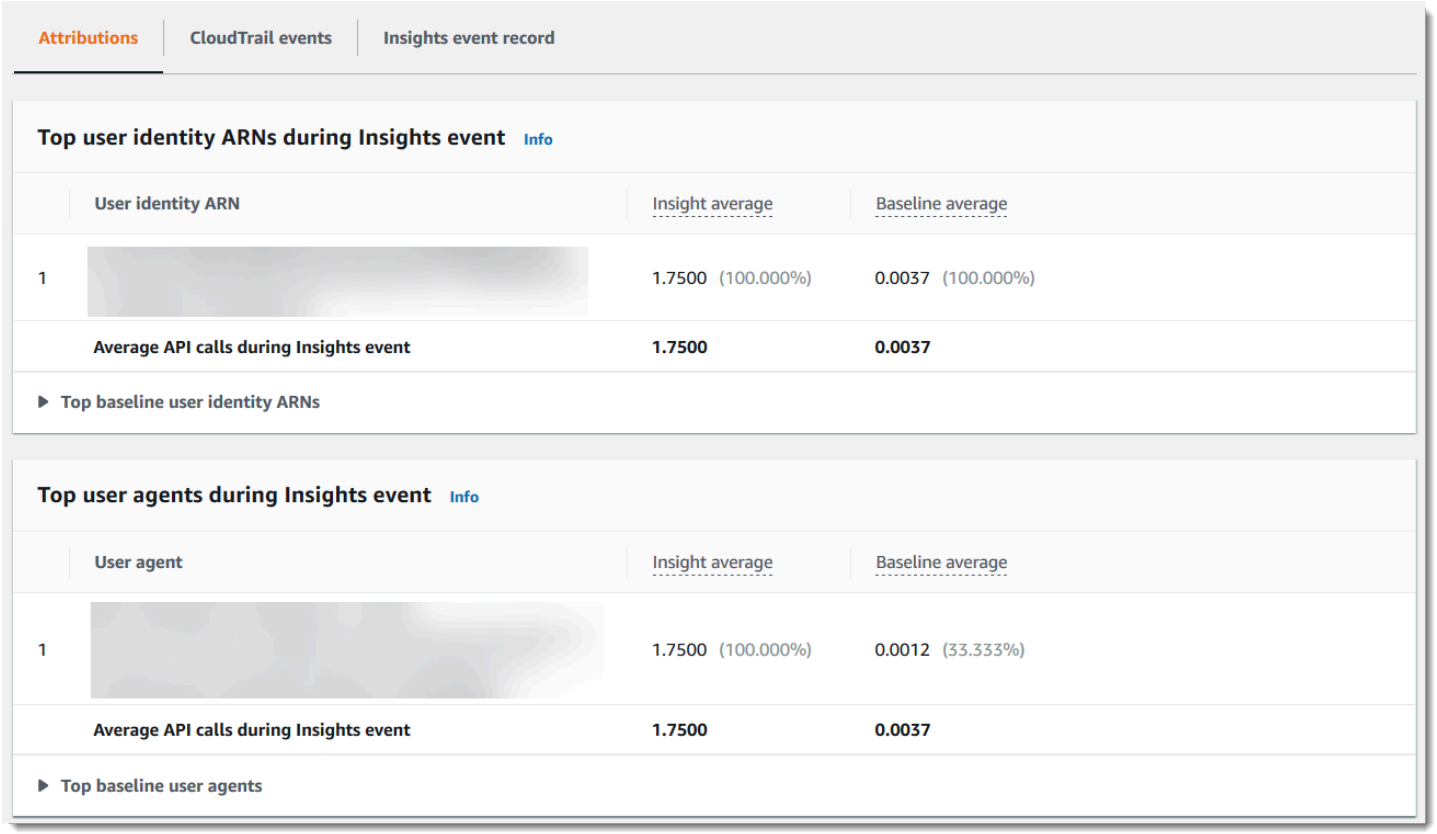


[Attributions] (属性) タブ

[属性] タブには、Insights イベントに関する次の情報が表示されます。[Attributions] (属性) タブは、Insights アクティビティの原因とソースを特定するのに役立ちます。上位ベースラインの領域を展開して、通常期間のユーザー ID、ユーザーエージェント、およびエラーコードアクティビティを、それらの Insights アクティビティ期間の結果と比較します。[Top baseline user identity ARNs] (上位ベースラインユーザー ID ARN)、[Top baseline user agents] (上位ベースラインエージェント)、および[Top baseline error codes] (上位ベースラインエラーコード) では、ベースライン平均のみが表示されます。ベースライン平均は、Insights イベントの開始時刻前の約 7 日間の、ユーザーアイデンティティもしくはユーザーエージェントによってログに記録される、またはエラーコードにつながる API のイベントの過去平均です。



次の図に示すように、[Attributions] (アトリビューション) タブには、エラーレートの Insights イベントの上位ユーザー ID ARN と上位ユーザーエージェントのみが表示されます。エラーレートの Insights イベントでは、上位エラーコードは必要ありません。



- 上位ユーザー ID ARN-この表には、 AWS 異常なアクティビティとベースライン期間中に API 呼び出しに貢献したユーザーまたは IAM ロール (ユーザー ID) の上位 5 件まで、寄与した API 呼び出しの平均数の降順で表示されます。異常なアクティビティに寄与したアクティビティ総数としての平均の割合を括弧内に示しています。5 以上のユーザー ID ARN が異常なアクティビティに寄与した場合、そのアクティビティは [Other] の列にまとめて表示されます。
- 上位ユーザーエージェント-この表には、 AWS 異常なアクティビティとベースライン期間中にユーザーIDがAPIコールに貢献したツールの上位5つまで、貢献したAPIコールの平均数の降順で表示されます。これらのツールには AWS Management Console、 AWS CLI、または SDK が含まれます。 AWS 例えば、`ec2.amazonaws.com` という名前のユーザーエージェントは、Amazon EC2 コンソールが API を呼び出すために使用されたツールの中にあったことを示します。異常なアクティビティに寄与したアクティビティ総数としての平均の割合を括弧内に示しています。5 以上のユーザーエージェントが異常なアクティビティに寄与した場合、そのアクティビティは [Other] の列にまとめて表示されます。
- Top error codes (上位エラーコード) - API コールレートの Insights イベントに対してのみ表示されます。この表は、異常なアクティビティおよびベースライン期間中に API コールで発生したエラーコードの上位 5 つまでを、API コールの最大数から最小数の順に表示しています。異常なアクティビティに寄与したアクティビティ総数としての平均の割合を括弧内に示しています。異常な

アクティビティまたはベースラインアクティビティ中に 5 つ以上のエラーコードが発生した場合は、それらのアクティビティは [Other] の列にまとめて表示されます。

None の値を上位 5 つのエラーコード値のうちの 1 つとして使用すると、Insights イベントに寄与したコールのかなりの割合がエラーにならなかったことを意味します。エラーコードの値が None、表内に他のエラーコードがない場合、[Insight average] および [Baseline average] の列は、Insights イベント全体の列と同じです。また、これらの値は、[API calls per minute] の [Insights graph] タブの [Insight average] および [Baseline average] 凡例に表示されます。

ベースライン平均とインサイト平均

ベースライン平均とインサイト平均は、上位ユーザ ID、上位ユーザエージェント、および上位エラーコードに対して表示されます。

- Baseline average (ベースライン平均) - アカウントの特定のリージョンで、過去約 7 日内に測定された、Insights イベント がログに記録された API での 1 分あたりの標準的な発生率。
- Insights average (インサイト平均) - Insights イベントをトリガーしたこの API の 1 分あたりのコールまたはエラーの割合。 CloudTrail 開始イベントのインサイト平均は、インサイトイベントをトリガーした API の 1 分あたりのコール数またはエラー率です。通常、これは異常なアクティビティの最初の 1 分です。終了イベントのインサイト平均は、開始 Insights イベントと終了 Insights イベントの間の異常なアクティビティの期間における 1 分あたりの API コールまたはエラーの割合です。

CloudTrail [イベント] タブ

[CloudTrail イベント] タブには、 CloudTrail異常なアクティビティが発生したと分析された関連イベントが表示されます。デフォルトで、フィルターはすでに Insights イベント名に適用されています。これは関連する API の名前でもあります。 CloudTrail 異常なアクティビティが発生した期間中に記録されたすべてのイベントを表示するには、「選択した Insights イベントのイベントのみを表示」をオフにします。CloudTrail イベントタブには、Insights イベントの開始時刻と終了時刻の間に発生した対象 API CloudTrail に関連する管理イベントが表示されます。これらのイベントは、より詳細な分析を実行して、Insights イベントの考えられる原因と、異常な API アクティビティとエラーレートアクティビティの理由を特定するのに役立ちます。

[Insights イベントレコード] タブ

CloudTrail 他のイベントと同様に、 CloudTrail Insights イベントは JSON 形式のレコードです。[Insights event record] タブには、Insights の開始イベントと終了イベントの JSON 構造とコンテン

ツが表示されます。これはイベントペイロードと呼ばれることもあります。Insights イベントレコードのフィールドとコンテンツの詳細については、このガイドの「Insights イベントのレコードフィールド」および「CloudTrail `insightDetails`インサイト要素」を参照してください。

Amazon CloudWatch ログへのトレイルイベントの送信

CloudTrail トレイルの Insights CloudWatch イベントをログに送信できます。Insights CloudWatch イベントをログロググループに送信するようにトレイルを設定すると、 CloudTrail Insights はトレイルで指定したイベントのみを送信します。たとえば、管理イベントと Insights イベントをログに記録するようにトレイルを設定すると、そのトレイルは管理イベントと Insights CloudWatch イベントをログロググループに配信します。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

CloudTrail レコードの内容

レコードの本文には、リクエストされたアクションと、リクエストがいつどこで行われたかを判断するのに役立つフィールドが含まれています。オプションの値が True の場合、そのフィールドは、サービス、API、またはイベントタイプに適用される場合にのみ表示されます。False のオプションの値は、そのフィールドが常に存在するか、その存在がサービス、API、またはイベントタイプに依存しないことを意味します。例は `responseElements` です。これは、変更を行うアクション (アクションの作成、更新、削除) のイベントに存在します。

CloudTrail フィールドの内容が最大フィールドサイズを超える場合、 はフィールドを切り捨てます。フィールドが切り捨てられると、`omitted` は `true` の値で示されます。

`eventTime`

リクエストが完了した日付と時刻、協定世界時 (UTC)。イベントのタイムスタンプは、API コールが行われたサービス API エンドポイントを提供するローカルホストから取得されます。例えば、米国西部 (オレゴン) リージョンで実行される CreateBucket API イベントは、Amazon S3 エンドポイント を実行している AWS ホストの時刻からタイムスタンプを取得します`s3.us-west-2.amazonaws.com`。一般に、 AWS サービスは Network Time Protocol (NTP) を使用してシステムクロックを同期します。

使用可能: 1.0 以降

オプション: False

`eventVersion`

ログイベント形式のバージョン。現在のバージョンは 1.10 です。

eventVersion の値は、*major_version*.*minor_version* の形式でメジャーおよびマイナーのバージョンです。例えば、eventVersion の値が 1.09 の場合には、1 がメジャーバージョンを示し、09 がマイナーバージョンを示します。

CloudTrail 下位互換性のないイベント構造が変更されると、 はメジャーバージョンを増やします。これには、既に存在する JSON フィールドの削除、またはフィールドの内容の表現方法 (日付形式など) の変更が含まれます。変更によってイベント構造に新しいフィールドが追加されると、 はマイナーバージョンを CloudTrail 増分します。これが発生する可能性があるのは、一部またはすべての既存のイベントに対して新しい情報が利用可能か、新しいイベントタイプでのみ新しい情報が利用可能な場合です。イベント構造の新しいマイナーバージョンとの将来の互換性を保つには、アプリケーションは新しいフィールドを無視する場合があります。

が新しいイベントタイプ CloudTrail を導入しても、イベントの構造が変更されない場合、イベントバージョンは変更されません。

アプリケーションがイベント構造を正しく解析できるようにするため、メジャーバージョン番号が同等かどうかの比較を行うことをお勧めします。アプリケーションに期待されるフィールドが存在することを確認するには、マイナーバージョンで greater-than-or-equal対 比較を実行することもお勧めします。マイナーバージョンには先頭のゼロはありません。*major_version* および *minor_version* を数値として解釈し、比較操作を実行できます。

使用可能: 1.0 以降

オプション: False

userIdentity

リクエストを作成した IAM アイデンティティに関する情報。詳細については、「CloudTrail userIdentity 要素」を参照してください。

使用可能: 1.0 以降

オプション: False

eventSource

リクエストが行われたサービス。この名前は通常、スペースなしのサービス名の短縮形に .amazonaws.com を付けたものです。例:

- AWS CloudFormation は ですcloudformation.amazonaws.com。
- Amazon EC2 は ec2.amazonaws.com です。

- Amazon Simple Workflow Service は `swf.amazonaws.com` です。

この規則にはいくつかの例外があります。例えば、Amazon `eventSource`の CloudWatch は ですす`monitoring.amazonaws.com`。

使用可能: 1.0 以降

オプション: False

`eventName`

リクエストされたアクション。そのサービスの API アクションの 1 つです。

使用可能: 1.0 以降

オプション: False

`awsRegion`

など、リクエスト AWS リージョン が行われた `us-east-2`。CloudTrail サポートされているリージョン を参照してください。

使用可能: 1.0 以降

オプション: False

`sourceIPAddress`

リクエストが行われた IP アドレス。サービスコンソールから行われたアクションの場合、報告されるアドレスは、コンソールウェブサーバーではなく、基礎となるカスタマーリソースのものです。のサービスの場合 AWS、DNS 名のみが表示されます。

> **Note**
>
> AWSからのイベントの場合、このフィールドは通常 `AWS Internal/#` で、`#` は内部で使用される数字です。

使用可能: 1.0 以降

オプション: False

userAgent

、 AWS サービス、 AWS SDKs AWS Management Console、 など、リクエストが行われたエージェント AWS CLI。このフィールドの最大サイズは 1 KB です。この制限を超えるコンテンツは切り捨てられます。以下は値の例です。

- `lambda.amazonaws.com` – リクエストは AWS Lambdaで行われました。
- `aws-sdk-java` – リクエストは AWS SDK for Javaで行われました。
- `aws-sdk-ruby` – リクエストは AWS SDK for Rubyで行われました。
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5` – リクエストは Linux に AWS CLI インストールされた で行われました。

> **Note**
>
> によって発信されたイベントの場合 AWS、 が呼び出し AWS のサービス を行ったことを CloudTrail 知っている場合、このフィールドは呼び出し元のサービスのイベントソースです (例: `ec2.amazonaws.com`)。それ以外の場合、このフィールドは です。ここでAWS Internal/#、 #は内部目的で使用される数値です。

使用可能: 1.0 以降

オプション: True

errorCode

リクエストが AWS エラーを返した場合のサービスエラー。このフィールドを示す例については、「エラーコードとメッセージログの例」を参照してください。このフィールドの最大サイズは 1 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.0 以降

オプション: True

errorMessage

リクエストがエラーを返す場合、エラーの説明。このメッセージには、承認失敗のメッセージが含まれます。 は、例外処理でサービスによって記録されたメッセージを CloudTrail キャプチャし

ます。例については、エラーコードとメッセージログの例を参照してください。このフィールドの最大サイズは 1 KB です。この制限を超えるコンテンツは切り捨てられます。

> **Note**
>
> 一部の AWS サービスでは、イベントの最上位フィールドerrorMessageとして errorCodeおよび が提供されます。他の AWS のサービスでは、responseElements の一部としてエラー情報を提供します。

使用可能: 1.0 以降

オプション: True

requestParameters

リクエストとともに送信されたパラメータ (ある場合)。これらのパラメータは、適切な AWS サービスの API リファレンスドキュメントに記載されています。このフィールドの最大サイズは 100 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.0 以降

オプション: False

responseElements

変更 (アクションの作成、更新、削除) を行うアクションのレスポンス要素がある場合。アクションが
はレスポンス要素を返しません。このフィールドは ですnull。の場合
アクションの状態は変更されません (オブジェクトの取得や一覧表示のリクエストなど)。
この要素は省略されます。アクションのレスポンス要素は、 API リファレンスに記載されています。
適切な のドキュメント AWS のサービス。このフィールドの最大サイズ
100 KB 。この制限を超えるコンテンツは切り捨てられます。

responseElements 値は、リクエストの追跡に役立ちます。
と AWS Support。x-amz-request-id と の両方 x-amz-id-2
には、 を使用してリクエストを追跡するのに役立つ情報が含まれています AWS Support。これらの値は

リクエストに対するレスポンスでサービスが返すものと同じ
はイベントを開始するため、イベントを と照合するために使用できます。
リクエスト。

使用可能: 1.0 以降

オプション: False

additionalEventData

リクエストまたはレスポンスの一部ではないイベントに関する追加のデータ。このフィールドの最大サイズは 28 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.0 以降

オプション: True

requestID

リクエストを識別する値。呼び出されているサービスがこの値を生成します。このフィールドの最大サイズは 1 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.01 以降

オプション: True

eventID

各イベントを一意に識別 CloudTrail するために によって生成された GUID。この値を使用して、単一のイベントを識別できます。たとえば、プライマリキーとして ID を使用し、検索可能なデータベースから ログデータを取得できます。

使用可能: 1.01 以降

オプション: False

eventType

イベントレコードを生成したイベントのタイプを識別します。これは、次のいずれかの値になります。

- AwsApiCall – API が呼び出されました。
- AwsServiceEvent – サービスはトレイルに関連するイベントを生成しました。たとえば、これは、自分が所有するリソースで別のアカウントが呼び出しをした場合に発生することがあります。
- AwsConsoleAction - コンソールで API コールではないアクションが実行されました。
- AwsConsoleSignIn – アカウントにサインインしたユーザー (ルート、IAM、フェデレーティッド、SAML、または SwitchRole ） AWS Management Console。
- AwsCloudTrailInsight – Insights イベントが有効になっている場合、 はリソースプロビジョニングのスパイクや AWS Identity and Access Management (IAM) アクションのバーストなど、異常な運用アクティビティ CloudTrail を検出すると Insights イベント CloudTrail を生成します。

  AwsCloudTrailInsight イベントは次のフィールドを使用しません:

  - eventName
  - eventSource
  - sourceIPAddress
  - userAgent
  - userIdentity

使用可能: 1.02 以降

オプション: False

apiVersion

AwsApiCalleventType 値に関連付けられた API バージョンを識別します。

使用可能: 1.01 以降

オプション: True

managementEvent

イベントが管理イベントかどうかを識別するブール値。eventVersion が 1.06 以上で、イベントタイプが次のいずれかである場合、managementEvent がイベントレコードに表示されます。

- AwsApiCall

- AwsConsoleAction
- AwsConsoleSignIn
- AwsServiceEvent

使用可能: 1.06 以降

オプション: True

readOnly

この操作が、読み取り専用オペレーションであるかどうかを識別します。これは、以下の値のいずれかになります。

- true – オペレーションは読み取り専用です (例:DescribeTrails)。
- false – オペレーションは書き込み専用です (例:DeleteTrail)。

使用可能: 1.01 以降

オプション: True

resources

イベントでアクセスされたリソースのリスト。このフィールドには以下の情報が含まれます。

- リソース ARN
- リソース所有者のアカウント ID
- 以下の形式でのリソースタイプ識別子 : AWS::*aws-service-name*::*data-type-name*

たとえば、AssumeRole イベントが記録されると、resources フィールドは次のようになります。

- ARN: arn:aws:iam::123456789012:role/*myRole*
- アカウント ID: 123456789012
- リソースタイプ識別子 : AWS::IAM::Role

resources フィールドを使用したログの例については、「IAM ユーザーガイドAWS STS 」の CloudTrail 「ログファイルの API イベント」または「 AWS Key Management Service デベロッパーガイド」のAWS KMS 「API コールのログ記録」を参照してください。

使用可能: 1.01 以降

オプション: True

recipientAccountId

このイベントを受信したアカウント ID を表します。recipientAccountID は CloudTrail userIdentity 要素 accountId とは異なる場合があります。これは、クロスアカウントのリソースへのアクセスで発生することがあります。例えば、AWS KMS key とも呼ばれる KMS キーが別のアカウントで使用されて、暗号化 APIが呼び出された場合、accountId の値と recipientAccountID の値は、呼び出しを行ったアカウントに配信されるイベントでは同じになりますが、KMS キーを所有するアカウントに配信されるイベントでの値は異なります。

使用可能: 1.02 以降

オプション: True

serviceEventDetails

イベントをトリガーしたものとその結果を含むサービスイベントを識別します。詳しくは、AWS サービスイベント を参照してください。このフィールドの最大サイズは 100 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.05 以降

オプション: True

sharedEventID

異なる AWS アカウントに送信されるのと同じ AWS アクションからの CloudTrail イベント CloudTrail を一意に識別するために によって生成される GUID。

例えば、アカウントAWS KMS keyが別のアカウントに属する を使用する場合、KMS キーを使用したアカウントと KMS キーを所有するアカウントは、同じアクションに対して個別の CloudTrail イベントを受け取ります。この AWS アクションで配信される各 CloudTrail イベントは同じ を共有しますがsharedEventID、一意の eventIDと もありますrecipientAccountID。

詳細については、「sharedEventID の例」を参照してください。

> **Note**
>
> sharedEventID フィールドは、 CloudTrail イベントが複数のアカウントに配信される場合にのみ表示されます。発信者と所有者が同じ AWS アカウントである場合、 は 1 つのイベントのみ CloudTrail を送信し、 sharedEventIDフィールドは存在しません。

使用可能: 1.03 以降

オプション: True

vpcEndpointId

VPC から Amazon S3 などの別の AWS のサービスへのリクエストが行われた VPC エンドポイントを識別します。

使用可能: 1.04 以降

オプション: True

eventCategory

イベントカテゴリを表示します。eventCategory は、管理イベントと Insights イベントの[LookupEvents]呼び出しに使用されます。

- 管理イベントの場合、値は Management です。
- データイベントの場合、値は Data です。
- Insights イベントの場合、値は Insight です。

使用可能: 1.07 以降

オプション: False

addendum

イベントの配信が遅れた場合、またはイベントの記録後に既存のイベントに関する追加情報が使用可能になった場合、補遺フィールドにはイベントが遅れた理由に関する情報が表示されます。既存のイベントから情報が欠落している場合、補遺フィールドには、不足している情報と、不足している理由が表示されます。内容は以下が含まれます。

- **reason** - イベントまたはその内容の一部が欠落していた理由。値は以下のいずれかです。

- **DELIVERY_DELAY** - イベントの配信に遅延がありました。これは、ネットワークトラフィックの増加、接続の問題、または CloudTrail サービスの問題が原因である可能性があります。
- **UPDATED_DATA** - イベントレコードのフィールドが見つからないか、正しくない値がありました。
- **SERVICE_OUTAGE** – イベントを にログ記録し、 CloudTrail にイベントを記録できなかったサービス CloudTrail。これは非常にまれです。

- **updatedFields** - 補遺によって更新されるイベントレコードフィールド。これは、理由が UPDATED_DATA の場合にのみ提供されます。
- **originalRequestID** - リクエストの元の一意の ID。これは、理由が UPDATED_DATA の場合にのみ提供されます。
- **originalEventID** - 元のイベントの ID。これは、理由が UPDATED_DATA の場合にのみ提供されます。

使用可能: 1.08 以降

オプション: True

sessionCredentialFromConsole

AWS Management Console イベントがセッションから発生したかどうかを示します。このフィールドは、値が `true` でなければ表示されません。つまり、API コールを行うために使用されたクライアントは、プロキシまたは外部クライアントのいずれかでなければ表示されません。プロキシクライアントが使用された場合、`tlsDetails` イベントフィールドは表示されません。

使用可能: 1.08 以降

オプション: True

edgeDeviceDetails

リクエストのターゲットであるエッジデバイスに関する情報を表示します。現在、S3 Outposts デバイスイベントには、このフィールドが含まれます。このフィールドの最大サイズは 28 KB です。この制限を超えるコンテンツは切り捨てられます。

使用可能: 1.08 以降

オプション: True

tlsDetails

サービス API コールで使用されるクライアント提供のホスト名の Transport Layer Security (TLS) バージョン、暗号スイート、および完全修飾ドメイン名 (FQDN) に関する情報を表示します。こ

れは通常、サービスエンドポイントの FQDN です。 CloudTrail は、予想される情報が欠落しているか、空の場合、TLS の詳細の一部をログに記録します。例えば、TLS バージョンと暗号スイートが存在するが、 HOSTヘッダーが空の場合、使用可能な TLS の詳細はイベントに記録されます CloudTrail 。

- **tlsVersion** - リクエストの TLS バージョン。
- **cipherSuite** - リクエストの暗号スイート (使用されるセキュリティアルゴリズムの組み合わせ)。
- **clientProvidedHostHeader** - サービス API コールで使用されるクライアント提供のホスト名 (通常はサービスエンドポイントの FQDN)。

> **Note**
>
> tlsDetails フィールドがイベントレコードに存在しない場合があります。
>
> - API コールが AWS のサービス ユーザーに代わって によって実行された場合、tlsDetailsフィールドは存在しません。userIdentity 要素内の invokedBy フィールドは、API 呼び出しを行った AWS のサービス を識別します。
> - sessionCredentialFromConsole が true の値を持つ場合、tlsDetails は、API 呼び出しを行うために外部クライアントが使用された場合にのみイベントレコードに存在します。

使用可能: 1.08 以降

オプション: True

Insights イベントのレコードフィールド

インサイトイベントの JSON 構造に表示される属性を以下に示します。管理イベントやデータイベントとは異なります。

sharedEventId

sharedEventID for CloudTrail Insights イベントは、イベントの管理タイプとデータ型sharedEventIDで CloudTrailとは異なります。Insights イベントでは、 sharedEventIDは CloudTrail Insights イベントを一意に識別するために Insights によって生成される GUID です。sharedEventIDは、Insights の開始イベントと終了イベントの間で一般的であり、両方のイベ

ントを接続して異常なアクティビティを一意に識別するのに役立ちます。sharedEventID は、全体的なインサイトイベント ID と考えることができます。

使用可能: 1.07 以降

オプション: False

insightDetails

インサイトイベントのみ。イベントソース、ユーザーエージェント、統計情報、API 名、イベントがインサイトイベントの開始か終了かなど、インサイトイベントの基礎となるトリガーに関する情報を示します。insightDetails ブロックの内容の詳細については、「CloudTrail insightDetailsインサイト要素」を参照してください。

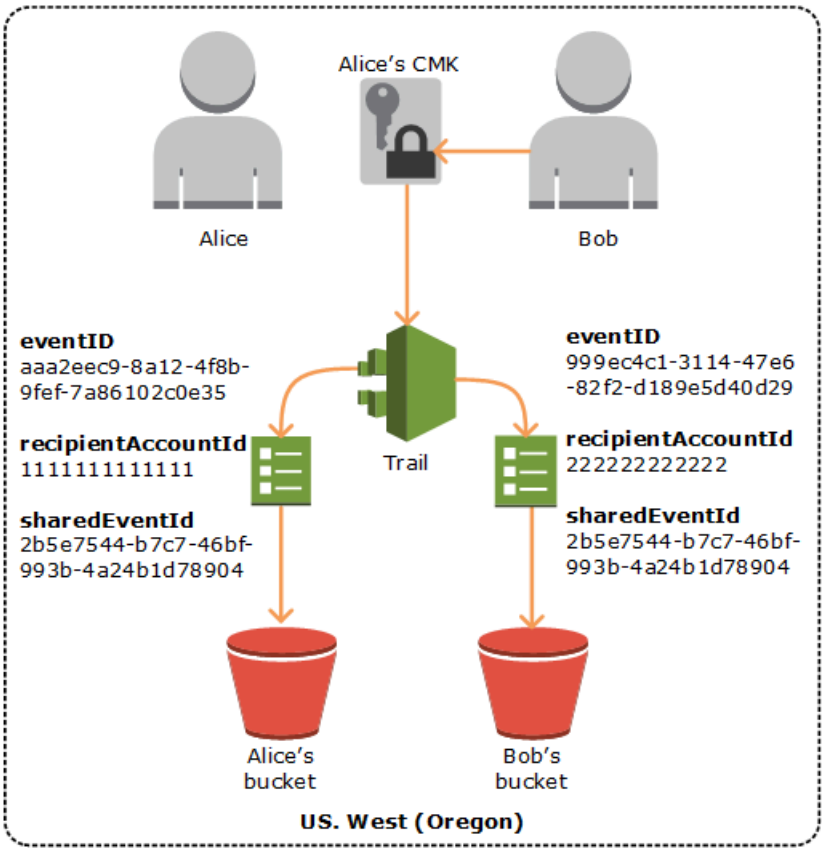
使用可能: 1.07 以降

オプション: False

sharedEventID の例

以下は、 が同じアクションに対して 2 つのイベントを CloudTrail が配信する方法を説明する例です。

1. Alice には AWS アカウント (111111111111) があり、 を作成します AWS KMS key。彼女はこの KMS キーの所有者です。
2. Bob には AWS アカウント (222222222222) があります。Alice は、Bob に KMS キーの使用を許可します。
3. 各アカウントにはトレイルおよび別のバケットがあります。
4. Bob は、KMS キーを使用して Encrypt API を呼び出します。
5. CloudTrail は 2 つの異なるイベントを送信します。
   - 1 つのイベントが Bob に送信されます。このイベントは、Bob が KMS キーを使用したことを示します。
   - 1 つのイベントが Alice に送信されます。このイベントは、Bob が KMS キーを使用したことを示します。
   - イベントと同じ sharedEventID ですが、eventID および recipientAccountID は一意です。



CloudTrail Insights の共有イベント IDs

`sharedEventID` for CloudTrail Insights イベントは、 CloudTrail イベントの管理タイプとデータ型`sharedEventID`で とは異なります。Insights イベントでは、 `sharedEventID`は CloudTrail Insights イベントの開始ペアと終了ペアを一意に識別するために Insights によって生成される GUID です。 `sharedEventID`は、開始 Insights イベントと終了 Insights イベントの間で一般的であり、両方のイベント間の相関関係を作成して異常なアクティビティを一意に識別するのに役立ちます。

`sharedEventID` は、全体的なインサイトイベント ID と考えることができます。

CloudTrail userIdentity 要素

AWS Identity and Access Management (IAM) は、さまざまなタイプの ID を提供します。`userIdentity` エレメントには、リクエストを行った IAM アイデンティティのタイプとどの認証情報が使用されたかに関する詳細が含まれます。一時的認証情報が使用された場合、エレメントは、認証情報がどのように取得されたかを示します。

目次

- フィールド
- SAML とウェブ ID AWS STS フェデレーションを使用する API の値
- AWS STS ソース ID

例

IAM ユーザー認証情報を使用する **userIdentity**

次の例は、userIdentity という名前の IAM ユーザー認証情報で行われた単純なリクエストの Alice エレメントを示しています。

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "",
  "userName": "Alice"
}
```

一時的セキュリティ認証情報を使用する **userIdentity**

次の例は、IAM ロールを引き受けることにより取得した一時的セキュリティ認証情報を使用して行われたリクエストの userIdentity エレメントを示しています。エレメントには、認証情報を取得するために引き受けられたロールに関する追加の情報の詳細が含まれています。

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
    "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",
    "accountId": "123456789012",
    "accessKeyId": "",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "20131102T010628Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIDPPEZS35WEXAMPLE",
```

```
        "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
        "accountId": "123456789012",
        "userName": "RoleToBeAssumed"
      }
    }
}
```

IAM アイデンティティーセンターのユーザーに代わって行われたリクエストの **userIdentity**

次の例は、IAM アイデンティティセンターのユーザーに代わって行われたリクエスト の userIdentity 要素を示しています。

```
"userIdentity": {
 "type": "IdentityCenterUser",
 "accountId": "123456789012",
 "onBehalfOf": {
  "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
  "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9067642ac7"
 },
 "credentialId": "EXAMPLEVHULjJdTUdPJfofVa1sufHDoj7aYcOYcxFVllWR_Whr1fEXAMPLE"
}
```

フィールド

以下のフィールドは userIdentity エレメントに表示されます。

type

ID のタイプ。以下の値を指定できます。

- Root— AWS アカウント リクエストはお客様の認証情報を使用して行われました。userIdentity タイプが Root で、アカウントのエイリアスを設定した場合、userName フィールドには、アカウントエイリアスが含まれます。詳細については、「AWS アカウント ID とそのエイリアス」を参照してください。
- IAMUser – リクエストが IAM ユーザーの認証情報を使用して行われました。
- AssumedRole – リクエストは、 AWS Security Token Service (AWS STS) AssumeRole API を呼び出すことによってロールで取得された一時的なセキュリティ認証情報を使用して行われました。これには、Amazon EC2 およびクロスアカウント API アクセスのロールが含まれる場合があります。

- Role— リクエストは、特定の許可を持つ永続的な IAM アイデンティティを使用して行われました。ロールセッションの発行者は常にロールです。ロールの詳細については、IAM ユーザーガイド の「ロールに関する用語と概念」を参照してください。
- FederatedUser— AWS STS GetFederationTokenAPI の呼び出しから取得した一時的なセキュリティ認証情報を使用してリクエストが行われました。sessionIssuer エレメントは、API がルートまたは IAM ユーザー認証情報で呼び出されたかどうかを示します。

  一時的なセキュリティ認証情報の詳細については、IAM ユーザーガイドの「IAM の一時的なセキュリティ認証情報」を参照してください。
- Directory — リクエストがディレクトリサービスに対して行われ、タイプが不明です。ディレクトリサービスには、Amazon WorkDocs と Amazon が含まれます QuickSight。
- AWSAccount— リクエストは別のユーザーによって行われました。 AWS アカウント
- AWSService— リクエストは、 AWS アカウント に所属するによって行われました AWS のサービス。たとえば、は、お客様のアカウントの IAM AWS Elastic Beanstalk ロールを引き受け、 AWS のサービス お客様に代わって他のユーザーに電話をかけます。
- IdentityCenterUser - IAM アイデンティティーセンターのユーザーに代わって行われたリクエスト
- Unknown— CloudTrail 特定できない ID タイプでリクエストが送信されました。

オプション: False

所有する IAM ロールを使用するクロスアカウントアクセスがある場合、AWSAccount と AWSService が、ログに type として表示されます。

例: 別の AWS アカウントによって開始されたクロスアカウントアクセス

1. アカウントには、IAM ロールがあります。
2. AWS 別のアカウントがそのロールに切り替わり、自分のアカウントのロールを引き継ぎます。
3. IAM ロールを所有しているため、他のアカウントがロールを引き受けたことを示すログを受信します。type は、AWSAccount です。ログエントリの例については、「AWS STS CloudTrail ログファイルの API イベント」を参照してください。

例:サービスによって開始されたクロスアカウントアクセス AWS

1. アカウントには、IAM ロールがあります。
2. AWS AWS サービスが所有するアカウントがその役割を引き受けます。

3. IAM ロールを所有しているため、 AWS サービスがロールを引き受けたことを示すログを受信します。type は、AWSService です。

userName

呼び出しを行った ID のフレンドリ名。userName に表示される値は、type の値に基づいています。次の表は、type と userName の関係を示しています。

type	userName	説明
Root (エイリアスセットなし)	[なし]	にエイリアスを設定していない場合 AWS アカウント、userNameそのフィールドは表示されません。アカウントエイリアスの詳細については、「Your AWS アカウント ID とそのエイリアス」を参照してください。Root は、ユーザー名ではなく ID の種類であるため、userName フィールドには、Root を含むことができないことに注意してください。
Root (エイリアスセット)	アカウントエイリアス	エイリアスの詳細については、「Your AWS アカウント ID AWS アカウント とそのエイリアス」を参照してください。
IAMUser	IAM ユーザーのユーザー名	
AssumedRole	[なし]	AssumedRole タイプの場合、**sessionIssuer** エレメントの一部として、sessionContext 内の userName フィールドを見つけることができます。エントリの例については、「例」を参照してください。
Role	ユーザー定義	sessionContext および sessionIssuer セクションには、ロールのセッションを発行した ID 関する情報が含まれています。
FederatedUser	[なし]	sessionContext および sessionIssuer セクションには、フェデレーションユーザーのセッ

type	userName	説明
		ションを発行した ID 関する情報が含まれています。
Directory	存在する場合があります	例えば、値は、アカウントエイリアスまたは関連する AWS アカウント ID の E メールアドレスの場合があります。
AWSService	[なし]	
AWSAccount	[なし]	
IdentityCenterUser	[なし]	onBehalfOf セクションには、呼び出しが行われた IAM アイデンティティセンターのユーザー ID とアイデンティティストア ARN に関する情報が含まれています。IAM アイデンティティセンターの詳細については、AWS IAM Identity Center ユーザーガイドを参照してください。
Unknown	存在する場合があります	例えば、値は、アカウントエイリアスまたは関連する AWS アカウント ID の E メールアドレスの場合があります。

> **Note**
>
> userName フィールドには、記録されたイベントが正しくないユーザー名の入力によって引き起こされたコンソールサインインの失敗である場合、文字列 HIDDEN_DUE_TO_SECURITY_REASONS が入ります。CloudTrail この場合は、次の例のようにテキストに機密情報が含まれている可能性があるため、内容は記録されません。
>
> - ユーザーが誤ってユーザー名フィールドにパスワードを入力した。
> - ユーザーは、 AWS あるアカウントのサインインページのリンクをクリックし、別のアカウントのアカウント番号を入力します。
> - ユーザーが、個人の E メールアカウント、銀行のサインイン ID、その他のプライベート ID のアカウント名を誤って入力した。

オプション: True

principalId

呼び出しを行ったエンティティの一意の識別子 一時的セキュリティ認証情報で行われたリクエストの場合、この値には、AssumeRole、AssumeRoleWithWebIdentity、GetFederationToken API 呼び出しに渡されるセッション名が含まれます。

オプション: True

arn

呼び出しを行ったプリンシパルの Amazon リソースネーム (ARN)。arn の最後のセクションには、呼び出しを行ったユーザーまたはロールが含まれています。

オプション: True

accountId

リクエストに対するアクセス許可を付与したエンティティを所有するアカウント。リクエストが、一時的なセキュリティ認証情報で行われた場合、これは、認証情報を取得するために使用された IAM ユーザーまたはロールを所有するアカウントです。

リクエストが、IAM アイデンティティセンターの承認済みアクセストークンを使って実行された場合、これが、IAM アイデンティティセンターインスタンスを所有するアカウントになります。

オプション: True

accessKeyId

リクエストに署名するために使用された アクセスキー ID。リクエストが、一時的セキュリティ認証情報で行われた場合、これは、一時的認証情報のアクセスキー IDです。セキュリティ上の理由から、accessKeyId が存在しないか、空の文字列として表示される可能性があります。

オプション: True

sessionContext

リクエストが、一時的なセキュリティ認証情報を使用して行われた場合、sessionContext はこれらの認証情報のために作成されたセッションに関する情報を提供します。一時的認証情報を返す API を呼び出すと、セッションを作成できます。また、ユーザーはコンソールで作業する際に、セッションを作成し、多要素認証を含む API を使用してリクエストを行います。この要素には、次の属性があります。

- `creationDate` – 一時的セキュリティ認証情報が発行された日付と時刻。ISO 8601 の基本表記で表されます。
- `mfaAuthenticated` – また、リクエストに認証情報が使用されたルートユーザーまたは IAM ユーザーも、MFA デバイスで認証された場合、この値は、`true` です。そうでない場合は、`false` です。
- `sourceIdentity` - このトピックの「AWS STS ソース ID」を参照してください。`sourceIdentity` フィールドは、ユーザーがアクションを実行するために IAM ロールを引き受けるときにイベントで発生します。`sourceIdentity` は、リクエストを行う元のユーザーアイデンティティを識別します。そのユーザーのアイデンティティが IAM ユーザー、IAM ロール、SAML ベースのフェデレーションで認証されたユーザー、OpenID Connect (OIDC) 準拠のウェブ ID フェデレーションで認証されたユーザーのいずれであるかを示します。ソース ID AWS STS 情報を収集するための設定の詳細については、IAM ユーザーガイドの「想定ロールで実行されるアクションの監視と制御」を参照してください。
- `ec2RoleDelivery` – Amazon EC2 インスタンスメタデータサービスバージョン 1 (IMDSv1) によって認証情報が提供された場合、値は `1.0` です。新しい IMDS スキームを使用して認証情報が提供された場合、値は `2.0` です。

  AWS Amazon EC2 インスタンスメタデータサービス (IMDS) によって提供される認証情報には、ec2: RoleDelivery IAM コンテキストキーが含まれます。このコンテキストキーを使用すると、IAM ポリシー、リソースポリシー、 service-by-service またはサービスコントロールポリシーの条件としてコンテキストキーを使用することにより、新しいスキームを簡単に OR resource-by-resource AWS Organizations ベースで使用できます。詳細については、「Amazon EC2 User Guide for Linux Instances」(Linux インスタンス用 Amazon EC2 ユーザーガイド) の「Instance metadata and user data」(インスタンスメタデータとユーザーデータ) を参照してください。

オプション: True

`invokedBy`

Amazon EC2 Auto Scaling AWS のサービス やなどによってリクエストが行われた場合の、リクエストを行った人の名前 AWS Elastic Beanstalk。 AWS のサービス このフィールドは、によってリクエストが行われた場合にのみ表示されます AWS のサービス。これには、転送アクセスセッション (FAS) を使用するサービス、 AWS のサービス プリンシパル、サービスにリンクされたロール、またはが使用するサービスロールからのリクエストが含まれます。 AWS のサービス

オプション: True

sessionIssuer

リクエストが一時的なセキュリティ認証情報を使用して行われた場合、sessionIssuerはユーザーが認証情報を取得した方法に関する情報を提供します。たとえば、ユーザーがロールを引き受けることで一時的セキュリティ認証情報を取得した場合、このエレメントは、引き受けたロールに関する情報を提供します。ユーザーが AWS STS GetFederationToken を呼び出すためのルートまたは IAM ユーザー認証情報で認証情報取得した場合、エレメントは、ルートアカウントまたは IAM ユーザーに関する情報を提供します。この要素には、次の属性があります。

- type – Root、IAMUser、Role などの一時的セキュリティ認証情報のソース。
- userName – セッションを発行したユーザーまたはロールのフレンドリ名。表示される値は、sessionIssuer ID type によって異なります。次の表は、sessionIssuer type と userName の関係を示しています。

sessionIssuer タイプ	**userName**	説明
Root (エイリアスセットなし)	[なし]	アカウントのエイリアスを設定していない場合、userName フィールドは表示されません。エイリアスの詳細については、「ID AWS アカウント とそのエイリアス」を参照してください。AWS アカウントRoot は、ユーザー名ではなく ID の種類であるため、userName フィールドには、Root を含むことができないことに注意してください。
Root (エイリアスセット)	アカウントエイリアス	エイリアスの詳細については、「AWS アカウント ID AWS アカウント とそのエイリアス」を参照してください。
IAMUser	IAM ユーザーのユーザー名	これは、フェデレーションユーザーが、IAMUser によって発行されたセッションを使用している場合にも適用されます。
Role	ロール名	IAM ユーザーまたはウェブ ID フェデレーティッドユーザーがロールセッションで引き受けるロール。 AWS のサービス

- principalId – 認証情報を取得するために使用されたエンティティの内部 ID。

- arn – 一時的セキュリティ認証情報を取得するために使用されたソース (アカウント、IAM ユーザー、ロール) のARN。
- accountId – 認証情報を取得するために使用されたエンティティを所有するアカウント。

オプション: True

onBehalfOf

リクエストが IAM アイデンティティセンターの呼び出し元によって行われた場合、onBehalfOf は、呼び出しが行われた IAM アイデンティティセンターのユーザー ID とアイデンティティストア ARN に関する情報を提供します。この要素には、次の属性があります。

- userId — 呼び出しが代理で実行された IAM アイデンティティセンターユーザーの ID。
- identityStoreArn — 呼び出しが代理で実行された IAM アイデンティティセンターの、アイデンティティストアの ARN。

オプション: True

credentialId

リクエストの認証情報 ID です。呼び出し元がベアラートークン (IAM アイデンティティセンターが認証したアクセストークンなど) を使用している場合のみ、設定されます。

オプション: True

webIdFederationData

リクエストが、ウェブ ID フェデレーションによって取得された一時的セキュリティ認証情報で行われた場合、webIdFederationData は ID プロバイダーに関する情報を一覧表示します。

この要素には、次の属性があります。

- federatedProvider – ID プロバイダーのプリンシパル名 (たとえば、Login with Amazon の場合は、www.amazon.com、Google の場合は、accounts.google.com)。
- attributes – プロバイダーからレポートされるアプリケーションの ID とユーザー ID (たとえば、Login with Amazon の場合は、www.amazon.com:app_id と www.amazon.com:user_id)。

> **Note**
>
> このフィールドが省略されたり、値が空だったりすると、ID プロバイダーに関する情報がないことを意味します。

オプション: True

SAML とウェブ ID AWS STS フェデレーションを使用する API の値

AWS CloudTrail セキュリティアサーションマークアップ言語 AWS Security Token Service (SAML AWS STS) とウェブ ID フェデレーションによるロギング () API 呼び出しをサポートします。ユーザーがと AssumeRoleWithWebIdentityAPI を呼び出すと、AssumeRoleWithSAML CloudTrail その呼び出しを記録し、イベントを Amazon S3 バケットに配信します。

これらの API の userIdentity エレメントには、次の値が含まれています。

type

ID のタイプ。

- SAMLUser – リクエストは、SAML アサーションを使用して行われました。
- WebIdentityUser – リクエストは、ウェブ ID フェデレーションプロバイダーによって行われました。

principalId

呼び出しを行ったエンティティの一意の識別子

- SAMLUser の場合、これは、saml:namequalifier キーと saml:sub キーの組み合わせです。
- WebIdentityUser の場合は、これは、発行者、アプリケーション ID、ユーザー ID の組み合わせです。

userName

呼び出しを行った ID の名前。

- SAMLUser の場合、これは、saml:sub キーです。
- WebIdentityUser の場合、これはユーザー ID です。

identityProvider

外部 ID プロバイダーのプリンシパル名。このフィールドは、SAMLUser または WebIdentityUser タイプに対してのみ表示されます。

- SAMLUser の場合、これは、SAML アサーションの saml:namequalifier キーです。

- WebIdentityUser の場合、これは、ウェブ ID フェデレーションプロバイダーの発行者の名前です。これは、次のように設定したプロバイダーになります。
  - cognito-identity.amazon.com Amazon Cognito for iOS
  - Login with Amazon の場合 www.amazon.com
  - Google の場合 accounts.google.com
  - Facebook の場合 graph.facebook.com

AssumeRoleWithWebIdentity アクションの userIdentity エレメントの例を次に示します。

```
"userIdentity": {
    "type": "WebIdentityUser",
    "principalId": "accounts.google.com:application-id.apps.googleusercontent.com:user-id",
    "userName": "user-id",
    "identityProvider": "accounts.google.com"
  }
```

userIdentitySAMLUserWebIdentityUser要素の表示方法やタイプのログの例については、「AWS CloudTrailでの IAM および AWS STS API 呼び出しの口ギング」を参照してください。

AWS STS ソース ID

IAM 管理者は、一時的な認証情報を使用してロールを引き受ける際に、ユーザーに ID AWS Security Token Service の指定を要求するように設定できます。sourceIdentity フィールドは、ユーザーが IAM ロールを引き受けるとき、または引き受けたロールでアクションを実行するときに、イベントで発生します。

sourceIdentity フィールドは、リクエストを行う元のユーザーアイデンティティを識別します。そのユーザーのアイデンティティが IAM ユーザー、IAM ロール、SAML ベースのフェデレーションを使用して認証されたユーザー、OpenID Connect (OIDC) 準拠のウェブ ID フェデレーションを使用して認証されたユーザーのいずれであるかを示します。IAM 管理者が設定したら AWS STS、CloudTrail sourceIdentity以下のイベントとイベントレコード内の場所に情報を記録します。

- ユーザー ID がロールを引き受けるときに実行する AWS STS AssumeRoleAssumeRoleWithSAML、、AssumeRoleWithWebIdentityまたはの呼び出し。sourceIdentityrequestParameters AWS STS 呼び出しのブロック内にあります。
- ユーザー ID がロールを使用して別のロールを引き受ける場合に発生する AWS STS AssumeRole、AssumeRoleWithSAML、AssumeRoleWithWebIdentityまたは呼び出し

は、ロールチェイニングと呼ばれます。 sourceIdentityrequestParameters AWS STS は呼び出しのブロックにあります。

- AWS サービス API は、ロールを引き受け、 AWS STSによって割り当てられた一時的な認証情報を使用して、ユーザー ID が実行する呼び出しを行います。サービス API イベントでは、sourceIdentity は、sessionContext ブロックにあります。例えば、ユーザーアイデンティティによって新しい S3 バケットが作成された場合、sourceIdentity は、CreateBucket イベントの sessionContext ブロックで発生します。

ソース ID AWS STS 情報を収集するように設定する方法の詳細については、IAM ユーザーガイドの「引き受けたロールで実行されるアクションの監視と制御」を参照してください。 AWS STS ログに記録されるイベントの詳細については CloudTrail、『IAM ユーザーガイド』の「IAM および AWS STS API AWS CloudTrail呼び出しのロギングウィング」を参照してください。

以下は、sourceIdentity フィールドを表示するイベントのスニペットの例です。

requestParameters セクションの例

次のイベントスニペットの例では、 AWS STS AssumeRoleユーザーがリクエストを行い、ソース ID を設定します。この例ではで表されます。*source-identity-value-set*ユーザーは、ロール ARN arn:aws:iam::123456789012:role/Assumed_Role で表されるロールを引き受けます。sourceIdentity フィールドが requestParameters イベントのブロックです。

```
"eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AIDAJ45Q7YFFAREXAMPLE",
        "accountId": "123456789012"
    },
    "eventTime": "2020-04-02T18:20:53Z",
    "eventSource": "sts.amazonaws.com",
    "eventName": "AssumeRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.64",
    "userAgent": "aws-cli/1.16.96 Python/3.6.0 Windows/10 botocore/1.12.86",
    "requestParameters": {
        "roleArn": "arn:aws:iam::123456789012:role/Assumed_Role",
        "roleSessionName": "Test1",
        "sourceIdentity": "source-identity-value-set",
    },
```

responseElements セクションの例

次のイベントス二ペットの例では、 AWS STS AssumeRoleユーザーがという名前のロールを引き受けるようにリクエストしDeveloper_Role、ソース ID を設定します。Adminユーザーは、ロール ARN arn:aws:iam::111122223333:role/Developer_Role で表されるロールを引き受けます。sourceIdentity フィールドは、イベントの requestParameters および responseElements 両方のブロックで表示されます。ロールを引き受けるために使用される一時的な認証情報、セッショントークン文字列、引き受けるロール ID、セッション名、セッション ARN は、responseElements ブロックで、ソースアイデンティティとともに表示されます。

```
    "requestParameters": {
        "roleArn": "arn:aws:iam::111122223333:role/Developer_Role",
        "roleSessionName": "Session_Name",
        "sourceIdentity": "Admin"
    },
    "responseElements": {
        "credentials": {
            "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
            "expiration": "Jan 22, 2021 12:46:28 AM",
            "sessionToken": "XXYYaz...
                            EXAMPLE_SESSION_TOKEN
                            XXyYaZAz"
        },
        "assumedRoleUser": {
            "assumedRoleId": "AROACKCEVSQ6C2EXAMPLE:Session_Name",
            "arn": "arn:aws:sts::111122223333:assumed-role/Developer_Role/Session_Name"
        },
        "sourceIdentity": "Admin"
    }
...
```

sessionContext セクションの例

次のイベントス二ペットの例では、ユーザーがサービス API DevRole を呼び出すというロールを引き受けています。 AWS ユーザーは、ここではで表されるソース ID を設定します。*source-identity-value-set*sourceIdentity フィールドはイベントの userIdentity ブロック内では sessionContext ブロックにあります。

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

```
    "principalId": "AROAJ45Q7YFFAREXAMPLE: Dev1",
    "arn": "arn: aws: sts: : 123456789012: assumed-role/DevRole/Dev1",
    "accountId": "123456789012",
    "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAJ45Q7YFFAREXAMPLE",
        "arn": "arn: aws: iam: : 123456789012: role/DevRole",
        "accountId": "123456789012",
        "userName": "DevRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-02-21T23: 46: 28Z"
      },
      "sourceIdentity": "source-identity-value-set"
    }
  }
}
```

CloudTrail **insightDetails**インサイト要素

AWS CloudTrail Insights イベントレコードには、JSON CloudTrail 構造内の他のイベントとは異なるフィールド (ペイロードと呼ばれることもあります) が含まれます。 CloudTrail Insights イベントレコードには、イベントソース、ユーザー ID、ユーザーエージェント、過去の平均またはベースライン、統計、API 名、イベントが Insights イベントの開始か終了かなど、Insights `insightDetails` イベントの基礎となるトリガーに関する情報を含むブロックが含まれます。`insightDetails` ブロックには、以下の情報が含まれています。

- **`state`** - Insights イベントが開始または終了の Insights イベントであるかどうか。ここには、`Start` または `End` が表示されます。

  使用可能: 1.07 以降

  オプション: False
- **`eventSource`**- AWS 異常なアクティビティの原因となったサービスエンドポイント (など)。`ec2.amazonaws.com`

  使用可能: 1.07 以降

オプション: False

- **eventName** - Insights イベントの名前。通常、異常なアクティビティのソースであった API の名前。

  使用可能: 1.07 以降

  オプション: False

- **insightType** - Insights イベントのタイプ。この値は `ApiCallRateInsight` または `ApiErrorRateInsight` となります。

  使用可能: 1.07 以降

  オプション: False

- **insightContext** -

  Insights AWS CloudTrail イベントを生成するために分析されたイベントに関連するツール (ユーザーエージェントと呼ばれる)、IAM ユーザーとロール (ユーザー ID と呼ばれる)、エラーコードに関する情報。また、この要素には、Insights イベントの異常なアクティビティがベースラインまたは通常のアクティビティとどのように比較されるかを示す統計も含まれます。

  使用可能: 1.07 以降

  オプション: False

  - **statistics** - ベースラインに関するデータ、ベースライン期間中に測定されたアカウントによるサブジェクト API への呼び出しまたはエラーの一般的な平均率、Insights イベントの最初の 1 分間に Insights イベントをトリガーしたコールまたはエラーの平均率、および Insights イベントの継続時間 (分)、およびベースラインの継続時間 (分) 測定期間が含まれます。

    使用可能: 1.07 以降

    オプション: False

    - **baseline** - Insights イベントの開始前の 7 日間に計算された、アカウントの Insights イベントのサブジェクト API のベースライン期間中の 1 分あたりの API コールまたはエラーの平均数。

      使用可能: 1.07 以降

      オプション: False

- **`insight`** -

  Insights イベントの開始の場合、この値は、異常なアクティビティの開始時の 1 分あたりの API コールまたはエラーの平均数です。終了 Insights イベントの場合、この値は、異常なアクティビティの期間中の 1 分あたりの API コールまたはエラーの平均数です。

  使用可能: 1.07 以降

  オプション: False

- **`insightDuration`** - Insights イベントの期間 (分) (サブジェクト API における異常なアクティビティの開始から終了までの期間) です。`insightDuration` は、開始および終了 Insights イベントの両方で発生します。

  使用可能: 1.07 以降

  オプション: False

- **`baselineDuration`** - ベースライン期間 (分) (サブジェクト API で通常のアクティビティが測定される期間) です。`baselineDuration` は、最低でも Insights イベントの 7 日間 (10080 分) 前である必要があります。このフィールドは、Insights イベントの開始と終了の両方で発生します。`baselineDuration` 測定の終了時刻に、必ず Insights イベントが開始します。

  使用可能: 1.07 以降

  オプション: False

- **`attributions`** - このブロックには、異常なアクティビティやベースラインアクティビティに関連するユーザーアイデンティティ、ユーザーエージェント、エラーコードに関する情報を表示します。最大 5 つのユーザーアイデンティティ、5 つのユーザーエージェント、5 つのエラーコードが、アクティビティ数の平均でソートされ、高いものから低いものへの降順で Insights イベント `attributions` ブロックでキャプチャされます。

  使用可能: 1.07 以降

  オプション: True

  - **`attribute`** - 属性タイプが含まれます。値は `userIdentityArn`、`userAgent`、または `errorCode` になります。
    - **`userIdentityArn`**-異常なアクティビティやベースライン期間中に API AWS 呼び出しやエラーの原因となったユーザーまたは IAM ロールの上位 5 件まで表示するブロック。CloudTrail レコードの内容 の `userIdentity` も参照してください。

使用可能: 1.07 以降

オプション: False

- **insight** - 異常なアクティビティ期間中に行われた API コールに貢献したユーザーアイデンティティ ARN の上位 5 つまでを、API コールAPI コールの最大数から最小数までの降順で表示するブロック。また、異常なアクティビティ期間中にユーザーアイデンティティによって行われた API コールの平均数も表示されます。

  使用可能: 1.07 以降

  オプション: False

  - **value** - 異常なアクティビティ期間中に行われた API コールに貢献したユーザーアイデンティティの上位 5 つの内の 1 つのARN。

    使用可能: 1.07 以降

    オプション: False

  - **average** - value フィールドのユーザーアイデンティティの異常なアクティビティ期間中の 1 分あたりの API コールまたはエラーの数。

    使用可能: 1.07 以降

    オプション: False

- **baseline** - 通常のアクティビティ期間中に行われた API コールまたはエラーに最も貢献したユーザーアイデンティティ ARN の上位 5 つまでを表示するブロック。また、通常のアクティビティ期間中にユーザーアイデンティティによって行われた API コールまたはエラーの平均数も表示されます。

  使用可能: 1.07 以降

  オプション: False

  - **value** - 通常のアクティビティ期間中に行われた API コールまたはエラーに貢献したユーザーアイデンティティの上位 5 つの内の 1 つのARN。

    使用可能: 1.07 以降

    オプション: False

- **average** - value フィールドのユーザーアイデンティティの Insights アクティビティ開始時間前の 7 日間の、1 分あたりの API コールまたはエラーの履歴平均。

  使用可能: 1.07 以降

  オプション: False

- **userAgent**-異常なアクティビティとベースライン期間中に、ユーザー ID が API AWS 呼び出しの原因となったツールの上位 5 つまで表示するブロック。これらのツールには AWS Management Console、 AWS CLI、または SDK が含まれます。 AWS CloudTrail レコードの内容 の userAgent も参照してください。

  使用可能: 1.07 以降

  オプション: False

  - **insight** - 異常なアクティビティ期間中に行われた API コールに貢献したユーザーエージェント ARN の上位 5 つまでを、API コールAPI コールの最大数から最小数までの降順で表示するブロック。また、異常なアクティビティ期間中にユーザーエージェントがログ記録された API コールまたはエラーの平均数も表示されます。

    使用可能: 1.07 以降

    オプション: False

    - **value** - 異常なアクティビティ期間中に行われた API コールに貢献したユーザーエージェントの上位 5 つの内の 1 つ。

      使用可能: 1.07 以降

      オプション: False

    - **average** - value フィールドのユーザーエージェントの異常なアクティビティ期間中の 1 分あたりにログ記録された API コールまたはエラーの数。

      使用可能: 1.07 以降

      オプション: False

  - **baseline** - 通常のアクティビティ期間中に行われた API コールに最も貢献したユーザーエージェント の上位 5 つまでを表示するブロック。また、通常のアクティビティ期間中にユーザーエージェントによってログ記録された API コールまたはエラーの平均数も表示されます。

使用可能: 1.07 以降

オプション: False

- **value** - 通常のアクティビティ期間中にログ記録された API コールまたはエラーに貢献したユーザーエージェントの上位 5 つの内の 1 つ。

  使用可能: 1.07 以降

  オプション: False

- **average** - value フィールドのユーザーエージェントの Insights アクティビティ開始時間前の 7 日間の、1 分あたりの API コールまたはエラーの履歴平均。

  使用可能: 1.07 以降

  オプション: False

- **errorCode** - 異常なアクティビティおよびベースライン期間中に API コールで発生したエラーコードの上位 5 つまでを、API コールの最大数から最小数の降順に表示するブロック。CloudTrail レコードの内容 の errorCode も参照してください。

  使用可能: 1.07 以降

  オプション: False

- **insight** - 異常なアクティビティ期間中に行われた API コールで発生したエラーコードの上位 5 つまでを、関連づけられた API コールの最大数から最小数の降順に表示するブロック。また、異常なアクティビティ期間中に発生したエラーに対して行われた API コールの平均数も表示されます。

  使用可能: 1.07 以降

  オプション: False

- **value** - AccessDeniedException など、異常なアクティビティ期間中に行われた API コールで発生した、上位 5 つのエラーコードのうちの 1 つ。

  Insights イベントをトリガーしたコールでエラーが発生しなかった場合、この値は null です。

  使用可能: 1.07 以降

  オプション: False

- **average** - value フィールドのエラーコードの異常なアクティビティ期間中の 1 分あたりの API コールの数。

  エラーコードの値が null の場合、insightブロックに他のエラーコードはなく、average 値はstatistics ブロックを Insights イベント全体のものと同じです。

  使用可能: 1.07 以降

  オプション: False

- **baseline** - 通常のアクティビティ期間中に行われた API コールで発生したエラーコードの上位 5 つまでを表示するブロック。また、通常のアクティビティ期間中にユーザーエージェントによって行われた API コールの平均数も表示されます。

  使用可能: 1.07 以降

  オプション: False

  - **value** - AccessDeniedException など、通常のアクティビティ期間中に行われた API コールで発生した、上位 5 つのエラーコードのうちの 1 つ。

    使用可能: 1.07 以降

    オプション: False

  - **average** - value フィールドのエラーコードの Insights アクティビティ開始時間前の 7 日間の、1 分あたりの API コールまたはエラーの履歴平均。

    使用可能: 1.07 以降

    オプション: False

insightDetails ブロックの例

次は、アプリケーション Auto Scaling API CompleteLifecycleAction が異常な回数呼び出されたときに発生した Insights イベントの insightDetails ブロックの Insights イベントの例です。完全な Insights イベントの例については、「Insights イベント」を参照してください。

この例は、"state": "Start" により示される、開始 Insights イベントからのものです。Insights イベントに関連付けられた API を呼び出した上位ユーザーアイデンティティ、CodeDeployRole1、CodeDeployRole2、および CodeDeployRole3 がこの Insights イベントの平均 API コールレート、CodeDeployRole1ロールのベースラインとともに

attributions ブロックに表示されます。attributionsこのブロックには、ユーザーエージェントcodedeploy.amazonaws.com、つまり上位のユーザー ID AWS CodeDeploy がコンソールを使用して API 呼び出しを実行したことも示されています。

Insights イベントを生成するために分析されたイベントに関連付けられたエラーコードがないため (値は null)、エラーコードの insight 平均は、statistics ブロックに表示された、全体の Insights イベント全体の insight 平均と同じです。

```
          "insightDetails": {
            "state": "Start",
            "eventSource": "autoscaling.amazonaws.com",
            "eventName": "CompleteLifecycleAction",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
              "statistics": {
                "baseline": {
                  "average": 0.0000882145
                },
                "insight": {
                  "average": 0.6
                },
                "insightDuration": 5,
                "baselineDuration": 11336
              },
              "attributions": [
                {
                  "attribute": "userIdentityArn",
                  "insight": [
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole2",
                      "average": 0.2
                    },
                    {
                      "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole3",
                      "average": 0.2
                    }
```

```
                ],
                "baseline": [
                  {
                    "value": "arn:aws:sts::012345678901:assumed-role/
CodeDeployRole1",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "userAgent",
                "insight": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "codedeploy.amazonaws.com",
                    "average": 0.0000882145
                  }
                ]
              },
              {
                "attribute": "errorCode",
                "insight": [
                  {
                    "value": "null",
                    "average": 0.6
                  }
                ],
                "baseline": [
                  {
                    "value": "null",
                    "average": 0.0000882145
                  }
                ]
              }
            ]
          }
        }
```

によってキャプチャされた非APIイベント CloudTrail

AWS API 呼び出しを記録するだけでなく、 AWS アカウントにセキュリティやコンプライアンスに影響を与える可能性のある、 CloudTrail または運用上の問題のトラブルシューティングに役立つ可能性のあるその他の関連イベントをキャプチャします。

トピック

- AWS サービスイベント
- AWS Management Console サインインイベント

AWS サービスイベント

CloudTrail API 以外のサービスイベントのロギングをサポートします。 AWS これらのイベントはサービスによって作成されますが、パブリック AWS API へのリクエストによって直接トリガーされるわけではありません。これらのイベントの場合、eventType フィールドは AwsServiceEvent です。

以下は、 AWS カスタマー管理キーが自動的にローテーションされるサービスイベントのシナリオの例です AWS Key Management Service (AWS KMS)。KMS キーのローテーションの詳細については、「KMS キーのローテーション」を参照してください。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2019-06-02T00:06:08Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "234f004b-EXAMPLE",
    "readOnly": false,
    "resources": [
        {
```

```
            "ARN": "arn:aws:kms:us-east-2:123456789012:key/7944f0ec-EXAMPLE",
            "accountId": "123456789012",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "keyId": "7944f0ec-EXAMPLE"
    }
}
```

AWS Management Console サインインイベント

CloudTrail 、 AWS ディスカッションフォーラム AWS Management Console、 AWS およびSupport センターへのサインイン試行を記録します。すべての IAM ユーザーと root ユーザーのサインインイベント、およびフェデレーティッドユーザーのすべてのサインインイベントは、ログファイルに記録を生成します。 CloudTrail ログの検索と表示の詳細については、「ログファイルを検索する CloudTrail 」および「 CloudTrail ログファイルのダウンロード」を参照してください。

> **Note**
>
> `ConsoleLogin`イベントに記録されるリージョンは、ユーザータイプや、サインインにグローバルエンドポイントとリージョナルエンドポイントのどちらを使用するかによって異なります。
>
> - root ユーザーとしてサインインすると、 CloudTrail us-east-1 にイベントを記録します。
> - IAM ユーザーでサインインしてグローバルエンドポイントを使用する場合、 CloudTrail イベントのリージョンを次のように記録します`ConsoleLogin`。
>   - アカウントエイリアスクッキーがブラウザに存在する場合、us-east-2、eu-north-1、または ap-southeast-2 CloudTrail `ConsoleLogin` のいずれかのリージョンでイベントを記録します。これは、コンソールプロキシがユーザーのサインイン場所からの待ち時間に基づいてユーザーをリダイレクトするためです。
>   - アカウントエイリアスクッキーがブラウザに存在しない場合は、 CloudTrail us-east-1 `ConsoleLogin` にイベントを記録します。これは、コンソールプロキシがグローバルサインインにリダイレクトするためです。
> - IAM ユーザーでサインインし、リージョナルエンドポイントを使用する場合、 CloudTrail `ConsoleLogin`エンドポイントの適切なリージョンにイベントを記録します。 AWS サイ

ンイン エンドポイントの詳細については、「AWS サインイン エンドポイントとクォータ」を参照してください。

トピック

- IAM ユーザーのイベントレコードの例
- root ユーザーのイベントレコードの例
- フェデレーションユーザーのイベントレコードの例

IAM ユーザーのイベントレコードの例

以下の例は、いくつかの IAM ユーザーサインインシナリオのイベントレコードを示しています。

トピック

- IAM ユーザー、MFA なしでサインインに成功
- IAM ユーザー、MFA を使用したサインインに成功
- IAM ユーザー、失敗したサインイン
- IAM ユーザー、MFA のサインインプロセスのチェック (単一の MFA デバイスタイプ)
- IAM ユーザー、MFA のサインインプロセスのチェック (複数の MFA デバイスタイプ)

IAM ユーザー、MFA なしでサインインに成功

次のレコードは、という名前のユーザが多要素認証 (MFA) Anaya AWS Management Console を使用せずにに正常にサインインしたことを示しています。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T21:44:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplee9aba7f8",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "e1bf1000-86a4-4a78-81d7-EXAMPLE83102",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


IAM ユーザー、MFA を使用したサインインに成功

次のレコードは、という名前の IAM ユーザーが多要素認証 (MFA) Anaya AWS Management Console を使用してに正常にサインインしたことを示しています。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::999999999999:user/Anaya",
        "accountId": "999999999999",
        "userName": "Anaya"
    },
    "eventTime": "2023-07-19T22:01:30Z",
    "eventSource": "signin.amazonaws.com",
```

```
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::999999999999:mfa/mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e1f76697-5beb-46e8-9cfc-EXAMPLEbde31",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "999999999999",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

IAM ユーザー、失敗したサインイン

次のレコードは Paulo という名前の IAM ユーザーからのサインインの試行が失敗したことを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Paulo"
    },
```

```
    "eventTime": "2023-07-19T22:01:20Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&state=hashArgsFromTB_us-east-1_examplebde32f3c9",
        "MobileVersion": "No",
        "MFAUsed": "Yes"
    },
    "eventID": "66c97220-2b7d-43b6-a7a0-EXAMPLEbae9c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


IAM ユーザー、MFA のサインインプロセスのチェック (単一の MFA デバイスタイプ)

サインイン時に IAM ユーザーに 多要素認証 (MFA) が必要かどうかを確認するサインプロセスを以下に示します。この例では、mfaType 値は U2F MFA です。これは、IAM ユーザーが単一の MFA デバイスまたは同じタイプ (U2F MFA) の複数の MFA デバイスのいずれかを有効にしたことを示します。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
```

```
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "Alice"
    },
    "eventTime": "2023-07-19T22:01:26Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Virtual MFA"
    },
    "eventID": "7d8a0746-b2e7-44f5-9917-EXAMPLEfb77c",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```


IAM ユーザー、MFA のサインインプロセスのチェック (複数の MFA デバイスタイプ)

サインイン時に IAM ユーザーに 多要素認証 (MFA) が必要かどうかを確認するサインプロセスを以下に示します。この例では、mfaType 値は Multiple MFA Devices です。これは、IAM ユーザーが複数の MFA デバイスタイプを有効にしたことを示します。


```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "accountId": "123456789012",
```

```
        "accessKeyId": "",
        "userName": "Mary"
    },
    "eventTime": "2023-07-19T23:10:09Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CheckMfa",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
 Firefox/102.0",
    "requestParameters": null,
    "responseElements": {
        "CheckMfa": "Success"
    },
    "additionalEventData": {
        "MfaType": "Multiple MFA Devices"
    },
    "eventID": "19bd1a1c-76b1-4806-9d8f-EXAMPLE02a96",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```


root ユーザーのイベントレコードの例

次の例は、複数の root ユーザーサインインシナリオのイベントレコードを示しています。root ユーザーを使用してサインインすると、us-east-1 CloudTrail ConsoleLogin にイベントが記録されます。

トピック

- ルートユーザー、MFA なしでサインインに成功
- ルートユーザー、MFA を使用したサインインに成功
- Root ユーザー、失敗したサインイン
- Root ユーザー、MFA が変更されました

- root ユーザー、パスワードが変更されました

ルートユーザー、MFA なしでサインインに成功

多要素認証 (MFA) を使用していないルートユーザーのサインインイベントの成功を次に示します。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-12T13:35:31Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://console.aws.amazon.com/console/home?hashArgs=
%23&isauthcode=true&nc2=h_ct&src=header-signin&state=hashArgsFromTB_ap-
southeast-2_example80afacd389",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "4217cc13-7328-4820-a90c-EXAMPLE8002e6",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "signin.aws.amazon.com"
```

```
    }
}
```

ルートユーザー、MFA を使用したサインインに成功

多要素認証 (MFA) を使用しているルートユーザーのサインインイベントの成功を次に示します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-13T03:04:43Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/114.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "LoginTo": "https://ap-southeast-1.console.aws.amazon.com/ec2/home?region=ap-
southeast-1&state=hashArgs%23Instances%3Av%3D3%3B%24case%3Dtags%3Atrue%255C%2Cclient
%3Afalse%3B%24regex%3Dtags%3Afalse%255C%2Cclient%3Afalse&isauthcode=true",
        "MobileVersion": "No",
        "MFAIdentifier": "arn:aws:iam::444455556666:mfa/root-account-mfa-device",
        "MFAUsed": "Yes"
    },
    "eventID": "e0176723-ea76-4275-83a3-EXAMPLEf03fb",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Root ユーザー、失敗したサインイン

以下に MFA を使用していない root ユーザーのサインインイベントが失敗したことを示します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": ""
    },
    "eventTime": "2023-07-16T04:33:40Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "errorMessage": "Failed authentication",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Failure"
    },
    "additionalEventData": {
        "LoginTo": "https://us-east-1.console.aws.amazon.com/billing/home?region=us-
east-1&state=hashArgs%23%2Faccount&isauthcode=true",
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "f28d4329-5050-480b-8de0-EXAMPLE07329",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
```

```
        "clientProvidedHostHeader": "signin.aws.amazon.com"
    }
}
```

Root ユーザー、MFA が変更されました

次の例は、root ユーザーが多要素認証 (MFA) 設定を変更したイベントを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE4XX3IEV4PFQTH",
        "userName": "AWS ROOT USER",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-15T03:51:12Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-15T04:37:08Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "EnableMFADevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": {
        "userName": "AWS ROOT USER",
        "serialNumber": "arn:aws:iam::111122223333:mfa/root-account-mfa-device"
    },
    "responseElements": null,
    "requestID": "9b45cd4c-a598-41e7-9170-EXAMPLE535f0",
    "eventID": "b4f18d55-d36f-49a0-afcb-EXAMPLEc026b",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

root ユーザー、パスワードが変更されました

次に、root ユーザーがパスワードを変更するイベントの例を示します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Root",
        "principalId": "444455556666",
        "arn": "arn:aws:iam::444455556666:root",
        "accountId": "444455556666",
        "accessKeyId": "EXAMPLEAOTKEG44KPW5P",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-11-25T13:01:14Z",
                "mfaAuthenticated": "false"
             }
        }
    },
    "eventTime": "2022-11-25T13:01:14Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "ChangePassword",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/111.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "c64254c2-e4ff-49c0-900e-EXAMPLE9e6d2",
    "eventID": "d059176c-4f4d-4a9e-b8d7-EXAMPLE2b7b3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management"
}
```

フェデレーションユーザーのイベントレコードの例

次に、フェデレーションユーザーのイベントレコードの例を示します。フェデレーティッドユーザーには、 AWS リクエストを通じてリソースにアクセスするための一時的なセキュリティ認証情報が与えられます。AssumeRole

次に、フェデレーション暗号化リクエストのイベントの例を示します。元のアクセスキー ID は userIdentity エレメントの accessKeyId フィールドに入力されます。responseElements の accessKeyId フィールドには、リクエストされる sessionDuration が暗号化リクエストで渡された場合は新しいアクセスキー ID が含まれ、それ以外の場合は元のアクセスキー ID の値が含まれます。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEUU4MH7OYK5ZCOA:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/roleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "originalAccessKeyID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEUU4MH7OYK5ZCOA",
                "arn": "arn:aws:iam::123456789012:role/roleName",
                "accountId": "123456789012",
                "userName": "roleName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-09-25T21:30:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-25T21:30:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "GetSigninToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Java/1.8.0_382",
    "requestParameters": null,
```

```
    "responseElements": {
        "credentials": {
            "accessKeyId": "accessKeyID"
        },
        "GetSigninToken": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "1d66615b-a417-40da-a38e-EXAMPLE8c89b",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

多要素認証 (MFA) を使用していないフェデレーションユーザーのサインインイベントの成功を次に示します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLEPHCNW7ZCASLJOH:JohnDoe",
        "arn": "arn:aws:sts::123456789012:assumed-role/RoleName/JohnDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLEPHCNW7ZCASLJOH",
                "arn": "arn:aws:iam::123456789012:role/RoleName",
                "accountId": "123456789012",
                "userName": "RoleName"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2023-09-22T16:15:47Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-09-22T16:15:47Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "ConsoleLogin",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": {
        "ConsoleLogin": "Success"
    },
    "additionalEventData": {
        "MobileVersion": "No",
        "MFAUsed": "No"
    },
    "eventID": "b73f1ec6-c064-4cd3-ba83-EXAMPLE441d7",
    "readOnly": false,
    "eventType": "AwsConsoleSignIn",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.signin.aws.amazon.com"
    }
}
```

CloudTrail ログファイルの操作

CloudTrail ファイルを使用してより高度なタスクを実行できます。

- リージョンごとに複数の証跡を作成します。
- CloudTrail ログファイルを CloudWatch Logs に送信して監視します。
- アカウント間でログファイルを共有します。
- AWS CloudTrail 処理ライブラリを使用して Java でログ処理アプリケーションを作成します。
- ログファイルを検証して、配信後に変更されていないことを確認します CloudTrail。

アカウントにイベントが発生すると、 CloudTrail そのイベントがトレイルの設定と一致するかどうかが評価されます。トレイル設定に一致するイベントのみが Amazon S3 バケットと Amazon CloudWatch Logs ロググループに配信されます。

証跡が指定したイベントのみを処理してログに記録するように、複数の証跡を異なる方法で設定することができます。たとえば、ある証跡は読み取り専用データと管理イベントをログに記録してすべての読み取り専用イベントを 1 つの S3 バケットに配信するように設定し、別の証跡は書き込み専用データと管理イベントをログに記録してすべての書き込み専用イベントを別の S3 バケットに配信するように設定できます。

また、ある証跡は 1 つの証跡ログを使用してすべての管理イベントを 1 つの S3 バケットに配信し、別の証跡はすべてのデータイベントをログに記録して別の S3 バケットに配信するように、設定することもできます。

次の情報をログ記録するように証跡を設定できます。

- データイベント: これらのイベントでは、リソース上またはリソース内で実行されたリソースオペレーションについての洞察が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。
- 管理イベント:管理イベントでは、 AWS アカウント内のリソースに対して実行される管理操作を可視化できます。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。管理イベントは、アカウントで発生する非 API イベントを含む場合もあります。たとえば、ユーザーがアカウントにログインすると、 CloudTrail `ConsoleLogin`イベントが記録されます。詳細については、「によってキャプチャされた非APIイベント CloudTrail」を参照してください。
- インサイトイベント: アカウントで検出された異常なアクティビティをインサイトイベントがキャプチャします。Insights イベントを有効にしていて、 CloudTrail 異常なアクティビティを検出

すると、Insights イベントはトレイルの送信先 S3 バケットに別のフォルダーに記録されます。CloudTrail コンソールで Insights イベントを表示すると、Insights イベントのタイプとインシデント期間を確認することもできます。 CloudTrail トレイルに記録される他の種類のイベントとは異なり、Insights イベントは、アカウントの API 使用量に、 CloudTrail アカウントの一般的な使用パターンと大きく異なる変化が検出された場合にのみ記録されます。

Insights イベントは、管理 API に対してのみ生成されます。詳細については、「Insights イベントのログ記録」を参照してください。

> **Note**
>
> CloudTrail 通常、API 呼び出しから平均約 5 分以内にログが配信されます。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。
> 証跡の設定を誤ると (S3 バケットにアクセスできないなど)、ログファイルを S3 バケットに 30 日間再配信しようとしますが、 CloudTrail attempted-to-deliver これらのイベントには標準料金が適用されます。 CloudTrail 証跡の不適切な設定による課金を避けるには、その証跡を削除する必要があります。

トピック

CloudTrail 複数の地域からのログファイルの受信

複数のリージョンのログファイルを 1 つのアカウントの 1 つの S3 バケットに配信するように設定できます CloudTrail 。たとえば、米国西部 (オレゴン) リージョンに S3 CloudWatch バケットにログファイルを配信するように設定されたトレイルとログロググループがあるとします。既存の単一

リージョントレイルをすべてのリージョンを記録するように変更すると、アカウントの 1 CloudTrail AWS つのパーティションにあるすべてのリージョンのイベントがログに記録されます。 CloudTrail ログファイルを同じ S3 CloudWatch バケットとロググループに配信します。S3 CloudTrail バケットに書き込む権限がある限り、マルチリージョントレイルのバケットはトレイルのホームリージョンにある必要はありません。

アカウントのすべてのパーティションのすべてのリージョンのイベントを記録するには、 AWS 各パーティションにマルチリージョントレイルを作成します。

コンソールでは、デフォルトで、作業している AWS パーティションのすべての AWS リージョン のイベントを口グ記録する証跡を作成します。これは推奨されるベストプラクティスです。単一リージョンでイベントの口グ記録を行うには (非推奨)、AWS CLIを使用します。すべてのリージョンにログインするように既存の単一リージョンの証跡を設定するには、 AWS CLIを使用する必要があります。

既存の証跡を変更し、すべてのリージョンに適用されるようにするには、`--is-multi-region-trail` オプションを update-trail コマンドに追加します。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

証跡がすべてのリージョンに適用されるようになったことを確認するために、出力の `IsMultiRegionTrail` 要素に `true` と表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "my-bucket"
}
```

> **Note**
>
> awsパーティション内で新しいリージョンが起動すると、 CloudTrail 元のトレイルと同じ設定で新しいリージョンに自動的にトレイルが作成されます。

詳細については、以下のリソースを参照してください。

- CloudTrail トレイルでの作業
- CloudTrail よくある質問

でのデータの一貫性の管理 CloudTrail

CloudTrail 結果整合性と呼ばれる分散コンピューティングモデルを使用しています。属性ベースのアクセス制御 (ABAC) で使用されるタグを含め、 CloudTrail 設定 (AWS または他のサービス) に加えた変更は、考えられるすべてのエンドポイントから認識されるまでに時間がかかります。遅延の原因の一部は、データをサーバーからサーバーへ、レプリケーションゾーンからレプリケーションゾーンへ、そして世界中のリージョンからリージョンへと送信するのにかかる時間です。 CloudTrail また、キャッシュを使用してパフォーマンスを向上させますが、場合によっては時間がかかることもあります。変更は、以前にキャッシュされたデータがタイムアウトになるまで反映されない場合があります。

発生する可能性のあるこれらの遅延を考慮して、アプリケーションを設計する必要があります。ある場所で行われた変更が他の場所で直ちに表示されない場合でも、正常に動作することを確認します。このような変更には、証跡やイベントデータストアの作成や更新、イベントセレクタの更新、ログ記録の開始や停止が含まれます。トレイルまたはイベントデータストアを作成または更新すると、変更がすべての場所に反映されるまで、最後に確認された設定に基づいて S3 CloudTrail バケットまたはイベントデータストアにログが配信されます。

これが他のユーザーに与える影響について詳しくは AWS のサービス、以下のリソースを参照してください。

- Amazon DynamoDB: 「Amazon DynamoDB よくある質問」の「DynamoDB の整合性モデルとは何ですか?」および「Amazon DynamoDB デベロッパーガイド」の「読み込み整合性」。
- Amazon EC2: 「Amazon Elastic Compute Cloud API リファレンス」の「Eventual consistency」(結果整合性)。
- Amazon EMR: AWS ビッグデータブログの ETL ワークフローに Amazon S3 と Amazon Elastic MapReduce を使用する際の一貫性の確保。
- AWS Identity and Access Management (IAM): 行った変更が IAM ユーザーガイドにすぐに反映されるとは限りません。
- Amazon Redshift: 「Amazon Redshift Database デベロッパーガイド」の「データの整合性の管理」。
- Amazon S3: 「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 のデータ整合性モデル」。

Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング

CloudTrail CloudWatch ログを使用してトレイルログを監視し、特定のアクティビティが発生したときに通知を受けるように設定できます。

1. ログイベントを CloudWatch Logs に送信するようにトレイルを設定します。
2. CloudWatch ログのメトリクスフィルターを定義して、用語、フレーズ、値に一致するログイベントがないかを評価します。例えば、`ConsoleLogin` イベントをモニタリングすることもできます。
3. CloudWatch メトリックスフィルターにメトリクスを割り当てます。
4. CloudWatch 指定したしきい値と期間に従ってトリガーされるアラームを作成します。アラームがトリガーされた際に通知が送信されるように設定することで、必要な対応がとれるようになります。
5. また、 CloudWatch アラームに応じて自動的にアクションを実行するように設定することもできます。

CloudWatch アマゾンとAmazon CloudWatch ログの標準価格が適用されます。詳細については、「Amazon CloudWatch 料金表」を参照してください。

ログをログに送信するようにトレイルを設定できるリージョンの詳細については、『ジェネラルリファレンス』の「Amazon CloudWatch CloudWatch Logs のリージョンとクォータ」を参照してください。AWS

トピック

- CloudWatch ログへのイベントの送信
- CloudWatch CloudTrail イベントのアラームの作成:例
- CloudTrail CloudWatch ログへのイベントの送信を停止する
- CloudWatch のロググループとログストリームの命名 CloudTrail
- CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント

CloudWatch ログへのイベントの送信

CloudWatch ログにイベントを送信するようにトレイルを設定すると、 CloudTrail トレイル設定に一致するイベントのみが送信されます。たとえば、データイベントのみを記録するようにトレイル

を設定した場合、トレイルはデータイベントを CloudWatch Logs ロググループにのみ送信します。CloudTrail データ、Insights、 CloudWatch 管理イベントのログへの送信をサポートします。詳細については、「 CloudTrail ログファイルの操作」を参照してください。

> **Note**
>
> CloudWatch コンソールを使用して組織トレイルのログロググループを設定できるのは管理アカウントだけです。委任管理者は、 AWS CLI CloudTrail `CreateTrail`または `UpdateTrail` API CloudWatch オペレーションを使用してログロググループを設定できます。

CloudWatch Logs ロググループにイベントを送信するには:

- IAM ロールを作成または指定するための十分なアクセス許可があることを確認してください。詳細については、「コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与」を参照してください。
- CloudWatch を使用してログロググループを設定する場合は AWS CLI、指定したロググループにログログストリームを作成し、 CloudWatch CloudTrail そのログストリームにイベントを配信するための十分な権限があることを確認してください。詳細については、「ポリシードキュメントを作成する」を参照してください。
- 新しい証跡を作成するか、既存の証跡を指定します。詳細については、「コンソールで証跡を作成および更新する」を参照してください。
- ロググループを作成するか、既存のロググループを指定します。
- IAM ロールを指定します。組織の証跡の既存の IAM ロールを変更する場合は、組織の証跡のログ記録を許可するように手動でポリシーを更新する必要があります。詳細については、このポリシー例と「組織の証跡の作成」を参照してください。
- ロールポリシーをアタッチするか、デフォルトを使用します。

目次

- ロググループを作成する
- ロールの作成
- ポリシードキュメントを作成する
- 証跡を更新する
- 制限

CloudWatch コンソールによるログ監視の設定

を使用して、 AWS Management Console CloudWatch イベントをログに送信してモニタリングするようにトレイルを設定できます。

ロググループを作成するか、既存のロググループを指定する

CloudTrail CloudWatch Logs ロググループをログイベントの配信エンドポイントとして使用します。ユーザーは、ロググループを作成するか、既存のロググループを指定することができます。

ロググループを作成または既存のロググループを指定するには

1. CloudWatch Logs 統合を設定するのに十分な権限を持つ管理ユーザーまたはロールでログインしてください。詳細については、「コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与」を参照してください。

   > **Note**
   >
   > CloudWatch コンソールを使用して組織トレイルのログロググループを設定できるのは管理アカウントだけです。委任管理者は、 AWS CLI CloudTrail `CreateTrail`または `UpdateTrail` API CloudWatch オペレーションを使用してログロググループを設定できます。

2. https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
3. 証跡名を選択します。すべてのリージョンに適用される証跡を選択した場合は、その証跡の作成元のリージョンにリダイレクトされます。ロググループを作成することもできますし、証跡と同じリージョン内の既存のロググループを選択することもできます。

> **Note**
>
> すべてのリージョンに適用されるトレイルは、 CloudWatch すべてのリージョンのログファイルを指定したロググループに送信します。

4. 「CloudWatch ログ」で「編集」を選択します。
5. [CloudWatch ログ] には [有効] を選択します。
6. [ロググループ名] で、[新規] を選択して新しいロググループを作成するか、[既存] を選択して既存のロググループを使用します。[New] を選択すると、 CloudTrail 新しいロググループの名前が自動的に指定されるか、名前を入力できます。命名の詳細については、「CloudWatch のロググループとログストリームの命名 CloudTrail」を参照してください。
7. [Existing] を選択した場合、ドロップダウンリストからロググループを選択します。
8. [Role name] で [New] を選択し、Logs にログを送信する権限を持つ新しい IAM ロールを作成します。 CloudWatch [Existing] を選択して、ドロップダウンリストから既存の IAM ロールを選択します。新しいロールまたは既存のロールのポリシーステートメントは、[ポリシードキュメント] を展開すると表示されます。このロールの詳細については、「 CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント」を参照してください。

> **Note**
>
> 証跡を設定する際には、別のアカウントに属している S3 バケットや SNS トピックを選択することもできます。ただし、 CloudWatch ログロググループにイベントを配信する場合は、現在のアカウントに存在するロググループを選択する必要があります。 CloudTrail

9. [変更を保存] を選択します。

IAM ロールを指定する

CloudTrail ログストリームにイベントを配信するために引き受ける役割を指定できます。

ロールを指定するには

1. デフォルトでは、`CloudTrail_CloudWatchLogs_Role` が指定されます。デフォルトのロールポリシーには、 CloudWatch 指定したロググループにログログストリームを作成し、 CloudTrail そのログストリームにイベントを配信するために必要な権限があります。

> **Note**
>
> 組織の証跡のロググループにこのロールを使用する場合は、ロールを作成した後に手動でポリシーを変更する必要があります。詳細については、このポリシー例と「組織の証跡の作成」を参照してください。

a. ロールを確認するには、https://console.aws.amazon.com/iam/ AWS Identity and Access Management のコンソールにアクセスしてください。

b. [ロール] を選択し、次に CloudTrail_ CloudWatchLogs _Role を選択します。

c. [アクセス許可] タブからポリシーを展開して、その内容が表示されます。

2. 別のロールを指定することもできますが、 CloudWatch そのロールを使用してイベントをログに送信する場合は、必要なロールポリシーを既存のロールにアタッチする必要があります。詳細については、「 CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント」を参照してください。

CloudWatch コンソールでのイベントの表示

CloudWatch Logs ロググループにイベントを送信するようにトレイルを設定すると、 CloudWatch コンソールにイベントを表示できます。 CloudTrail 通常、API 呼び出しから平均約 5 分以内にロググループにイベントを配信します。この時間は保証されません。詳細については、「AWS CloudTrail サービスレベルアグリーメント」をご覧ください。

CloudWatch コンソールにイベントを表示するには

1. https://console.aws.amazon.com/cloudwatch/ CloudWatch でコンソールを開きます。
2. ナビゲーションペインで、[ログ]、[ロググループ] の順に選択します。
3. 証跡用に指定したロググループを選択します。
4. 表示するログストリームを選択します。
5. 証跡によって記録されたイベントの詳細を表示するには、イベントを選択します。

> **Note**
>
> CloudWatch コンソールの Time (UTC) 列には、イベントがロググループに配信された日時が表示されます。イベントが記録された実際の時間を確認するには CloudTrail、`eventTime`フィールドを参照してください。

CloudWatch を使用してログモニタリングを設定します。 AWS CLI

を使用して、 AWS CLI CloudTrail CloudWatch 監視対象のイベントをログに送信するように設定できます。

ロググループを作成する

1. 既存のロググループがない場合は、Logs CloudWatch CloudWatch `create-log-group` コマンドを使用してログイベントの配信エンドポイントとしてログロググループを作成します。

   ```
   aws logs create-log-group --log-group-name name
   ```

   次の例では、`CloudTrail/logs` という名前のロググループが作成されます。

   ```
   aws logs create-log-group --log-group-name CloudTrail/logs
   ```

2. ロググループの Amazon リソースネーム (ARN) を取得します。

   ```
   aws logs describe-log-groups
   ```

ロールの作成

CloudWatch Logs CloudTrail ロググループにイベントを送信できるようにするロールを作成します。IAM の `create-role` コマンドには、2 つのパラメータがあります。1 つはロール名で、もう 1 つは、JSON 形式のロールポリシー割り当てドキュメントへのファイルパスです。使用するポリシードキュメントは、`AssumeRole` CloudTrailにアクセス権限を付与します。`create-role` コマンドを実行すると、必要なアクセス許可を持ったロールが作成されます。

ポリシードキュメントを含んだ JSON ファイルを作成するには、テキストエディタを開き、`assume_role_policy_document.json` という名前のファイルに次のポリシーコンテンツを保存します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

以下のコマンドを実行して、AssumeRoleの権限を持つロールを作成します CloudTrail。

```
aws iam create-role --role-name role_name --assume-role-policy-document file://<path to
 assume_role_policy_document>.json
```

コマンドが完了したら、出力内のロール ARN を書き留めておきます。

ポリシードキュメントを作成する

の次のロールポリシードキュメントを作成します CloudTrail。 CloudTrail このドキュメントは、CloudWatch 指定したロググループにログログストリームを作成し、 CloudTrail そのログストリームにイベントを配信するのに必要な権限を付与します。

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

      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
```

```
    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:accountID:log-group:log_group_name:log-
stream:accountID_CloudTrail_region*"
      ]
    }
  ]
}
```

role-policy-document.json という名前のファイルにポリシードキュメントを保存します。

組織の証跡にも使用される可能性があるポリシーを作成している場合は、少し異なる方法で構成する必要があります。たとえば、次のポリシーは、 CloudWatch 指定したロググループにログログストリームを作成し、 CloudTrail CloudTrail そのログストリームにイベントを配信するために必要な権限を付与します。この権限は、 AWS アカウント 111111111111 の証跡と、111111111111 アカウントで作成され、*o-exampleorgid* の ID AWS Organizations を持つ組織に適用された組織証跡の両方に対して行われます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
```

```
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:CloudTrail/
DefaultLogGroupTest:log-stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

組織の証跡の詳細については、「組織の証跡の作成」を参照してください。

次のマンドを実行して、ロールにポリシーを適用します。

```
aws iam put-role-policy --role-name role_name --policy-name cloudtrail-policy --policy-
document file://<path to role-policy-document>.json
```

証跡を更新する

コマンドを使用して、ロググループとロール情報でトレイルを更新します。 CloudTrail update-trail

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

AWS CLI コマンドの詳細については、『AWS CloudTrail コマンドラインリファレンス』を参照してください。

制限

CloudWatch EventBridge ログとそれぞれの最大イベントサイズは 256 KB です。ほとんどのサービスイベントの最大サイズは 256 KB ですが、一部のサービスにはまだそれより大きいイベントがあります。 CloudTrail これらのイベントは CloudWatch Logs やには送信されません EventBridge。

CloudTrail イベントバージョン 1.05 以降、イベントの最大サイズは 256 KB です。これは、悪意のある攻撃者による悪用を防ぎ、 AWS CloudWatch イベントをログやなどの他のサービスで利用できるようにするためです。 EventBridge

CloudWatch CloudTrail イベントのアラームの作成:例

このトピックでは、 CloudTrail イベントのアラームを設定する方法と例を交えて説明します。

トピック

前提条件

このトピックの例を使用する前に、次のことを行う必要があります。

- コンソールまたは CLI を使用して証跡を作成します。
- ロググループを作成します。ロググループは、証跡の作成の一部として実行できます。証跡の作成方法の詳細については、「証跡の作成」を参照してください。
- 指定したロググループにログログストリームを作成し、 CloudTrail CloudWatch CloudTrail そのログストリームにイベントを配信する権限を付与する IAM ロールを指定または作成します。これは、デフォルト `CloudTrail_CloudWatchLogs_Role` によって行われます。

詳細については、「 CloudWatch ログへのイベントの送信」を参照してください。このセクションの例は Amazon CloudWatch Logs コンソールで実行されています。メトリックスフィルタとアラームを作成する方法の詳細については、Amazon CloudWatch User Guide の「フィルタを使用してログイベントからメトリックスを作成する」と「Amazon CloudWatch アラームを使用する」を参照してください。

メトリックスフィルタを作成し、アラームを作成する

アラームを作成するには、まずメトリックスフィルタを作成してから、そのフィルタに基づいてアラームを設定する必要があります。すべての例の手順が示されます。 CloudTrail メトリックスフィルタの構文とログイベントのパターンの詳細については、Amazon CloudWatch Logs ユーザーガイドの「フィルタとパターンの構文」の JSON 関連のセクションを参照してください。

例 : セキュリティグループの設定の変更

以下の手順に従って、セキュリティグループの設定が変更されたときにトリガーされる Amazon CloudWatch アラームを作成します。

メトリックフィルタを作成する

1. https://console.aws.amazon.com/cloudwatch/ CloudWatch でコンソールを開きます。
2. ナビゲーションペインで、[Logs] (ログ)、[Log groups] (ロググループ) の順に選択します。
3. ロググループのリストで、 証跡のために作成したロググループを選択します。
4. [メトリクスフィルター] または [アクション] メニューから [メトリクスフィルターの作成] を選択します。
5. [パターンを定義] ページの [フィルターパターンの作成] で、[フィルターパターン] に以下の値を入力します。

```
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName =
 AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) ||
 ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup)
 || ($.eventName = DeleteSecurityGroup) }
```

6. [テストパターン] のデフォルト値はそのままにしておきます。[次へ] をクリックします。
7. [メトリクスの割り当て] ページの [フィルター名]に「**SecurityGroupEvents**」と入力します。
8. [メトリクスの詳細] ページで、[新しく作成する] をオンにして [メトリクス名前空間] に「**CloudTrailMetrics**」と入手します。
9. [メトリクス名] に「**SecurityGroupEventCount**」と入力します。
10. [メトリクス値] に「**1**」と入力します。
11. [Default value] は空白のままにします。
12. [次へ] をクリックします。
13. [Review and create] ページで選択内容を確認します。[Create metric filter] を選択してフィルターを作成するか、[編集] を選択して戻って値を変更します。

アラームの作成

メトリックスフィルターを作成すると、 CloudWatch CloudTrail トレイルロググループの「ロログループ詳細」ページが開きます。アラームを作成するには、次の手順を実行します。

1. [メトリクスフィルター] タブで、the section called “メトリックフィルタを作成する” で作成したメトリクスフィルターを見つけます。メトリクスフィルターのチェックボックスをオンにします。[メトリクスフィルター] バーで、[アラームの作成] を選択します。
2. [メトリクスと条件の指定] で、以下を入力します。

   a. [グラフ] には、アラームを作成したときに設定した他の設定に基づいてラインが **1** で設定されています。

   b. [メトリクス名] は、現在のメトリクス名、**SecurityGroupEventCount** のままにしておきます。

   c. [Statistic] は、デフォルト値、**Sum** のままにしておきます。

   d. [Period] は、デフォルト値、**5 minutes** のままにしておきます。

   e. [条件] セクションの [しきい値のタイプ] で、[静的] を選択します。

   f. [Whenever ***metric_name*** is] は、[Greater/Equal] を選択します。

   g. しきい値に「**1**」と入力します。

   h. [Additional configuration] は、デフォルト値のままにしておきます。[次へ] をクリックします。
3. 「アクションの設定」ページで「通知」を選択し、「アラーム中」を選択します。これにより、5 分以内に 1 件の変更イベントというしきい値を超えたときにアクションが実行され、SecurityGroupEventCountアラーム状態になったことが示されます。

   a. [次の SNS トピックに通知を送信] で、[新しいトピックの作成] を選択します。

   b. 新しい Amazon SNS トピックの名前として「**SecurityGroupChanges_CloudWatch_Alarms_Topic**」と入力します。

   c. [通知を受け取る E メールエンドポイント] に、このアラームが発生した場合に通知を受信するユーザーの E メールアドレスを入力します。E メールアドレスはカンマで区切ります。

      それぞれの E メール受信者に Amazon SNS トピックのサブスクライブを確認する E メールが送信されます。

   d. [Create topic] (トピックの作成) を選択します。
4. この例では、他のアクションタイプはスキップします。[次へ] をクリックします。
5. [Add name and description] ページで、アラームのフレンドリ名と説明を入力します。この例では、名前には「**Security group configuration changes**」、説明には「**Raises alarms if security group configuration changes occur**」を入力します。[次へ] をクリックします。

6. [Review and create] ページで選択内容を確認します。[] で変更を加えることができます。または、[アラームの作成] を選択してアラームを作成します。

   アラームを作成すると、「アラーム CloudWatch 」ページが開きます。アラームの[アクション] 列に、 SNS トピックのすべての E メール受信者が SNS 通知のサブスクライブを希望していることを確認するまで、[Pending confirmation] が表示されます。

AWS Management Console ログイン失敗の例

5 分間に 3 AWS Management Console 回以上サインインに失敗したときにトリガーされる Amazon CloudWatch アラームを作成するには、次の手順に従います。

メトリックフィルタを作成する

1. https://console.aws.amazon.com/cloudwatch/ CloudWatch でコンソールを開きます。
2. ナビゲーションペインで、[Logs] (ログ)、[Log groups] (ロググループ) の順に選択します。
3. ロググループのリストで、 証跡のために作成したロググループを選択します。
4. [メトリクスフィルター] または [アクション] メニューから [メトリクスフィルターの作成] を選択します。
5. [パターンを定義] ページの [フィルターパターンの作成] で、[フィルターパターン] に以下の値を入力します。

   ```
   { ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }
   ```

6. [テストパターン] のデフォルト値はそのままにしておきます。[次へ] をクリックします。
7. [メトリクスの割り当て] ページの [フィルター名]に「**ConsoleSignInFailures**」と入力します。
8. [メトリクスの詳細] ページで、[新しく作成する] をオンにして [メトリクス名前空間] に「**CloudTrailMetrics**」と入手します。
9. [メトリクス名] に「**ConsoleSigninFailureCount**」と入力します。
10. [メトリクス値] に「**1**」と入力します。
11. [Default value] は空白のままにします。
12. [次へ] をクリックします。
13. [Review and create] ページで選択内容を確認します。[Create metric filter] を選択してフィルターを作成するか、[編集] を選択して戻って値を変更します。

アラームの作成

メトリックスフィルターを作成すると、 CloudWatch CloudTrailトレイルロググループの「ログログループ詳細」ページが開きます。アラームを作成するには、次の手順を実行します。

1. [メトリクスフィルター] タブで、the section called “メトリックフィルタを作成する” で作成したメトリクスフィルターを見つけます。メトリクスフィルターのチェックボックスをオンにします。[メトリクスフィルター] バーで、[アラームの作成] を選択します。
2. [アラームの作成] ページの、[メトリクスと条件を指定] ページで、以下の値を入力します。

   a. [グラフ] には、アラームを作成したときに設定した他の設定に基づいてラインが **3** で設定されています。

   b. [メトリクス名] は、現在のメトリクス名、**ConsoleSigninFailureCount** のままにしておきます。

   c. [Statistic] は、デフォルト値、**Sum** のままにしておきます。

   d. [Period] は、デフォルト値、**5 minutes** のままにしておきます。

   e. [条件] セクションの [しきい値のタイプ] で、[静的] を選択します。

   f. [Whenever ***metric_name*** is] は、[Greater/Equal] を選択します。

   g. しきい値に「**3**」と入力します。

   h. [Additional configuration] は、デフォルト値のままにしておきます。[次へ] をクリックします。
3. [アクションの設定] ページの [通知] で [アラーム中] を選択します。これは、5 分以内に 3 件の変更イベントというしきい値を超えConsoleSigninFailureCount、アラーム状態になったときにアクションが実行されることを示します。

   a. [次の SNS トピックに通知を送信] で、[新しいトピックの作成] を選択します。

   b. 新しい Amazon SNS トピックの名前として「**ConsoleSignInFailures_CloudWatch_Alarms_Topic**」と入力します。

   c. [通知を受け取る E メールエンドポイント] に、このアラームが発生した場合に通知を受信するユーザーの E メールアドレスを入力します。E メールアドレスはカンマで区切ります。

      それぞれの E メール受信者に Amazon SNS トピックのサブスクライブを確認する E メールが送信されます。

   d. [Create topic] (トピックの作成) を選択します。
4. この例では、他のアクションタイプはスキップします。[次へ] をクリックします。

5. [Add name and description] ページで、アラームのフレンドリ名と説明を入力します。この例では、名前には「**Console sign-in failures**」、説明には「**Raises alarms if more than 3 console sign-in failures occur in 5 minutes**」を入力します。[次へ] をクリックします。
6. [Review and create] ページで選択内容を確認します。[] で変更を加えることができます。または、[アラームの作成] を選択してアラームを作成します。

   アラームを作成したら、「アラーム CloudWatch 」ページを開きます。アラームの[アクション] 列に、 SNS トピックのすべての E メール受信者が SNS 通知のサブスクライブを希望していることを確認するまで、[Pending confirmation] が表示されます。

例: IAM ポリシーの変更

IAM ポリシーを変更するための API 呼び出しが行われたときにトリガーされる Amazon CloudWatch アラームを作成するには、次の手順に従います。

メトリックフィルタを作成する

1. https://console.aws.amazon.com/cloudwatch/ CloudWatch でコンソールを開きます。
2. ナビゲーションペインで [ログ] を選択します。
3. ロググループのリストで、 証跡のために作成したロググループを選択します。
4. [アクション]、[メトリクスフィルターの作成] の順に選択します。
5. [パターンを定義] ページの [フィルターパターンの作成] で、[フィルターパターン] に以下の値を入力します。

   ```
   {($.eventName=DeleteGroupPolicy)||($.eventName=DeleteRolePolicy)||
   ($.eventName=DeleteUserPolicy)||($.eventName=PutGroupPolicy)||
   ($.eventName=PutRolePolicy)||($.eventName=PutUserPolicy)||
   ($.eventName=CreatePolicy)||($.eventName=DeletePolicy)||
   ($.eventName=CreatePolicyVersion)||($.eventName=DeletePolicyVersion)||
   ($.eventName=AttachRolePolicy)||($.eventName=DetachRolePolicy)||
   ($.eventName=AttachUserPolicy)||($.eventName=DetachUserPolicy)||
   ($.eventName=AttachGroupPolicy)||($.eventName=DetachGroupPolicy)}
   ```

6. [テストパターン] のデフォルト値はそのままにしておきます。[次へ] をクリックします。
7. [メトリクスの割り当て] ページの [フィルター名]に「**IAMPolicyChanges**」と入力します。
8. [メトリクスの詳細] ページで、[新しく作成する] をオンにして [メトリクス名前空間] に「**CloudTrailMetrics**」と入手します。

9. [メトリクス名] に「**IAMPolicyEventCount**」と入力します。
10. [メトリクス値] に「**1**」と入力します。
11. [Default value] は空白のままにします。
12. [次へ] をクリックします。
13. [Review and create] ページで選択内容を確認します。[Create metric filter] を選択してフィルターを作成するか、[編集] を選択して戻って値を変更します。

アラームの作成

メトリックスフィルターを作成すると、 CloudWatch CloudTrailトレイルロググループの「ログロググループ詳細」ページが開きます。アラームを作成するには、次の手順を実行します。

1. [メトリクスフィルター] タブで、the section called “メトリックフィルタを作成する” で作成したメトリクスフィルターを見つけます。メトリクスフィルターのチェックボックスをオンにします。[メトリクスフィルター] バーで、[アラームの作成] を選択します。
2. [アラームの作成] ページの、[メトリクスと条件を指定] ページで、以下の値を入力します。

   a. [グラフ] には、アラームを作成したときに設定した他の設定に基づいてラインが **1** で設定されています。

   b. [メトリクス名] は、現在のメトリクス名、**IAMPolicyEventCount** のままにしておきます。

   c. [Statistic] は、デフォルト値、**Sum** のままにしておきます。

   d. [Period] は、デフォルト値、**5 minutes** のままにしておきます。

   e. [条件] セクションの [しきい値のタイプ] で、[静的] を選択します。

   f. [Whenever ***metric_name*** is] は、[Greater/Equal] を選択します。

   g. しきい値に「**1**」と入力します。

   h. [Additional configuration] は、デフォルト値のままにしておきます。[次へ] をクリックします。

   i.

3. 「アクションの設定」ページの「通知」で、「アラーム中」を選択します。これは、5 分以内に 1 件の変更イベントというしきい値を超え、IAM PolicyEventCount がアラーム状態になったときにアクションが実行されることを示します。

   a. [次の SNS トピックに通知を送信] で、[新しいトピックの作成] を選択します。

b. 新しい Amazon SNS トピックの名前として「**IAM_Policy_Changes_CloudWatch_Alarms_Topic**」と入力します。

c. [通知を受け取る E メールエンドポイント] に、このアラームが発生した場合に通知を受信するユーザーの E メールアドレスを入力します。E メールアドレスはカンマで区切ります。

それぞれの E メール受信者に Amazon SNS トピックのサブスクライブを確認する E メールが送信されます。

d. [Create topic] (トピックの作成) を選択します。

4. この例では、他のアクションタイプはスキップします。[次へ] をクリックします。

5. [Add name and description] ページで、アラームのフレンドリ名と説明を入力します。この例では、名前には「**IAM Policy Changes**」、説明には「**Raises alarms if IAM policy changes occur**」を入力します。[次へ] をクリックします。

6. [Review and create] ページで選択内容を確認します。[] で変更を加えることができます。または、[アラームの作成] を選択してアラームを作成します。

アラームを作成したら、「アラーム CloudWatch 」ページを開きます。アラームの[アクション] 列に、 SNS トピックのすべての E メール受信者が SNS 通知のサブスクライブを希望していることを確認するまで、[Pending confirmation] が表示されます。

CloudWatch Logs アラームの通知を設定します。

アラームがトリガーされるたびに通知を送信するように CloudWatch Logs を設定できます。CloudTrailこれにより、イベントに記録され、 CloudTrail CloudWatch ログによって検出された重要な運用イベントに迅速に対応できます。 CloudWatch Amazon Simple Notification Service (SNS) を使用して E メールを送信します。詳細については、CloudWatch ユーザーガイドの「Amazon SNS 通知の設定」を参照してください。

CloudTrail CloudWatch ログへのイベントの送信を停止する

CloudWatch CloudWatch 記録を更新してログ設定を無効にすることで、Amazon Logs AWS CloudTrail へのイベントの送信を停止できます。

CloudWatch Logs へのイベントの送信を停止する (コンソール)

CloudWatch Logs CloudTrail へのイベントの送信を停止するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. ナビゲーションペインで、[Trails] (追跡) を選択します。
3. CloudWatch Logs インテグレーションを無効にするトレイルの名前を選択します。
4. 「CloudWatch ログ」で「編集」を選択します。
5. [有効] チェックボックスをオフにします。
6. [変更を保存] を選択します。

CloudWatch ログへのイベントの送信を停止する (CLI)

update-trailコマンドを実行すると、 CloudWatch Logs ロググループを配信エンドポイントから削除できます。次のコマンドは、ロググループ ARN とログロール ARN の値を空の値に置き換えることにより、 CloudWatch トレイル設定からロググループとロールをクリアします。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

CloudWatch のロググループとログストリームの命名 CloudTrail

Amazon CloudWatch は、 CloudTrail イベント用に作成したロググループを、リージョン内の他のロググループとともに表示します。他のロググループと簡単に区別できようなロググループ名を使用することをお勧めします。例えば、**`CloudTrail/logs`** 。

ロググループの名前を指定する際は、これらのガイドラインに従います。

- ロググループ名は AWS アカウントのリージョン内で一意である必要があります。
- ロググループの名前は 1～512 文字で指定します。
- ロググループ名には、a～z、A～Z、0～9、'_' (下線)、'-' (ハイフン)、'/' (スラッシュ)、 '.' (ピリオド) および '#' (番号記号) を使用できます。

CloudTrail *####################Account_ID _ _ CloudTrail trail_region ###### ##################*

> **Note**
>
> CloudTrail ログの量が多い場合は、複数のログストリームを作成してログデータをロググループに配信できます。*###############account_ID _ trail_region CloudTrail _ number CloudTrail ######################*

CloudWatch ロググループの詳細については、Amazon CloudWatch Logs ユーザーガイドと Amazon Logs API リファレンスの「CreateLogGroup CloudWatch ロググループとログストリームの操作」を参照してください。

CloudTrail CloudWatch ログを監視に使用するためのロールポリシードキュメント

このセクションでは、 CloudTrail ロールがログイベントを CloudWatch Logs に送信するために必要なアクセス権限ポリシーについて説明します。で説明されているように、 CloudTrail イベントを送信するように設定するときに、ポリシードキュメントをロールにアタッチできます CloudWatch ログへのイベントの送信。IAM を使用してロールを作成することもできます。詳細については、「にアクセス権限を委任するロールの作成」 AWS のサービスまたは「IAM ロールの作成 ()AWS CLI」を参照してください。

次のポリシードキュメントの例には、 CloudWatch 指定したロググループにログストリームを作成し、米国東部 (オハイオ) CloudTrail リージョンのそのログストリームにイベントを配信するために必要な権限が含まれています。(これは、デフォルトの IAM ロール `CloudTrail_CloudWatchLogs_Role` に対するデフォルトのポリシーです。)

> **Note**
>
> 混乱した代理防止は、 CloudWatch ログ監視のロールポリシーには適用されません。`aws:SourceArn`ロールポリシーはとの使用をサポートしていませんaws:SourceAccount。

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

```
      "Sid": "AWSCloudTrailCreateLogStream2014110",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]

    },
    {
      "Sid": "AWSCloudTrailPutLogEvents20141101",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:us-east-2:accountID:log-group:log_group_name:log-
stream:CloudTrail_log_stream_name_prefix*"
      ]
    }
  ]
}
```

組織の証跡にも使用される可能性があるポリシーを作成している場合は、その口ール用に作成されたデフォルトポリシーから変更する必要があります。*##############log_group_name CloudWatch ################################## 111111111111 #####o-exampleorgid # ID ########### 111111111111 CloudTrail CloudTrail AWS ###### ## AWS Organizations*

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream20141101",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
```

```
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:111111111111_CloudTrail_us-east-2*",
                "arn:aws:logs:us-east-2:111111111111:log-group:log_group_name:log-
stream:o-exampleorgid_*"
            ]
        }
    ]
}
```

組織の証跡の詳細については、「組織の証跡の作成」を参照してください。

CloudTrail 複数のアカウントからのログファイルの受信

複数のログファイルを 1 つの Amazon S3 CloudTrail AWS アカウント バケットに配信できます。たとえば、アカウント ID が 111111111111、222222222222、333333333333、444444444444 の 4 AWS アカウント つのアカウントがあり、これらの 4 つのアカウントすべてのログファイルをアカウント 111111111111 CloudTrail に属するバケットに配信するように設定したいとします。これを行うには、以下の手順を実行します。

1. 配信先バケットが配置されるアカウント (この例では 111111111111) で、証跡を作成します。他のアカウントについては、まだ証跡を作成しないでください。

   手順については、「コンソールで証跡を作成する」を参照してください。
2. 宛先バケットのバケットポリシーを更新して、にクロスアカウント権限を付与します。CloudTrail

   手順については、「複数のアカウントのバケットポリシーの設定」を参照してください。
3. アクティビティを ログ記録したい他のアカウント (この例では 222222222222、333333333333、444444444444) で、証跡を作成します。各アカウントで証

跡を作成する場合は、ステップ 1 で指定したアカウント (この例では 111111111111) に属する Amazon S3 バケットを指定します。手順については、「追加アカウントでの証跡の作成」を参照してください。

> **Note**
>
> SSE-KMS 暗号化を有効にする場合は、KMS キーポリシーで、キーを使用してログファイルを暗号化し、 CloudTrail 指定したユーザーが暗号化されていない形式のログファイルを読み取ることを許可する必要があります。キーポリシーを手動で編集する方法については、AWS KMS の主要ポリシーの設定 CloudTrail を参照してください。

他のアカウントでコールされたデータイベントのバケット所有者アカウント ID を秘匿化する

従来、Amazon S3 CloudTrail データイベント API 呼び出し側でデータイベントが有効になっていた場合は、データイベント (など`PutObject`) に S3 バケット所有者のアカウント ID CloudTrail が表示されていました。 AWS アカウント これは、バケット所有者アカウントで S3 データイベントが有効ではない場合も発生します。

これで、以下の条件が両方とも満たされた場合に、`resources`ブロック内の S3 バケット所有者のアカウント ID CloudTrail が削除されるようになりました。

- データイベント API 呼び出しは、Amazon S3 AWS アカウント バケット所有者とは別のユーザーからのものです。
- API 発信者が発信者アカウントでのみ `AccessDenied` エラーを受信した場合。

API コールを実行したリソースの所有者は、引き続き完全なイベントを受信します。

次のイベントレコードのスニペットは、期待される動作の一例です。`Historic` スニペットでは、S3 バケット所有者のアカウント ID 123456789012 が、別のアカウントから API 発信者に表示されます。現在の動作例では、バケット所有者のアカウント ID は表示されません。

```
# Historic

"resources": [
    {
        "type": "AWS::S3::Object",
```

```
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

以下は現在の動作です。

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::test-my-bucket-2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::test-my-bucket-2"
    }
]
```

トピック

- 複数のアカウントのバケットポリシーの設定
- 追加アカウントでの証跡の作成

複数のアカウントのバケットポリシーの設定

バケットが複数のアカウントからログファイルを受信するには、そのバケットポリシーで、CloudTrail 指定したすべてのアカウントからログファイルを書き込む権限を付与する必要があります。つまり、宛先バケットのバケットポリシーを変更して、 CloudTrail 指定した各アカウントからログファイルを書き込む権限を付与する必要があります。

> **Note**
>
> セキュリティ上の理由から、権限のないユーザーは S3KeyPrefix パラメータとして AWSLogs/ を含む証跡を作成することはできません。

複数のアカウントからファイルを受信できるようにバケットのアクセス権限を変更するには

1. バケットを所有するアカウント (この例では 111111111111) AWS Management Console を使用してにサインインし、Amazon S3 コンソールを開きます。
2. CloudTrail ログファイルを配信するバケットを選択し、[権限] を選択します。
3. [Bucket policy] (バケットポリシー) で [Edit] (編集) を選択します。
4. 既存のポリシーを変更して、このバケットに配信するログファイルを持つ追加のアカウントごとに行を追加します。次のサンプルポリシーを参照して、2 番目のアカウント ID を指定する下線が引かれた Resource 行に注意してください。セキュリティのベストプラクティスとして、aws:SourceArn 条件キーを Amazon S3 バケットポリシーに追加します。これにより、S3 バケットへの不正アクセスを防止できます。既存の証跡がある場合は、必ず 1つまたは複数の条件キーを追加してください。

   > **Note**
   >
   > AWS アカウント ID は、先頭のゼロを含む 12 桁の数字です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSCloudTrailAclCheck20131101",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::myBucketName",
      "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
```

```
                "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
              ]
            }
          }
      },
      {
        "Sid": "AWSCloudTrailWrite20131101",
        "Effect": "Allow",
        "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": [
          "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/111111111111/*",
          "arn:aws:s3:::myBucketName/optionalLogFilePrefix/AWSLogs/222222222222/*"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceArn": [
              "arn:aws:cloudtrail:region:111111111111:trail/primaryTrailName",
              "arn:aws:cloudtrail:region:222222222222:trail/secondaryTrailName"
            ],
            "s3:x-amz-acl": "bucket-owner-full-control"
          }
        }
      }
    ]
}
```

追加アカウントでの証跡の作成

AWS アカウント コンソールまたはを使用して追加の記録を作成し、 AWS CLI そのログファイルを 1 つの Amazon S3 バケットに集約できます。あるいは、組織証跡を作成して、 AWS アカウント 組織に属するすべての人を記録することもできます。 AWS Organizations詳細については、「組織の証跡の作成」を参照してください。

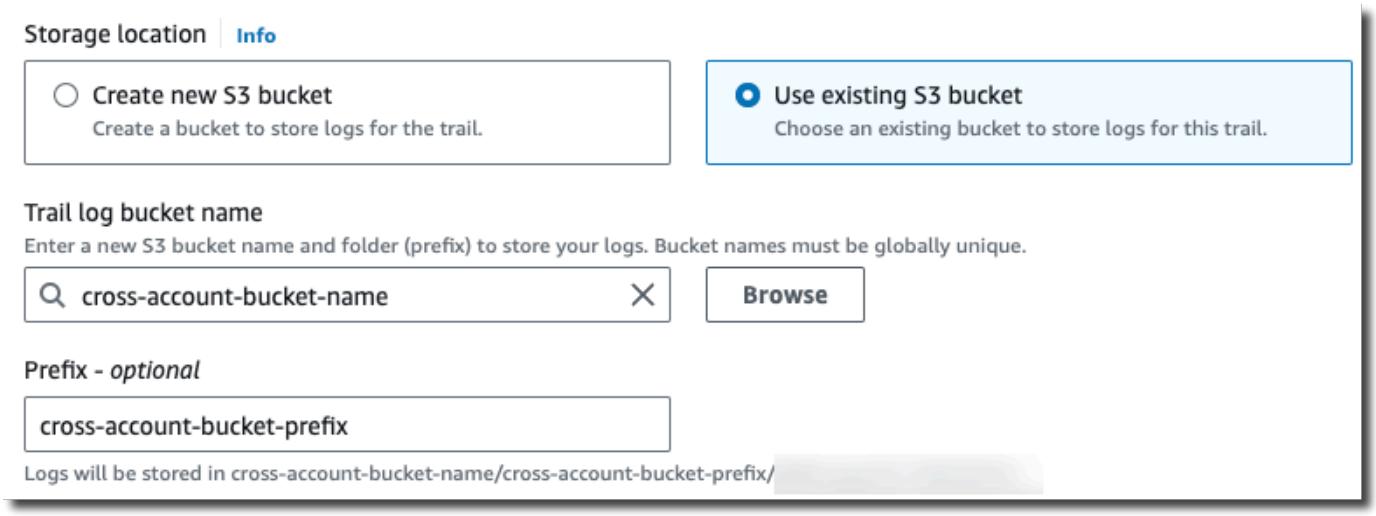
AWS コンソールを使用して追加のアカウントの証跡を作成します。

CloudTrail コンソールを使用して、追加のアカウントの証跡を作成できます。

1. AWS Management Console 証跡を作成したいアカウントでサインインします。コンソールを使用して証跡を作成するには、「コンソールで証跡を作成する」の手順に従います。

2. ストレージの場所で、既存の S3 バケットを使用を選択します。テキストボックスに、アカウント全体のログファイルの保存に使用するバケットの名前を入力します。

> **Note**
>
> バケットポリシーは、 CloudTrail 書き込み権限を付与する必要があります。バケットポリシーを手動で編集する方法については、複数のアカウントのバケットポリシーの設定を参照してください。



3. [プレフィックス] には、アカウント全体のログファイルの保存に使用するプレフィックスを入力します。バケットポリシーで指定したものとは異なるプレフィックスを使用する場合は、宛先バケットのバケットポリシーを編集して、 CloudTrail この新しいプレフィックスを使用してバケットにログファイルを書き込めるようにする必要があります。

CLI AWS を使用して追加のアカウントで証跡を作成する

AWS コマンドラインツールを使用して、追加のアカウントの記録を作成し、そのログファイルを 1 つの Amazon S3 バケットに集約できます。これらのツールの詳細については、『AWS CLI コマンドリファレンス』の「cloudtrail」を参照してください。

create-trail コマンドを使用して以下を指定し、証跡を作成します。

- `--name` は、証跡の名前を指定します。
- `--s3-bucket-name` は、アカウント全体のログファイルの保存に使用する Amazon S3 バケットを指定します。

- `--s3-prefix` は、ログファイルの配信パスのプレフィックスを指定します (オプション)。
- `--is-multi-region-trail` AWS 作業中のパーティション内のすべてのリージョンのイベントをこのトレイルが記録するように指定します。

AWS アカウントがリソースを運用しているリージョンごとに 1 つのトレイルを作成できます。

次のコマンド例は、 AWS CLIを使用して追加のアカウントの証跡を作成する方法を示しています。これらのアカウントのログファイルが、最初のアカウント (この例では 111111111111) で作成したバケットに配信されるようにするには、`--s3-bucket-name` オプションでバケット名を指定します。Amazon S3 バケット名は、グローバルに一意です。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name my-bucket --is-multi-
region-trail
```

コマンドを実行すると、以下のような出力が表示されます。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "AWSCloudTrailExample",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:222222222222:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "MyBucketBelongingToAccount111111111111"
}
```

CloudTrail コマンドラインツールの使用について詳しくは、 AWS CloudTrail コマンドラインリファレンスをご覧ください。

CloudTrail AWS アカウント間でのログファイルの共有

このセクションでは、 CloudTrail AWS 複数のアカウント間でログファイルを共有する方法について説明します。ログを共有するために使用する方法は、S3 AWS アカウント バケットの設定によって異なります。ログファイルを共有するためのオプションは次のとおりです。

- バケット所有者の強制 – S3 オブジェクトの所有権は Amazon S3 バケットレベルの設定であり、バケットにアップロードされたオブジェクトの所有権を制御し、アクセスコントロールリスト (ACL) を有効または無効にために使用できます。デフォルトでは、オブジェクト所有権は [バケット所有者の強制] により設定され、すべての ACL は無効になっています。ACL が無効になってい

る場合、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。[バケット所有者の強制] オプションを設定すると、アクセスはバケットポリシーによって管理されるため、ユーザーが役割を引き受ける必要がなくなります。

- ログファイルを共有するロールを引き受ける – [バケット所有者の強制] 設定を選択していない場合、ユーザーは S3 バケット内のログファイルにアクセスするロールを引き受ける必要があります。

ロールを引き受けてアカウント間でログファイルを共有する

> **Note**
>
> このセクションは、[バケット所有者の強制] 設定を使用していない Amazon S3 バケットにのみ適用されます。

このセクションでは、 CloudTrail AWS アカウント ロールを引き受けて複数の間でログファイルを共有する方法と、ログファイルを共有するシナリオについて説明します。

- シナリオ 1: Amazon S3 バケットに保存されているログファイルの生成元のアカウントに、読み取り専用のアクセス権限を付与します。
- シナリオ 2: Amazon S3 バケット内のすべてのログファイルへのアクセス権を、ログファイルを分析するためのサードパーティのアカウントに付与します。

Amazon S3 バケット内のログファイルへの読み取り専用アクセス権を付与するには

1. ログファイルを共有する各アカウントのために、IAM ロールを作成します。アクセス許可を付与するには管理者である必要があります。

   ロールを作成する場合、以下の作業を行います。

   - [その他の AWS アカウント] オプションを選択します。
   - アクセス許可が付与されるアカウントの、12 桁のアカウント ID を入力します。
   - ロールを割り当てる前に、ユーザーに多要素認証を提供させる場合は、[Require MFA] ボックスをオンにします。
   - AmazonS3 ReadOnlyAccess ポリシーを選択してください。

> **Note**
>
> デフォルトでは、AmazonS3 ReadOnlyAccess ポリシーは、アカウント内のすべての Amazon S3 バケットに取得権限と一覧表示権限を付与します。

IAM ロールのアクセス許可の管理の詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

2. ログファイルを共有するアカウントに読み取り専用のアクセス権限を付与する、アクセスポリシーを作成します。
3. ログファイルを取得するロールを引き受けるよう、各アカウントに指示します。

サードパーティアカウントにログファイルへの読み取り専用アクセス権を付与するには

1. ログファイルを共有するサードパーティアカウント用の IAM ロールを作成します。アクセス許可を付与するには管理者である必要があります。

   ロールを作成する場合、以下の作業を行います。

   - [その他の AWS アカウント] オプションを選択します。
   - アクセス許可が付与されるアカウントの、12 桁のアカウント ID を入力します。
   - ロールを担当できるユーザーをより高度に制御できるようにするための、外部 ID を入力します。詳細については、IAM ユーザーガイドの「AWS リソースへのアクセスを第三者に許可する際に外部 ID を使用する方法」を参照してください。
   - AmazonS3 ReadOnlyAccess ポリシーを選択します。

   > **Note**
   >
   > デフォルトでは、AmazonS3 ReadOnlyAccess ポリシーは、アカウント内のすべての Amazon S3 バケットに取得権限と一覧表示権限を付与します。

2. ログファイルを共有するサードパーティアカウントに読み取り専用のアクセス権限を付与する、アクセスポリシーを作成します。
3. ログファイルを取得するロールを引き受けるよう、サードパーティアカウントに指示します。

次のセクションでは、これらの手順についてさらに詳しく説明しています。

トピック

- 自分が所有するアカウントへのアクセスを許可するアカウントポリシーの作成
- アクセスポリシーを作成してサードパーティにアクセス権限を付与する
- ロールを割り当てる
- CloudTrail AWS アカウント間でのログファイルの共有を停止します。

自分が所有するアカウントへのアクセスを許可するアカウントポリシーの作成

Amazon S3 バケットの所有者は、 CloudTrail 他のアカウントのログファイルを書き込む Amazon S3 バケットを完全に制御できます。各ビジネスユニットのログファイルを、それらを作成したビジネスユニットと共有したい場合を考えます。ただし、ユニットが他のユニットのログファイルを読み取ることはできないようにします。

例えば、アカウント B が所有するログファイルをアカウント B と共有し、アカウント C とは共有しない場合は、アカウント B が信頼されたアカウントであることを指定する新しい IAM ロールを、自分のアカウントに作成する必要があります。このロールの信頼ポリシーは、アカウント B が信頼されており、自分のアカウントによって作成されたロールを継承できることを指定するもので、次の例のようになります。コンソールを使用してロールを作成した場合は、信頼ポリシーが自動的に作成されます。SDK を使用してロールを作成する場合は、`CreateRole` API へのパラメータとして信頼ポリシーを指定する必要があります。CLI を使用してロールを作成する場合は、`create-role` CLI コマンドで信頼ポリシーを指定する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-B-id:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

アカウント B が読み取りできるのは、それ自体がログファイルを書き込んだ先の場所からのみであることを指定するために、アクセスポリシーも作成する必要があります。アクセスポリシーは次のようになります。リソース ARN には、アカウント B の 12 桁のアカウント ID と、集計プロセス中にアカウント B CloudTrail で有効にしたときに指定したプレフィックス (存在する場合) が含まれることに注意してください。プレフィックスを指定する方法については、「追加アカウントでの証跡の作成」を参照してください。

> **Important**
>
> アクセスポリシーのプレフィックスは、アカウント B で有効にしたときに指定したプレフィックスとまったく同じであることを確認する必要があります。そうでない場合は、アカウントの IAM ロールアクセスポリシーを編集して、アカウント B の実際のプレフィックスを組み込む必要があります。ロールアクセスポリシーのプレフィックスが、アカウント B CloudTrail でオンにしたときに指定したプレフィックスとまったく同じでない場合、アカウント B はログファイルにアクセスできません。 CloudTrail

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/account-B-id/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::bucket-name"
    }
  ]
}
```

追加するアカウントに対しても前述のプロセスを使用します。

各アカウントのロールを作成し、適切な信頼ポリシーとアクセスポリシーを指定した後、また、各アカウントの IAM ユーザーがそのアカウントの管理者によってアクセスを許可された後、アカウント B または C の IAM ユーザーは、プログラムによってロールを継承できます。

詳細については、「ロールを割り当てる」を参照してください。

アクセスポリシーを作成してサードパーティにアクセス権限を付与する

サードパーティアカウント用に個別の IAM ロールを作成する必要があります。ロールを作成すると、 AWS によって信頼関係が自動的に作成され、サードパーティアカウントが信頼されたロールの割り当て先であることを指定します。アカウントがどのアクションを実行できるかは、ロールのアクセスポリシーによって指定されます。ロールの作成の詳細については、「IAM ロールの作成」を参照してください。

たとえば、によって作成された信頼関係では、作成したロールをサードパーティのアカウント (この例ではアカウント Z) AWS が信頼されるよう指定されています。以下に示しているのは、信頼ポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole"
    }]
}
```

サードパーティアカウント用のロールを作成する際に外部 ID を指定した場合は、そのアカウントによって割り当てられた一意の ID をテストする Condition 要素が、アクセスポリシー内に追加されます。このテストはロールを引き受けた時点で実行されます。次の例では、アクセスポリシーに Condition 要素が含まれています。

詳細については、IAM ユーザーガイドの「AWS リソースへのアクセスを第三者に許可する際に外部 ID を使用する方法」を参照してください。

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

```
    "Statement": [{
        "Sid": "",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::account-Z-id:root"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"sts:ExternalId": "external-ID-issued-by-
account-Z"}}
    }]
}
```

また、自分のアカウントでアクセスポリシーを作成して、サードパーティアカウントが Amazon S3 バケットからすべてのログを読み取れるように指定する必要もあります。アクセスポリシーは、次の例のようになります。Resource 値の末尾のワイルドカード (*) は、アクセス権限を付与されたサードパーティアカウントが、S3 バケット内の任意のログファイルをアクセスできることを示しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
    ]
}
```

サードパーティアカウントのロールを作成し、適切な信頼関係とアクセスポリシーを指定した後、そのサードパーティアカウント内の IAM ユーザーにプログラムでロールを割り当てて、ユーザーがバケットからログファイルを読み取れるようにする必要があります。詳細については、「ロールを割り当てる」を参照してください。

ロールを割り当てる

各アカウントで作成したロールを担う、IAM ユーザーを個別に指定する必要があります。次に、各 IAM ユーザーに適切な権限が与えられていることを確認する必要があります。

IAM ユーザーとロール

必要なロールとポリシーを作成した後は、ファイルを共有するアカウントで IAM ユーザーを指定する必要があります。ログファイルにアクセスするには、プログラムによって各 IAM ユーザーが適切なロールを引き受けます。ユーザーがロールを引き受けると、 AWS は、一時的なセキュリティ認証情報をそのユーザーに返します。その後、ロールに関連するアクセスポリシーによって付与された権限に応じて、ログファイルのリスト、取得、コピー、削除をリクエストできます。

IAM ID の詳細については、「IAM ID (ユーザー、ユーザーグループ、ロール)」を参照してください。

各シナリオで各 IAM ロールに対して作成するアクセスポリシーの主な相違点。

- シナリオ 1 では、アクセスポリシーが、各アカウントを自分のログファイルの読み取りのみに制限します。詳細については、「自分が所有するアカウントへのアクセスを許可するアカウントポリシーの作成」を参照してください。
- シナリオ 2 では、アクセスポリシーが、Amazon S3 バケットに集計されたすべてのログファイルを読み取ることを、サードパーティに許可します。詳細については、「アクセスポリシーを作成してサードパーティにアクセス権限を付与する」を参照してください。

IAM ユーザーに対するアクセス許可ポリシーを作成する

ロールで許可されているアクションを実行するには、IAM ユーザーに API を呼び出す権限が必要です。 AWS STS `AssumeRole` ユーザーごとのポリシーを編集し、ユーザーに適切なアクセス許可を付与する必要があります。そのためには、IAM ユーザーにアタッチするポリシーの [リソース] 要素を設定します。以下の例では、アカウント A によって以前に作成された `Test` という名前のロールを引き受けることを、別のアカウントのIAM ユーザーに許可するためのポリシーを示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::account-A-id:role/Test"
```

```
    }
  ]
}
```

カスタマー管理ポリシーを編集するには (コンソール)

1. AWS Management Console にサインインし、https://console.aws.amazon.com/iam/ にある IAM コンソールを開きます。
2. ナビゲーションペインで、ポリシー を選択します。
3. ポリシーの一覧で、編集するポリシーの名前を選択します。検索ボックスを使用して、ポリシーのリストをフィルタリングできます。
4. [アクセス許可] タブを選択し、[編集] を選択します。
5. 次のいずれかを行います。

   - [ビジュアル] オプションを選択し、JSON 構文を理解することなくポリシーを変更します。ポリシー内の各権限ブロックのサービス、アクション、リソース、またはオプションの条件を変更することができます。また、ポリシーをインポートして、ポリシーの最下部に権限を追加することもできます。変更が完了したら、[次へ] を選択して続行します。
   - [JSON] オプションを選択し、JSON テキストボックスにテキストを入力または貼り付けてポリシーを変更します。また、ポリシーをインポートして、ポリシーの最下部に権限を追加することもできます。ポリシーの検証中に生成されたセキュリティ警告、エラー、または一般的な警告を解決してから、[Next] (次へ) を選択します。

   > **Note**
   >
   > いつでも [Visual] と [JSON] エディタオプションを切り替えることができます。ただし、[Visual] エディタで [次] に変更または選択した場合、IAM はポリシーを再構成して visual エディタに合わせて最適化することがあります。詳細については、「IAM ユーザーガイド」の「ポリシーの再構成」を参照してください。

6. [確認して保存] ページで、このポリシーで定義されているアクセス許可を確認し、[変更を保存] を選択して作業を保存します。
7. 最大 5 つのバージョンの管理ポリシーがすでにある場合は、[変更を保存] を選択すると、ダイアログボックスが表示されます。新しいバージョンを保存するには、ポリシーの最も古い非デフォルトバージョンが削除され、この新しいバージョンに置き換えられます。オプションで、新しいバージョンをポリシーのデフォルトバージョンとして設定できます。

[ポリシーを保存] を選択して、新しいバージョンのポリシーを保存します。

通話 AssumeRole

ユーザーは、 AWS STS AssumeRoleAPI を呼び出し、ロールセッション名、引き受けるロールの Amazon リソース番号 (ARN)、およびオプションの外部 ID を渡すアプリケーションを作成することで、ロールを引き受けることができます。ロールセッション名は、引き受けるロールを作成したアカウントによって定義されます。外部 ID (ある場合) は、サードパーティアカウントによって定義され、ロールに含めるよう、そのロールの作成時に所有アカウントに渡されます。詳細については、『IAM ユーザーガイド』の「AWS リソースへのアクセスを第三者に許可する際に外部 ID を使用する方法」を参照してください。IAM コンソールを開くことによって、アカウント A から ARN を取得できます。

IAM コンソールを使用してアカウント A で ARN の値を探すには

1. [Roles] を選択します。
2. 調べるロールを選択します。
3. [Summary] セクションで [Role ARN] を検索します。

AssumeRole API は、所有アカウントのリソースへのアクセスに使用する一時的な認証情報を返します。この例では、アクセスするリソースは Amazon S3 バケットと、そのバケットに含まれるログファイルです。この一時的な認証情報には、ロールのアクセスポリシーで定義したアクセス許可があります。

次の Python の例 (AWS SDK for Python (Boto) を使用) では、AssumeRole を呼び出す方法、および返された一時的な認証情報を使用して、アカウント A によって管理されるすべての Amazon S3 バケットの一覧を取得する方法を示します。

```
def list_buckets_from_assumed_role(user_key, assume_role_arn, session_name):
    """
    Assumes a role that grants permission to list the Amazon S3 buckets in the account.
    Uses the temporary credentials from the role to list the buckets that are owned
    by the assumed role's account.

    :param user_key: The access key of a user that has permission to assume the role.
    :param assume_role_arn: The Amazon Resource Name (ARN) of the role that
                            grants access to list the other account's buckets.
    :param session_name: The name of the STS session.
```

```
    """
    sts_client = boto3.client(
        "sts", aws_access_key_id=user_key.id, aws_secret_access_key=user_key.secret
    )
    try:
        response = sts_client.assume_role(
            RoleArn=assume_role_arn, RoleSessionName=session_name
        )
        temp_credentials = response["Credentials"]
        print(f"Assumed role {assume_role_arn} and got temporary credentials.")
    except ClientError as error:
        print(
            f"Couldn't assume role {assume_role_arn}. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise

    # Create an S3 resource that can access the account with the temporary credentials.
    s3_resource = boto3.resource(
        "s3",
        aws_access_key_id=temp_credentials["AccessKeyId"],
        aws_secret_access_key=temp_credentials["SecretAccessKey"],
        aws_session_token=temp_credentials["SessionToken"],
    )
    print(f"Listing buckets for the assumed role's account:")
    try:
        for bucket in s3_resource.buckets.all():
            print(bucket.name)
    except ClientError as error:
        print(
            f"Couldn't list buckets for the account. Here's why: "
            f"{error.response['Error']['Message']}"
        )
        raise
```

CloudTrail AWS アカウント間でのログファイルの共有を停止します。

他のアカウントとのログファイルの共有を停止するには AWS アカウント、そのアカウント用に作成したロールを削除します。ロールを削除する方法の詳細については、「ロールまたはインスタンスプロファイルの削除」を参照してください。

CloudTrail ログファイルの整合性の検証

CloudTrail ログファイルが配信後に変更されたか、削除されたか、変更されていないかを判断するには、 CloudTrail ログファイルの整合性検証を使用できます。この機能は、業界標準のアルゴリズムを使用して構築されています。ハッシュ用の SHA-256 とデジタル署名用の RSA を備えた SHA-256。これにより、検出されずにログファイルを変更、削除、または偽造することは計算上不可能になります。 CloudTrail を使用して、 AWS CLI 配信された場所にあるファイルを検証できます。 CloudTrail

使用する理由

検証されたログファイルは、セキュリティおよびフォレンシック調査で非常に重要です。たとえば、検証されたログファイルを使用すると、ログファイル自体が変更されていないこと、または特定のユーザーの認証情報が特定の API アクティビティを実行したことを確実にアサートできます。CloudTrail ログファイルの整合性検証プロセスでは、ログファイルが削除または変更されたかどうかを確認したり、特定の期間にログファイルがアカウントに配信されなかったことを確認したりすることもできます。

仕組み

ログファイルの整合性検証を有効にすると、 CloudTrail 配信されるすべてのログファイルのハッシュが作成されます。 CloudTrail また、過去 1 時間のログファイルを参照し、それぞれのハッシュを含むファイルを 1 時間ごとに作成して配信します。このファイルはダイジェストファイルと呼ばれます。 CloudTrail 公開鍵と秘密鍵のkey pair 秘密鍵を使用して各ダイジェストファイルに署名します。配信後、公開鍵を使用してダイジェストファイルを検証できます。 CloudTrail AWS リージョンそれぞれに異なるキーペアを使用します。

ダイジェストファイルは、 CloudTrail ログファイルと同じトレイルに関連付けられた Amazon S3 バケットに配信されます。ログファイルがすべてのリージョンまたは複数のアカウントから 1 つの Amazon S3 バケットに配信される場合、 CloudTrail それらのリージョンとアカウントのダイジェストファイルを同じバケットに配信します。

ダイジェストファイルは、ログファイルとは別のフォルダに格納されます。このようにダイジェストファイルとログファイルを分離することで、細かいセキュリティポリシーを適用することができ、既存のログ処理ソリューションを変更せずに引き続き運用することができます。各ダイジェストファイルには、存在する場合、前のダイジェストファイルのデジタル署名も含まれます。現在のダイジェストファイルの署名は、ダイジェストファイル Amazon S3 オブジェクトのメタデータプロパティにあります。ダイジェストファイルの内容の詳細については、「CloudTrail ダイジェストファイル構造」を参照してください。

ログおよびダイジェストファイルの保存

CloudTrail ログファイルとダイジェストファイルは、Amazon S3 または S3 Glacier に安全かつ耐久性があり、かつ低コストで無期限に保存できます。Amazon S3 に保存されているダイジェストファイルのセキュリティを強化するために、Amazon S3 MFA Delete を使用することができます。

検証の有効化とファイルの検証

ログファイルの整合性検証を有効にするには、、、または API を使用できます。 AWS Management Console AWS CLI CloudTrail ログファイルの整合性検証を有効にすると、Amazon S3 バケットにダイジェストログファイルを配信できますが、ファイルの整合性は検証されません。 CloudTrail 詳細については、「のログファイルの整合性検証を有効にする CloudTrail」を参照してください。

CloudTrail ログファイルの整合性を検証するには、 AWS CLI を使用するか、独自のソリューションを作成できます。 AWS CLI は、 CloudTrail 配信された場所にあるファイルを検証します。Amazon S3 または他の場所のいずれかで、別の場所に移動したログを検証する場合、独自の検証ツールを作成することができます。

を使用してログを検証する方法については AWS CLI、を参照してください。 CloudTrail とのログファイルの整合性の検証 AWS CLI CloudTrail ログファイル検証のカスタム実装の開発については、を参照してください。 CloudTrail ログファイルの整合性検証のカスタム実装

のログファイルの整合性検証を有効にする CloudTrail

ログファイルの整合性検証は AWS Management Console、 AWS コマンドラインインターフェイス (AWS CLI)、または CloudTrail API を使用して有効にできます。 CloudTrail 約 1 時間でダイジェストファイルの配信を開始します。

AWS Management Console

CloudTrail コンソールでログファイルの整合性検証を有効にするには、証跡を作成または更新するときに「ログファイルの検証を有効にする」オプションで 「はい」を選択します。新しい証跡では、この機能はデフォルトで有効になります。詳細については、「コンソールで証跡を作成および更新する」を参照してください。

AWS CLI

でログファイルの整合性検証を有効にするには AWS CLI、create-trail コマンドまたは update-trail `--enable-log-file-validation` コマンドでオプションを使用してください。ログファイルの整合性検証を無効にするには、`--no-enable-log-file-validation` オプションを使用します。

例

次の update-trail コマンドは、ログファイルの整合性検証を有効にして、指定された証跡の Amazon S3 バケットへのダイジェストファイルの配信を開始します。

```
aws cloudtrail update-trail --name your-trail-name --enable-log-file-validation
```

CloudTrail API

CloudTrail API によるログファイルの整合性検証を有効にするには、EnableLogFileValidationtrueCreateTrailまたはを呼び出すときにリクエストパラメータをに設定しますUpdateTrail。

詳細については、『AWS CloudTrail API リファレンス』UpdateTrailの「」CreateTrailと「」を参照してください。

CloudTrail とのログファイルの整合性の検証 AWS CLI

でログを検証するには AWS Command Line Interface、 CloudTrail validate-logsコマンドを使用します。このコマンドは、Amazon S3 バケットに配信されたダイジェストファイルを使用して、検証を実行します。ダイジェストファイルの詳細については、「CloudTrail ダイジェストファイル構造」を参照してください。

AWS CLI を使用すると、次の種類の変更を検出できます。

- CloudTrail ログファイルの変更または削除。
- CloudTrail ダイジェストファイルの変更または削除
- 上記の両方の変更または削除

> **Note**
>
> は、 AWS CLI ダイジェストファイルが参照するログファイルのみを検証します。詳細については、「特定のファイルがによって配信されたかどうかの確認 CloudTrail」を参照してください。

前提条件

とのログファイルの整合性を検証するには AWS CLI、次の条件を満たす必要があります。

- へのオンライン接続が必要です AWS。
- ダイジェストファイルとログファイルを含む Amazon S3 バケットへの読み取りアクセスが必要です。
- ダイジェストファイルとログファイルは、 CloudTrail 配信された元の Amazon S3 の場所から移動してはなりません。

> **Note**
>
> ローカルディスクにダウンロードしたログファイルは、 AWS CLIで検証することはできません。検証のために独自のツールを作成する際のガイダンスについては、「CloudTrail ログファイルの整合性検証のカスタム実装」を参照してください。

validate-logs

構文

次に、validate-logs の構文を示します。オプションパラメータは角括弧で示されます。

```
aws cloudtrail validate-logs --trail-arn <trailARN> --start-time <start-time> [--end-time <end-time>] [--s3-bucket <bucket-name>] [--s3-prefix <prefix>] [--account-id <account-id>] [--verbose]
```

> **Note**
>
> validate-logs コマンドはリージョン固有です。 AWS リージョン特定のログを検証するには、--regionグローバルオプションを指定する必要があります。

オプション

validate-logs のコマンドラインオプションは、次のとおりです。--trail-arn と --start-time オプションは必須です。この --account-id オプションは、組織の証跡に追加で必要です。

--start-time

指定された UTC タイムスタンプ値またはその後に配信されるログファイルを検証するように指定します。例えば、2015-01-08T05:21:42Z などです。

`--end-time`

必要に応じて、指定された UTC タイムスタンプ値、またはその前に配信されるログファイルを検証するように指定します。デフォルト値は、現在の UTC 時間 (`Date.now()`) です。例えば、`2015-01-08T12:31:41Z` などです。

> **Note**
>
> 指定された時間範囲では、`validate-logs` コマンドは、対応するダイジェストファイルで参照されるログファイルのみをチェックします。Amazon S3 バケットの他のログファイルは、チェックされません。詳細については、「特定のファイルがによって配信されたかどうかの確認 CloudTrail 」を参照してください。

`--s3-bucket`

必要に応じて、ダイジェストファイルが保存される Amazon S3 バケットを指定します。バケット名が指定されていない場合、 AWS CLI はを呼び出してバケット名を取得しますDescribeTrails()。

`--s3-prefix`

必要に応じて、ダイジェストファイルが保存される Amazon S3 プレフィックスを指定します。指定しない場合、 AWS CLI `DescribeTrails()`はを呼び出して取得します。

> **Note**
>
> 現在のプレフィックスが、指定した時間範囲内で使用されていたプレフィックスと異なる場合にのみ、このオプションを使用してください。

`--account-id`

オプションで、ログを検証するためのアカウントを指定します。このパラメータは、組織内の特定のアカウントのログを検証するための組織証跡に必要です。

`--trail-arn`

検証する証跡の Amazon リソースネーム (ARN) を指定します。証跡の ARN の形式を次に示します。

```
arn:aws:cloudtrail:us-east-2:111111111111:trail/MyTrailName
```

> **Note**
>
> 証跡の証跡 ARN を取得するには、`describe-trails` を実行する前に `validate-logs` コマンドを使用することができます。
> 指定した時間範囲内で複数のバケットにログファイルが配信され、そのバケットのうち 1 つのみのログファイルに検証を限定する場合、証跡の ARN に加えてバケット名とプレフィックスを指定することができます。

`--verbose`

必要に応じて、指定された時間範囲内のすべてのログまたはダイジェストファイルの検証情報を出力します。出力は、ファイルが変更されていないか、変更または削除されたかどうかを示します。非詳細モード (デフォルト) では、検証に失敗した場合にのみ情報が返されます。

例

次の例では、現在の証跡に設定された Amazon S3 バケットを使用し、詳細な出力を指定して、指定された開始時刻から現在までのログファイルを検証します。

```
aws cloudtrail validate-logs --start-time 2015-08-27T00:00:00Z --end-time
 2015-08-28T00:00:00Z --trail-arn arn:aws:cloudtrail:us-east-2:111111111111:trail/my-
trail-name --verbose
```

`validate-logs` の働き

`validate-logs` コマンドは、指定された時間範囲で最新のダイジェストファイルを検証することによって開始します。まず、ダイジェストファイルが属している場所からダウンロードされたことを検証します。つまり、CLI が、S3 の場所 p1 からダイジェストファイル df1 をダウンロードすると、validate-logs は、`p1 == df1.digestS3Bucket + '/' + df1.digestS3Object` を確認します。

ダイジェストファイルの署名が有効である場合、ダイジェストファイルで参照されている各ログのハッシュ値をチェックします。次に、このコマンドは時間内に戻り、前のダイジェストファイルとその参照されたログファイルを連続して検証します。start-time の指定した値まで、またはダイジェストチェーンが終了するまで続きます。ダイジェストファイルが見つからない、または有効でない場合、検証不能な時間範囲が出力が示されます。

検証結果

検証結果は、次の形式の要約ヘッダーで始まります。

```
Validating log files for trail trail_ARN  between time_stamp and time_stamp
```

メイン出力の各行には、1 つのダイジェストまたはログファイルの検証結果が、次の形式で格納されます。

```
<Digest file | Log file> <S3 path> <Validation Message>
```

次の表は、ログファイルとダイジェストファイルの有効な検証メッセージを示しています。

ファイルタイプ	検証メッセージ	説明
Digest file	valid	ダイジェストファイルの署名は、有効です。参照するログファイルをチェックすることができます。このメッセージは詳細モードでのみ表示されます。
Digest file	INVALID: has been moved from its original location	ダイジェストファイルが取得されている S3 バケットまたは S3 オブジェクトは、ダイジェストファイル自体に記録されている S3 バケット または S3 オブジェクトの場所と一致しません。
Digest file	INVALID: invalid format	ダイジェストファイルの形式が無効です。ダイジェストファイルが表す時間範囲に対応するログファイルは検証できません。
Digest file	INVALID: not found	ダイジェストファイルが見つかりませんでした。ダイジェストファイルが表す時間範

ファイルタイプ	検証メッセージ	説明
		囲に対応するログファイルは検証できません。
Digest file	INVALID: public key not found for fingerprint #########	ダイジェストファイルに記録されたフィンガープリントに対応するパブリックキーが見つかりませんでした。ダイジェストファイルが検証できません。
Digest file	INVALID: signature verification failed	ダイジェストファイルの署名が有効ではありません。ダイジェストファイルが有効ではないため、参照するログファイルを検証することはできず、その中の API アクティビティについてアサーションを作成することはできません。
Digest file	INVALID: Unable to load PKCS #1 key with fingerprint #########	指定されたフィンガープリントを持つ PKCS #1 形式の DER でエンコードされたパブリックキーをロードできなかったため、ダイジェストファイルを検証することはできません。
Log file	valid	ログファイルは検証され、配信後に変更されていません。このメッセージは詳細モードでのみ表示されます。
Log file	INVALID: hash value doesn't match	ログファイルのハッシュが一致しません。ログファイルは配信後にによって変更されました CloudTrail。
Log file	INVALID: invalid format	ログファイルの形式が無効です。ログファイルを検証できません。
Log file	INVALID: not found	ログファイルが見つからず、検証できません。

出力には、返された結果に関する要約情報が含まれます。

出力例

詳細

次の例の validate-logs コマンドは、--verbose フラグを使用して、それに続くサンプル出力を作成します。[...] は、サンプル出力を省略したことを示します。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T201728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/09/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T191728Z.json.gz valid
```

```
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T091728Z.json.gz valid
Log file       s3://example-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T081728Z.json.gz valid
Digest file    s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T071728Z.json.gz valid
[...]
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://example-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://example-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2015/08/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150831T221728Z.json.gz valid
```

```
Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

非詳細

次の例 validate-logs コマンドでは、--verbose フラグを使用しません。次の出力例では、1 つのエラーが見つかりました。ヘッダー、エラー、要約情報のみが返されます。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2015-08-31T22:00:00Z --end-
time 2015-09-01T19:17:29Z
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2015-08-31T22:00:00Z and 2015-09-01T19:17:29Z

Digest file s3://example-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2015/09/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150901T101728Z.json.gz INVALID: signature verification failed

Results requested for 2015-08-31T22:00:00Z to 2015-09-01T19:17:29Z
Results found for 2015-08-31T22:17:28Z to 2015-09-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
63/63 log files valid
```

特定のファイルがによって配信されたかどうかの確認 CloudTrail

バケット内の特定のファイルが配信されたかどうかを確認するには CloudTrail、validate-logsそのファイルを含む期間を冗長モードで実行します。ファイルがの出力に表示されている場合validate-logs、そのファイルはによって配信されました。 CloudTrail

CloudTrail ダイジェストファイル構造

各ダイジェストファイルには、過去 1 時間の間に Amazon S3 バケットに送られたログファイルの名前、これらのログファイルのハッシュ値、前のダイジェストファイルのデジタル署名が含まれます。現在のダイジェストファイルの署名は、ダイジェストファイルオブジェクトのメタデータプロパティに格納されます。デジタル署名とハッシュは、ログファイルおよびダイジェストファイル自体の整合性を検証するために使用されます。

ダイジェストファイルの場所

ダイジェストファイルは、次の構文で表される Amazon S3 バケットの場所に送られます。

```
s3://s3-bucket-name/optional-prefix/AWSLogs/aws-account-id/CloudTrail-Digest/
    region/digest-end-year/digest-end-month/digest-end-date/
    aws-account-id_CloudTrail-Digest_region_trail-
name_region_digest_end_timestamp.json.gz
```

> **Note**
>
> 組織の証跡の場合、次のようにバケットの場所に組織ユニット ID も含まれます。
>
> ```
> s3://s3-bucket-name/optional-prefix/AWSLogs/O-ID/aws-account-id/CloudTrail-
> Digest/
>     region/digest-end-year/digest-end-month/digest-end-date/
>     aws-account-id_CloudTrail-Digest_region_trail-
> name_region_digest_end_timestamp.json.gz
> ```

ダイジェストファイルの内容の例

次のダイジェストファイルの例には、 CloudTrail ログに関する情報が含まれています。

```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "S3-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T150131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": "2015-08-17T14:52:27Z",
  "oldestEventTime": "2015-08-17T14:42:27Z",
  "previousDigestS3Bucket": "S3-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/17/111122223333_CloudTrail-Digest_us-east-2_your-trail-name_us-
east-2_20150817T140131Z.json.gz",
```

```
  "previousDigestHashValue":
 "97fb791cf91ffc440d274f8190dbdd9aa09c34432aba82739df18b6d3c13df2d",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "50887ccffad4c002b97caa37cc9dc626e3c680207d41d27fa5835458e066e0d3652fc4dfc30937e4d5f4cc7f796e7
  "logFiles": [
    {
      "s3Bucket": "S3-bucket-name",
      "s3Object": "AWSLogs/111122223333/CloudTrail/us-
east-2/2015/08/17/111122223333_CloudTrail_us-
east-2_20150817T1445Z_9nYN7gp2eWAJHIfT.json.gz",
      "hashValue": "9bb6196fc6b84d6f075a56548feca262bd99ba3c2de41b618e5b6e22c1fc71f6",
      "hashAlgorithm": "SHA-256",
      "newestEventTime": "2015-08-17T14:52:27Z",
      "oldestEventTime": "2015-08-17T14:42:27Z"
    }
  ]
}
```

ダイジェストファイルのフィールドの説明

以下では、ダイジェストファイルの各フィールドについて説明します。

`awsAccountId`

ダイジェストファイルが配信された AWS アカウント ID。

`digestStartTime`

ダイジェストファイルがカバーする開始 UTC 時間範囲。ログファイルが によって配信された時刻をリファレンスとして扱います CloudTrail。つまり、時間範囲が [Ta, Tb] の場合、Ta と Tb の間に顧客に配信されたすべてのログファイルが、ダイジェストに含まれます。

`digestEndTime`

ダイジェストファイルがカバーする終了 UTC 時間範囲。ログファイルが によって配信された時刻をリファレンスとして扱います CloudTrail。つまり、時間範囲が [Ta, Tb] の場合、Ta と Tb の間に顧客に配信されたすべてのログファイルが、ダイジェストに含まれます。

`digestS3Bucket`

現在のダイジェストファイルの配信先であった Amazon S3 バケットの名前です。

`digestS3Object`

現在のダイジェストファイルの Amazon S3 オブジェクトキー (つまり、Amazon S3 バケットの場所) です。文字列の最初の 2 つのリージョンは、ダイジェストファイルの配信元のリージョンを示します。最後のリージョン (`your-trail-name` の後) は、証跡のホームリージョンです。ホームリージョンは、証跡が作成されたリージョンです。マルチリージョンの証跡の場合、このリージョンはダイジェストファイル配信元のリージョンと異なる場合があります。

`newestEventTime`

ダイジェストに含まれるログファイルのすべてのイベントの中で最新のイベントの UTC 時刻です。

`oldestEventTime`

ダイジェストに含まれるログファイルのすべてのイベントの中で最も古いイベントの UTC 時刻です。

> **Note**
>
> ダイジェストファイルが遅れて配信された場合、`oldestEventTime` の値は `digestStartTime` の値より前になります。

`previousDigestS3Bucket`

前のダイジェストファイルの配信先であった Amazon S3 バケットです。

`previousDigestS3Object`

前のダイジェストファイルの Amazon S3 オブジェクトキー (つまり、Amazon S3 バケットの場所) です。

`previousDigestHashValue`

前のダイジェストファイルの圧縮されていない内容の 16 進エンコードされたハッシュ値です。

`previousDigestHashAlgorithm`

前のダイジェストファイルのハッシュ計算に使用されたハッシュアルゴリズムの名前です。

`publicKeyFingerprint`

このダイジェストファイルの署名に使用されたプライベートキーと一致するパブリックキーの 16 進エンコードされたフィンガープリントです。 AWS CLI または CloudTrail API を使用して、ダイジェストファイルに対応する時間範囲のパブリックキーを取得できます。返されたパブリックキーのうち、フィンガープリントがこの値と一致するものを使用して、ダイジェストファイルを検証できます。ダイジェストファイルのパブリックキーの取得については、 コマンドまたは CloudTrail `ListPublicKeys` API を参照してください AWS CLI `list-public-keys`。

> **Note**
>
> CloudTrail は、リージョンごとに異なるプライベート/パブリックキーペアを使用します。各ダイジェストファイルは、リージョンに固有のプライベートキーを使用して署名されます。したがって、特定のリージョンからのダイジェストファイルを検証するときは、同じリージョンで対応するパブリックキーを検索する必要があります。

`digestSignatureAlgorithm`

ダイジェストファイルの署名に使用されるアルゴリズムです。

`logFiles.s3Bucket`

ログファイルの Amazon S3 バケットの名前です。

`logFiles.s3Object`

現在のログファイルの Amazon S3 オブジェクトキーです。

`logFiles.newestEventTime`

ログファイルに含まれる最新のイベントの UTC 時刻です。この時刻は、ログファイル自体のタイムスタンプにも対応しています。

`logFiles.oldestEventTime`

ログファイルに含まれる最も古いイベントの UTC 時刻です。

`logFiles.hashValue`

圧縮されていないログファイルの内容の 16 進エンコードされたハッシュ値です。

`logFiles.hashAlgorithm`

ログファイルのハッシュ計算に使用されたハッシュアルゴリズムです。

開始ダイジェストファイル

ログファイルの整合性の検証が開始されると、開始ダイジェストファイルが生成されます。開始ダイジェストファイルは、ログファイルの整合性の検証が再開されるときにも生成されます (ログファイルの整合性検証をいったん無効にしてから再び有効にすることで、またはログ記録を停止してから検証を有効にしてログ記録を再び開始することで)。開始ダイジェストファイルでは、前のダイジェストファイルに関する以下のフィールドは null になります。

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestHashValue`
- `previousDigestHashAlgorithm`
- `previousDigestSignature`

"空の" ダイジェストファイル

CloudTrail は、ダイジェストファイルが表す 1 時間の間にアカウントに API アクティビティがない場合でも、ダイジェストファイルを配信します。これは、ダイジェストファイルによって報告される 1 時間の間にログファイルが配信されなかったことをアサートする必要がある場合に役に立つことがあります。

次の例では、API アクティビティが発生しなかった 1 時間を記録したダイジェストファイルの内容を示します。ダイジェストファイルの内容の最後にある logFiles:[ ] フィールドが空であることに注意してください。


```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-20T17:01:31Z",
  "digestEndTime": "2015-08-20T18:01:31Z",
  "digestS3Bucket": "example-bucket-name",
  "digestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T180131Z.json.gz",
  "digestPublicKeyFingerprint": "31e8b5433410dfb61a9dc45cc65b22ff",
  "digestSignatureAlgorithm": "SHA256withRSA",
  "newestEventTime": null,
  "oldestEventTime": null,
  "previousDigestS3Bucket": "example-bucket-name",
  "previousDigestS3Object": "AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/20/111122223333_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20150820T170131Z.json.gz",
  "previousDigestHashValue":
 "ed96c4bac9eaa8fe9716ca0e515da51938be651b1db31d781956416a9d05cdfa",
  "previousDigestHashAlgorithm": "SHA-256",
  "previousDigestSignature":
 "82705525fb0fe7f919f9434e5b7138cb41793c776c7414f3520c0242902daa8cc8286b29263d2627f2f259471c745
  "logFiles": []
}
```


ダイジェストファイルの署名

ダイジェストファイルの署名情報は、Amazon S3 ダイジェストファイルオブジェクトの 2 つのオブジェクトメタデータプロパティにあります。各ダイジェストファイルには、次のメタデータエントリが含まれます。

- x-amz-meta-signature

  ダイジェストファイルの署名の 16 進エンコードされた値です。以下に、署名の例を示します。


```
3be472336fa2989ef34de1b3c1bf851f59eb030eaff3e2fb6600a082a23f4c6a82966565b994f9de4a5989d053d9d
28f1cc237f372264a51b611c01da429565def703539f4e71009051769469231bc22232fa260df02740047af53222
05d3ffcb5d2dd5dc28f8bb5b7993938e8a5f912a82b448a367eccb2ec0f198ba71e23eb0b97278cf65f3c8d1e652c
```

- `x-amz-meta-signature-algorithm`

  次に示すのは、ダイジェストの署名を生成するために使用されたアルゴリズムの値の例です。

  `SHA256withRSA`

ダイジェストファイルの連鎖

各ダイジェストファイルに以前のダイジェストファイルへの参照が含まれているため、 などの検証ツールがダイジェストファイルが削除されたかどうかを検出 AWS CLI できる「チェーン」が可能になります。また、指定された時間範囲内のダイジェストファイルを、新しいものから順に連続的に検査することもできます。

> **Note**
>
> ログファイルの整合性検証を無効にすると、1 時間後にダイジェストファイルのチェーンが壊れます。 CloudTrail は、ログファイルの整合性検証が無効になっている期間中に配信されたログファイルのダイジェストファイルを作成しません。たとえば、1 月 1 日の正午にログファイルの整合性検証を有効にし、1 月 2 日の正午にそれを無効にした後、1 月 10 日の正午に再び有効にした場合、1 月 2 日正午から 1 月 10 日正午までの間に配信されたログファイルに対しては、ダイジェストファイルは作成されません。 CloudTrail ログ記録を停止したり、証跡を削除したりするたびに同じことが当てはまります。

証跡の S3 バケットポリシーの設定が間違っていたり、予期しないサービス中断 CloudTrail が発生した場合、ダイジェストファイルの一部または全部が受信されないことがあります。証跡にダイジェスト配信エラーがあるかどうかを確認するには、 `get-trail-status` コマンドを実行し、`LatestDigestDeliveryError`パラメータにエラーがないか確認します。配信の問題が解決されると (バケットポリシーの修正など)、 は欠落しているダイジェストファイルの再配信を試み CloudTrail ます。再配信期間中、ダイジェストファイルが順不同で配信される可能性があるため、チェーンが一時的に壊れているように見える場合があります。

ログ記録が停止するか、証跡が削除された場合、 CloudTrail は最終的なダイジェストファイルを配信します。このダイジェストファイルには、`StopLogging` イベントまでのイベントを対象とする残りのすべてのログファイルに関する情報が含まれている場合があります。

CloudTrail ログファイルの整合性検証のカスタム実装

CloudTrail 業界標準の公開されている暗号化アルゴリズムとハッシュ関数を使用しているため、CloudTrail ログファイルの整合性を検証する独自のツールを作成できます。ログファイルの整合性検証が有効になっている場合、Amazon S3 CloudTrail バケットにダイジェストファイルを配信します。これらのファイルを使用して、独自の検証ソリューションを実装できます。ダイジェストファイルについて詳しくは、「CloudTrail ダイジェストファイル構造」を参照してください。

このトピックでは、ダイジェストファイルの署名方法について説明し、ダイジェストファイルと、ダイジェストファイルによって参照されるログファイルを検証するソリューションの実装に必要な手順を詳しく示します。

CloudTrail ダイジェストファイルの署名方法を理解する

CloudTrail ダイジェストファイルは RSA デジタル署名で署名されています。ダイジェストファイルごとに、 CloudTrail次の処理を行います。

1. 指定されたダイジェストファイルフィールド (次のセクションで説明) に基づいて、データに署名する文字列を作成します。
2. リージョンに固有のプライベートキーを取得します。
3. 文字列の SHA-256 ハッシュとプライベートキーを RSA 署名アルゴリズムに渡すと、そこでデジタル署名が作成されます。
4. 署名のバイトコードを 16 進形式にエンコードします。
5. デジタル署名を Amazon S3 ダイジェストファイルオブジェクトの `x-amz-meta-signature` メタデータプロパティに設定します。

データ署名文字列の内容

CloudTrail データ署名の文字列には以下のオブジェクトが含まれます。

- UTC 拡張形式のダイジェストファイル終了タイムスタンプ (例: `2015-05-08T07:19:37Z`)
- 現在のダイジェストファイルの S3 パス
- 現在のダイジェストファイルの 16 進エンコードされた SHA-256 ハッシュ
- 以前のダイジェストファイルの 16 進エンコードされた署名

この文字列を計算するための形式と文字列の例は、このドキュメントの後半で示します。

カスタム検証を実装する手順

カスタム検証ソリューションを実装するときは、最初にダイジェストファイルを検証してから、その後で、ダイジェストファイルが参照するログファイルを検証する必要があります。

ダイジェストファイルを検証する

ダイジェストファイルを検証するには、署名、対応するプライベートキーが署名に使用されたパブリックキー、計算したデータ署名文字列が必要です。

1. ダイジェストファイルを取得します。
2. 本来の場所からダイジェストファイルが取得されたことを確認します。
3. ダイジェストファイルの 16 進エンコードされた署名を取得します。
4. パブリックキー (対応するプライベートキーがダイジェストファイルの署名に使用された) の 16 進エンコードされたフィンガープリントを取得します。
5. ダイジェストファイルに対応する時間範囲のパブリックキーを取得します。
6. 取得したパブリックキーの中から、フィンガープリントがダイジェストファイルのフィンガープリントと一致するパブリックキーを選択します。
7. ダイジェストファイルのハッシュや他のダイジェストファイルフィールドを使用して、ダイジェストファイル署名の検証に使用されるデータ署名文字列を再作成します。
8. 文字列の SHA-256 ハッシュ、パブリックキー、署名を、パラメータとしてRSA 署名検証アルゴリズムに渡して、署名を検証します。結果が true の場合、ダイジェストファイルは有効です。

ログファイルを検証する

ダイジェストファイルが有効であれば、そのダイジェストファイルが参照するログファイルそれぞれを検証します。

1. ログファイルの整合性を検証するには、未圧縮の内容に対して SHA-256 ハッシュ値を計算し、その結果を、ダイジェストに 16 進数で記録されたログファイルのハッシュと比較します。ハッシュが一致する場合、ログファイルは有効です。
2. 現在のダイジェストファイルに含まれる以前のダイジェストファイルの情報を使用して、以前のダイジェストファイルとそれに対応するログファイルを連続して検証します。

以下のセクションで、これらの手順について詳しく説明します。

A. ダイジェストファイルを取得する

最初の手順では、最新のダイジェストファイルを取得し、それを本来の場所から取得したことを確認し、デジタル署名を確認し、パブリックキーのフィンガープリントを取得します。

1. S3 GetObjectまたは AmazonS3Client クラス (たとえば) を使用して、検証したい時間範囲の最新のダイジェストファイルを Amazon S3 バケットから取得します。
2. ファイルの取得に使用した S3 バケットと S3 オブジェクトが、ダイジェストファイルそのものに記録された S3 バケットと S3 オブジェクトの場所と一致することを確認します。
3. 次に、ダイジェストファイルのデジタル署名を、Amazon S3 のダイジェストファイルオブジェクトの `x-amz-meta-signature` メタデータプロパティから取得します。
4. ダイジェストファイルで、ダイジェストファイルの署名に使用されたプライベートキーに対応するパブリックキーのフィンガープリントを `digestPublicKeyFingerprint` フィールドから取得します。

B. ダイジェストファイルの検証のためにパブリックキーを取得する

パブリックキーを取得してダイジェストファイルを検証するには、または API を使用できます。AWS CLI CloudTrail どちらの場合も、検証しようとするダイジェストファイルの時間範囲 (開始時刻と終了時刻) を指定します。指定した時間範囲について 1 つ以上のパブリックキーが返されることがあります。返されたキーの有効な時間範囲が重複する可能性があります。

> **Note**
>
> CloudTrail リージョンごとに異なる秘密鍵と公開鍵のペアを使用するため、各ダイジェストファイルはそのリージョン固有の秘密鍵で署名されます。したがって、特定のリージョンのダイジェストファイルを検証するときは、同じリージョンからパブリックキーを取得する必要があります。

を使用して公開鍵を取得してください。 AWS CLI

を使用してダイジェストファイルの公開鍵を取得するには AWS CLI、`cloudtrail list-public-keys`コマンドを使用します。このコマンドの形式は次のとおりです。

```
aws cloudtrail list-public-keys [--start-time <start-time>] [--end-time <end-time>]
```

start-time および end-time パラメータには UTC タイムスタンプを使用します。これらはオプションです。指定しない場合、現在の時刻が使用され、現在アクティブなパブリックキー (1 つまたは複数) が返されます。

レスポンス例

レスポンスは、返されるキー (1 つまたは複数) を表す JSON オブジェクトのリストです。


```
{
    "publicKeyList": [
        {
            "ValidityStartTime": "1436317441.0",
            "ValidityEndTime": "1438909441.0",
            "Value": "MIIBCgKCAQEAn11L2YZ9h7onug2ILi1MWyHiMRsTQjfWE
+pHVRLk1QjfWhirG+lpOa8NrwQ/r7Ah5bNL6HepznOU9XTDSfmmnP97mqyc7z/upfZdS/AHhYcGaz7n6Wc/
RRBU6VmiPCrAUojuSk6/GjvA8iOPFsYDuBtviXarvuLPlrT9kAd4Lb+rFfR5peEgBEkhlzc5HuWO7S0y
+KunqxX6jQBnXGMtxmPBPP0FylgWGNdFtks/4YSKcgqwH0YDcawP9GGGDAeCIqPWIXDLG1jOjRRzWfCmD0iJUkz8vTsn4hq
            "Fingerprint": "8eba5db5bea9b640d1c96a77256fe7f2"
        },
        {
            "ValidityStartTime": "1434589460.0",
            "ValidityEndTime": "1437181460.0",
            "Value": "MIIBCgKCAQEApfYL2FiZhpN74LNWVUzhR
+VheYhwhYm8w0n5Gf6i95ylW5kBAWKVEmnAQG7BvS5g9SMqFDQx52fW7NWV44IvfJ2xGXT
+wT+DgR6ZQ+6yxskQNqV5YcXj4Aa5Zz4jJfsYjDuO2MDTZNIzNvBNzaBJ+r2WIWAJ/
Xq54kyF63B6WE38vKuDE7nSd1FqQuEoNBFLPInvgggYe2Ym1Refe2z71wNcJ2kY
+q0h1BSHrSM8RWuJIw7MXwF9iQncg9jYzUlNJomozQzAG5wSRfbplcCYNY40xvGd/aAmO0m+Y
+XFMrKwtLCwseHPvj843qVno6x4BJN9bpWnoPo9sdsbGoiK3QIDAQAB",
            "Fingerprint": "8933b39ddc64d26d8e14ffbf6566fee4"
        },
        {
            "ValidityStartTime": "1434589370.0",
            "ValidityEndTime": "1437181370.0",
            "Value":
 "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqlzPJbvZJ42UdcmLfPUqXYNfOs6I8lCfao/
tOs8CmzPOEdtLWugB9xoIUz78qVHdKIqxbaG4jWHfJBiOSSFBM0lt8cdVo4TnRa7oG9io5pysS6DJhBBAeXsicufsiFJR
+wrUNh8RSLxL4k6G1+BhLX20tJkZ/erT97tDGBujAelqseGg3vPZbTx9SMfOLN65PdLFudLP7Gat0Z9p5jw/
rjpclKfo9Bfc3heeBxWGKwBBOKnFAaN9V57pOaosCvPKmHd9bg7jsQkI9Xp22IzGLsTFJZYVA3KiTAElDMu80iFXPHEq9hK
+1utKVEiLkR2disdCmPTK0VQIDAQAB",
            "Fingerprint": "31e8b5433410dfb61a9dc45cc65b22ff"
        }
    ]
}
```

CloudTrail API を使用してパブリックキーを取得します。

CloudTrail API を使用してダイジェストファイルの公開鍵を取得するには、開始時刻と終了時刻の値を ListPublicKeys API に渡します。この ListPublicKeys API は、指定された時間範囲内の、対応するプライベートキーがダイジェストファイルの署名に使用されたパブリックキーを返します。API は、各パブリックキーに対応するフィンガープリントも返します。

ListPublicKeys

このセクションでは、ListPublicKeys API のリクエストパラメータとレスポンス要素について説明します。

> **Note**
>
> ListPublicKeys のバイナリフィールドのエンコードは変更される可能性があります。

リクエストパラメータ

名前	説明
StartTime	オプションで、 CloudTrail ダイジェストファイルの公開鍵を検索する時間範囲の開始時間を UTC で指定します。 StartTime 指定されていない場合は、現在の時刻が使用され、現在の公開鍵が返されます。 タイプ: DateTime
EndTime	オプションで、 CloudTrail ダイジェストファイルの公開鍵を検索する時間範囲の終了時間を UTC で指定します。指定しない場合は EndTime 、現在の時刻が使用されます。 タイプ: DateTime

レスポンス要素

PublicKeyList は、次の要素を含む PublicKey オブジェクトの配列です。

名前	説明

Value	DER エンコードされたパブリックキー値 (PKCS #1 形式)。 型: Blob
ValidityStartTime	パブリックキーの有効期間の開始時刻。 タイプ: DateTime
ValidityEndTime	パブリックキーの有効期間の終了時刻。 タイプ: DateTime
Fingerprint	パブリックキーのフィンガープリント。フィンガープリントを使用して、ダイジェストファイルの検証に使用する必要があるパブリックキーを特定できます。 型: 文字列

C. 検証に使用するパブリックキーを選択する

list-public-keys または ListPublicKeys によって取得されたパブリックキーの中から、ダイジェストファイルの digestPublicKeyFingerprint フィールドに記録されているフィンガープリントと一致するフィンガープリントのパブリックキーを選択します。これはダイジェストファイルの検証に使用するパブリックキーです。

D. データ署名文字列を再作成する

ダイジェストファイルの署名と、関連付けられたパブリックキーを取得しました。次は、データ署名文字列を計算する必要があります。データ署名文字列の計算が完了すると、署名の検証に必要な入力を得られます。

データ署名文字列は次の形式になります。

```
Data_To_Sign_String =
  Digest_End_Timestamp_in_UTC_Extended_format + '\n' +
  Current_Digest_File_S3_Path + '\n' +
  Hex(Sha256(current-digest-file-content)) + '\n' +
  Previous_digest_signature_in_hex
```

例の Data_To_Sign_String を次に示します。

```
2015-08-12T04:01:31Z
S3-bucket-name/AWSLogs/111122223333/CloudTrail-Digest/us-
east-2/2015/08/12/111122223333_us-east-2_CloudTrail-Digest_us-
east-2_20150812T040131Z.json.gz
4ff08d7c6ecd6eb313257e839645d20363ee3784a2328a7d76b99b53cc9bcacd
6e8540b83c3ac86a0312d971a225361d28ed0af20d70c211a2d405e32abf529a8145c2966e3bb47362383a52441545e
d4c7c09dd152b84e79099ce7a9ec35d2b264eb92eb6e090f1e5ec5d40ec8a0729c02ff57f9e30d5343a8591638f8b79
98b0aee2c1c8af74ec620261529265e83a9834ebef6054979d3e9a6767dfa6fdb4ae153436c567d6ae208f988047ccf
```

この文字列を再作成した後、ダイジェストファイルを検証できます。

E. ダイジェストファイルを検証する

再作成したデータ署名文字列の SHA-256 ハッシュ、デジタル署名、パブリックキーを、RSA 署名検証アルゴリズムに渡します。出力が true の場合、ダイジェストファイルの署名が検証され、ダイジェストファイルは有効です。

F. ログファイルを検証する

ダイジェストファイルの検証が完了したら、ダイジェストファイルが参照するログファイルを検証することができます。ダイジェストファイルにはログファイルの SHA-256 ハッシュが含まれています。ログファイルの 1 CloudTrail つが配信後に変更された場合、SHA-256 ハッシュが変更され、ダイジェストファイルの署名が一致しなくなります。

ログファイルの検証方法を次に示します。

1. ダイジェストファイルの `logFiles.s3Bucket` フィールドと `logFiles.s3Object` フィールドの S3 の場所に関する情報を使用して、ログファイルの `S3 Get` を実行します。
2. `S3 Get` の操作が成功した場合は、ダイジェストファイルの logFiles 配列にリストされている口グファイルに対して次の手順を繰り返します。
   a. ダイジェストファイル内で、対応するログの `logFiles.hashValue` フィールドからファイルの元のハッシュを取得します。
   b. Hash the uncompressed contents of the log file with the hashing algorithm specified in `logFiles.hashAlgorithm` 指定されたハッシュアルゴリズムを使用して、ログファイルの未圧縮の内容をハッシュします。
   c. 生成されたハッシュ値を、ダイジェストファイルのログのハッシュ値と比較します。ハッシュが一致する場合、ログファイルは有効です。

G. その他のダイジェストファイルとログファイルを検証する

各ダイジェストファイルの次のフィールドには、以前のダイジェストファイルの場所と署名が含まれています。

- `previousDigestS3Bucket`
- `previousDigestS3Object`
- `previousDigestSignature`

この情報を使用して、以前のダイジェストファイルに順番にアクセスし、前のセクションの手順に従って、それぞれの署名と参照先のログファイルを検証します。以前のダイジェストファイルの場合に 1 つ異なるのは、ダイジェストファイルオブジェクトの Amazon S3 メタデータプロパティからデジタル署名を取得する必要がないことです。以前のダイジェストファイルの署名は `previousDigestSignature` フィールドにあります。

どちらが先になるとしても、最初のダイジェストファイルに到達するか、ダイジェストファイルのチェーンが途切れるまで、さかのぼることができます。

ダイジェストファイルとログファイルをオフラインで検証する

ダイジェストファイルとログファイルをオフラインで検証するとき、通常は前のセクションで説明した手順に従います。ただし、次のことを考慮に入れる必要があります。

最新のダイジェストファイルの処理

最新 (つまり "現在") のダイジェストファイルのデジタル署名は、ダイジェストファイルオブジェクトの Amazon S3 メタデータプロパティにあります。オフラインのシナリオでは、現在のダイジェストファイルのデジタル署名を取得できません。

これに対処するには次の 2 つの方法があります。

- 前のダイジェストファイルのデジタル署名は現在のダイジェストファイルにあるため、ダイジェストファイルから検証を開始します。 next-to-last この方法では、最新のダイジェストファイルを検証できません。
- 準備の手順として、現在のダイジェストファイルの署名をダイジェストファイルオブジェクトのメタデータプロパティから取得し、オフラインで安全に保存します。このようにすれば、チェーン内の以前のファイルだけでなく現在のダイジェストファイルも検証できるようになります。

パスの解決

s3Object や previousDigestS3Object など、ダウンロードしたダイジェストファイル内のフィールドは、ログファイルとダイジェストファイルについて Amazon S3 のオンライン上の場所を指しています。オフラインソリューションでは、ダウンロードしたログファイルとダイジェストファイルの現在の場所を指すようにこれらを再設定する方法を見つける必要があります。

パブリックキー

オフラインで検証するには、所定の時間範囲のログファイルの検証に必要なすべてのパブリックキーを最初にオンラインで取得し (たとえば、ListPublicKeys を呼び出す)、オフラインで安全に保存する必要があります。指定した最初の時間範囲外の他のファイルを検証するには、常にこの手順を繰り返す必要があります。

検証のサンプルスニペット

次のサンプルスニペットは、ダイジェストファイルとログファイルを検証するためのスケルトンコードを示しています。 CloudTrail このスケルトンコードはオンラインでもオフラインでも使用できます。つまり、実装する際に AWSとのオンライン接続を使用するかどうかはユーザーが決めることができます。推奨の実装では、Java Cryptography Extension (JCE) と Bouncy Castle をセキュリティプロバイダーとして使用しています。

サンプルスニペットには次の内容が含まれます。

- ダイジェストファイルの署名の検証に使用されるデータ署名文字列を作成する方法。
- ダイジェストファイルの署名を確認する方法。
- ログファイルのハッシュを確認する方法。
- ダイジェストファイルのチェーンを検証するためのコード構造。

```
import java.util.Arrays;
import java.security.MessageDigest;
import java.security.KeyFactory;
import java.security.PublicKey;
import java.security.Security;
import java.security.Signature;
import java.security.spec.X509EncodedKeySpec;
import org.json.JSONObject;
import org.bouncycastle.jce.provider.BouncyCastleProvider;
import org.apache.commons.codec.binary.Hex;
```

```
public class DigestFileValidator {

    public void validateDigestFile(String digestS3Bucket, String digestS3Object, String
 digestSignature) {

        // Using the Bouncy Castle provider as a JCE security provider - http://
www.bouncycastle.org/
        Security.addProvider(new BouncyCastleProvider());

        // Load the digest file from S3 (using Amazon S3 Client) or from your local
 copy
        JSONObject digestFile = loadDigestFileInMemory(digestS3Bucket, digestS3Object);

        // Check that the digest file has been retrieved from its original location
        if (!digestFile.getString("digestS3Bucket").equals(digestS3Bucket) ||
                !digestFile.getString("digestS3Object").equals(digestS3Object)) {
            System.err.println("Digest file has been moved from its original
 location.");
        } else {
            // Compute digest file hash
            MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");
            messageDigest.update(convertToByteArray(digestFile));
            byte[] digestFileHash = messageDigest.digest();
            messageDigest.reset();

            // Compute the data to sign
            String dataToSign = String.format("%s%n%s/%s%n%s%n%s",
                                digestFile.getString("digestEndTime"),
                                digestFile.getString("digestS3Bucket"),
digestFile.getString("digestS3Object"), // Constructing the S3 path of the digest file
as part of the data to sign
                                Hex.encodeHexString(digestFileHash),
                                digestFile.getString("previousDigestSignature"));

            byte[] signatureContent = Hex.decodeHex(digestSignature);

            /*
                NOTE:
                To find the right public key to verify the signature, call CloudTrail
 ListPublicKey API to get a list
                of public keys, then match by the publicKeyFingerprint in the digest
 file. Also, the public key bytes
                returned from ListPublicKey API are DER encoded in PKCS#1 format:
```

```
                PublicKeyInfo ::= SEQUENCE {
                    algorithm       AlgorithmIdentifier,
                    PublicKey       BIT STRING
                }

                AlgorithmIdentifier ::= SEQUENCE {
                    algorithm       OBJECT IDENTIFIER,
                    parameters      ANY DEFINED BY algorithm OPTIONAL
                }
            */
            pkcs1PublicKeyBytes =
getPublicKey(digestFile.getString("digestPublicKeyFingerprint")));

            // Transform the PKCS#1 formatted public key to x.509 format.
            RSAPublicKey rsaPublicKey = RSAPublicKey.getInstance(pkcs1PublicKeyBytes);
            AlgorithmIdentifier rsaEncryption = new
AlgorithmIdentifier(PKCSObjectIdentifiers.rsaEncryption, null);
            SubjectPublicKeyInfo publicKeyInfo = new
SubjectPublicKeyInfo(rsaEncryption, rsaPublicKey);

            // Create the PublicKey object needed for the signature validation
            PublicKey publicKey = KeyFactory.getInstance("RSA",
"BC").generatePublic(new X509EncodedKeySpec(publicKeyInfo.getEncoded()));

            // Verify signature
            Signature signature = Signature.getInstance("SHA256withRSA", "BC");
            signature.initVerify(publicKey);
            signature.update(dataToSign.getBytes("UTF-8"));

            if (signature.verify(signatureContent)) {
                System.out.println("Digest file signature is valid, validating log
files…");
                for (int i = 0; i < digestFile.getJSONArray("logFiles").length(); i++)
{

                    JSONObject logFileMetadata =
digestFile.getJSONArray("logFiles").getJSONObject(i);

                    // Compute log file hash
                    byte[] logFileContent = loadUncompressedLogFileInMemory(
                                                logFileMetadata.getString("s3Bucket"),
                                                logFileMetadata.getString("s3Object")
                                            );
```

```
                    messageDigest.update(logFileContent);
                     byte[] logFileHash = messageDigest.digest();
                    messageDigest.reset();

                    // Retrieve expected hash for the log file being processed
                    byte[] expectedHash =
 Hex.decodeHex(logFileMetadata.getString("hashValue"));

                    boolean signaturesMatch = Arrays.equals(expectedHash, logFileHash);
                    if (!signaturesMatch) {
                        System.err.println(String.format("Log file: %s/%s hash doesn't
 match.\tExpected: %s Actual: %s",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object"),
                                Hex.encodeHexString(expectedHash),
 Hex.encodeHexString(logFileHash)));
                    } else {
                        System.out.println(String.format("Log file: %s/%s hash match",
                                logFileMetadata.getString("s3Bucket"),
 logFileMetadata.getString("s3Object")));
                    }
                }

            } else {
                System.err.println("Digest signature failed validation.");
            }

            System.out.println("Digest file validation completed.");

            if (chainValidationIsEnabled()) {
                // This enables the digests' chain validation
                validateDigestFile(
                        digestFile.getString("previousDigestS3Bucket"),
                        digestFile.getString("previousDigestS3Object"),
                        digestFile.getString("previousDigestSignature"));
            }
        }
    }
}
```

CloudTrail ログファイルの例

CloudTrail アカウントのイベントを監視します。証跡を作成した場合、証跡によりそれらのイベントがログファイルとして Amazon S3 バケットに配信されます。 CloudTrail Lake にイベントデータストアを作成すると、イベントはイベントデータストアに記録されます。イベントデータストアは S3 バケットを使用しません。

トピック

CloudTrail ログファイル名の形式

CloudTrail Amazon S3 バケットに配信されるログファイルオブジェクトには、次のファイル名形式を使用します。

```
AccountID_CloudTrail_RegionName_YYYYMMDDTHHmmZ_UniqueString.FileNameFormat
```

- YYYY、MM、DD、HH、および mm は、ログファイルが配信された時の年、月、日、時、分を表す数字です。時間は 24 時間形式です。Z は時間が UTC であることを示します。

> **Note**
>
> ある時点で配信されたログファイルには、その時点より前に書き込まれたレコードが含まれます。

- ログファイル名の 16 文字の UniqueString コンポーネントは、ファイルの上書きを防止するためのものです。意味はないため、ログ処理ソフトウェアでは無視されます。
- FileNameFormat はファイルのエンコードです。現在のところ、これは json.gz で、圧縮された gzip 形式の JSON テキストファイルです。

例: CloudTrail ログファイル名

```
111122223333_CloudTrail_us-east-2_20150801T0210Z_Mu0KsOhtH1ar15ZZ.json.gz
```

ログファイルの例

ログファイルには、1 つ以上のレコードが含まれます。次の例では、ログファイルの作成を開始したアクションのレコードを示すログのスニペットです。

CloudTrail イベントレコードフィールドの詳細については、を参照してくださいCloudTrail レコードの内容。

目次

Amazon EC2 ログの例

Amazon Elastic Compute Cloud (Amazon EC2) は、 AWS クラウドでサイズ変更可能なコンピューティングキャパシティーを提供します。仮想サーバーを起動し、セキュリティおよびネットワーキングを構成し、ストレージを管理できます。Amazon EC2 により、要件変更や需要増に対応して迅速に拡張または縮小できるため、サーバートラフィック予測が不要になります。詳細については、「Linux インスタンス用Amazon EC2 ユーザーガイド」を参照してください。

次の例では、Mateo という名前の IAM ユーザーが aws ec2 start-instances コマンドを実行し、インスタンス i-EXAMPLE56126103cb とi-EXAMPLEaff4840c22 に関する Amazon EC2 の StartInstances アクションを呼び出しています。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::123456789012:user/Mateo",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mateo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:17:28Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.start-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        }
    },
    "responseElements": {
        "requestId": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                },
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 0,
                        "name": "pending"
```

```
                    },
                    "previousState": {
                        "code": 80,
                        "name": "stopped"
                    }
                }
            ]
        }
    },
    "requestID": "e4336db0-149f-4a6b-844d-EXAMPLEb9d16",
    "eventID": "e755e09c-42f9-4c5c-9064-EXAMPLE228c7",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


次の例では、Nikki という名前の IAM ユーザーが aws ec2 stop-instances コマンドを実行し、Amazon EC2 の StopInstances アクションを呼び出し、2 つのインスタンスを停止しています。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EXAMPLE6E4XEGITWATV6R",
        "arn": "arn:aws:iam::777788889999:user/Nikki",
        "accountId": "777788889999",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Nikki",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-07-19T21:14:20Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.stop-instances",
    "requestParameters": {
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb"
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22"
                }
            ]
        },
        "force": false
    },
    "responseElements": {
        "requestId": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
        "instancesSet": {
            "items": [
                {
                    "instanceId": "i-EXAMPLE56126103cb",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                },
                {
                    "instanceId": "i-EXAMPLEaff4840c22",
                    "currentState": {
                        "code": 64,
                        "name": "stopping"
                    },
```

```
                    "previousState": {
                        "code": 16,
                        "name": "running"
                    }
                }
            ]
        }
    },
    "requestID": "c308a950-e43e-444e-afc1-EXAMPLE73e49",
    "eventID": "9357a8cc-a0eb-46a1-b67e-EXAMPLE19b14",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777788889999",
    "eventCategory": "Management",
     "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

次の例では、Arnav という名前の IAM ユーザーが aws ec2 create-key-pair コマンドを実行して CreateKeyPair アクションを呼び出したことを示します。responseElementsにはキーペアのハッシュが含まれており、 AWS キーマテリアルが削除されていることに注意してください。

```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Arnav",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "Arnav",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-07-19T21:19:22Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateKeyPair",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/ec2.create-key-pair",
    "requestParameters": {
        "keyName": "my-key",
        "keyType": "rsa",
        "keyFormat": "pem"
    },
    "responseElements": {
        "requestId": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
        "keyName": "my-key",
        "keyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "keyPairId": "key-abcd12345eEXAMPLE",
        "keyMaterial": "<sensitiveDataRemoved>"
    },
    "requestID": "9aa4938f-720f-4f4b-9637-EXAMPLE9a196",
    "eventID": "2ae450ff-e72b-4de1-87b0-EXAMPLE5227cb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "444455556666",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


IAM ログの例

AWS Identity and Access Management (IAM) は、 AWS リソースへのアクセスを安全に制御するのに役立つウェブサービスです。IAM を使用すると、ユーザーがアクセスできる AWS のリソースを制御するアクセス許可を集中管理できます。IAM を使用して、誰を認証 (サインイン) し、誰にリソー

スの使用を認可する (アクセス許可を付与する) かを制御します。詳細については、IAM ユーザーガイドを参照してください。

次の例では、Mary という名前の IAM ユーザーが aws iam create-user コマンドを実行し、CreateUser アクションを呼び出し、Richard という新規ユーザーを作成しています。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::888888888888:user/Mary",
        "accountId": "888888888888",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Mary",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-user",
    "requestParameters": {
        "userName": "Richard"
    },
    "responseElements": {
        "user": {
            "path": "/",
            "arn": "arn:aws:iam::888888888888:user/Richard",
            "userId": "AIDA6ON6E4XEP7EXAMPLE",
            "createDate": "Jul 19, 2023 9:25:09 PM",
            "userName": "Richard"
        }
    },
```

```
    "requestID": "2d528c76-329e-410b-9516-EXAMPLE565dc",
    "eventID": "ba0801a1-87ec-4d26-be87-EXAMPLE75bbb",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "888888888888",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


次の例では、Paulo という名前の IAM ユーザーが aws iam add-user-to-group コマンドを実行し、AddUserToGroup アクションを呼び出し、Jane というユーザーを Admin グループに追加しています。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::555555555555:user/Paulo",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Paulo",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:25:09Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "AddUserToGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.add-user-to-group",
    "requestParameters": {
        "groupName": "Admin",
        "userName": "Jane"
    },
    "responseElements": null,
    "requestID": "ecd94349-b36f-44bf-b6f5-EXAMPLE9c463",
    "eventID": "2939ba50-1d26-4a5a-83bd-EXAMPLE85850",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```


次の例では、Saanvi という名前の IAM ユーザーが aws iam create-role コマンドを実行し、CreateRole アクションを呼び出し、ロールを作成しています。


```
{"Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGITEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/Saanvi",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Saanvi",
        "sessionContext": {
            "sessionIssuer": {},
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2023-07-19T21:29:12Z",
    "eventSource": "iam.amazonaws.com",
    "eventName": "CreateRole",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.5 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/iam.create-role",
    "requestParameters": {
        "roleName": "TestRole",
        "description": "Allows EC2 instances to call AWS services on your behalf.",
        "assumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Action\":[\"sts:AssumeRole\"],\"Principal\":{\"Service\":
[\"ec2.amazonaws.com\"]}}]}"
    },
    "responseElements": {
        "role": {
            "assumeRolePolicyDocument": "%7B%22Version%22%3A%222012-10-17%22%2C
%22Statement%22%3A%5B%7B%22Effect%22%3A%22Allow%22%2C%22Action%22%3A%5B%22sts
%3AAssumeRole%22%5D%2C%22Principal%22%3A%7B%22Service%22%3A%5B%22ec2.amazonaws.com
%22%5D%7D%7D%5D%7D",
            "arn": "arn:aws:iam::777777777777:role/TestRole",
            "roleId": "AROA6ON6E4XEFFEXAMPLE",
            "createDate": "Jul 19, 2023 9:29:12 PM",
            "roleName": "TestRole",
            "path": "/"
        }
    },
    "requestID": "ff38f36e-ebd3-425b-9939-EXAMPLE1bbe",
    "eventID": "9da77cd0-493f-4c89-8852-EXAMPLEa887c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "777777777777",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "iam.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

エラーコードとメッセージログの例

次の例では、Terry という名前の IAM ユーザーが aws cloudtrail update-trail コマンドを実行し、UpdateTrail アクションを呼び出し、myTrail2 という名前の証跡を更新しましたが、その証跡名が見つかりませんでした。ログには、このエラーが errorCode および errorMessage 要素で表示されます。

```
{"Records": [{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDA6ON6E4XEGIEXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Terry",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Terry",
        "sessionContext": {
            "attributes": {
                "creationDate": "2023-07-19T21:11:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-07-19T21:35:03Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "UpdateTrail",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.13.0 Python/3.11.4 Linux/4.14.255-314-253.539.amzn2.x86_64
 exec-env/CloudShell exe/x86_64.amzn.2 prompt/off command/cloudtrail.update-trail",
    "errorCode": "TrailNotFoundException",
    "errorMessage": "Unknown trail: arn:aws:cloudtrail:us-east-1:111122223333:trail/
myTrail2 for the user: 111122223333",
    "requestParameters": {
        "name": "myTrail2",
        "isMultiRegionTrail": true
    },
    "responseElements": null,
    "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
    "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}]}
```

CloudTrail Insights イベントログの例

次の例は、 CloudTrail Insights イベントログを示しています。Insights イベントは、異常な書き込み管理 API アクティビティまたはエラー応答アクティビティの期間の開始と終了を示すイベントのペアです。`state` フィールドには、異常なアクティビティの開始時と終了時にイベントが記録されたかどうかが表示されます。イベント名は`UpdateInstanceInformation`、 CloudTrail 管理イベントを分析して異常なアクティビティが発生したと判断した AWS Systems Manager API と同じ名前です。開始イベントと終了イベントには一意の `eventID` 値がありますが、ペアによって使用される `sharedEventID` 値もあります。Insights イベントには `baseline` (アクティビティの通常のパターン)、`insight` (開始 Insights イベントをトリガーした異常なアクティビティの平均) が表示され、終了イベントには Insights イベントの期間における異常なアクティビティの平均である `insight` 値が表示されます。 CloudTrail Insights の詳細については、を参照してくださいInsights イベントのログ記録。

```
{
    "Records": [{
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T02:51:00Z",
        "awsRegion": "us-east-1",
        "eventID": "654a30ff-b0f3-4527-81b6-EXAMPLEf2393",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "bcbfc274-8559-4a56-beb0-EXAMPLEa6c34",
        "insightDetails": {
            "state": "Start",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
```

```
                        "average": 84.410596421
                    },
                    "insight": {
                        "average": 669
                    }
                }
            }
        },
        "eventCategory": "Insight"
    },
    {
        "eventVersion": "1.08",
        "eventTime": "2023-01-02T00:22:00Z",
        "awsRegion": "us-east-1",
        "eventID": "258de2fb-e2a9-4fb5-aeb2-EXAMPLE449a4",
        "eventType": "AwsCloudTrailInsight",
        "recipientAccountId": "123456789012",
        "sharedEventID": "8b74a7bc-d5d3-4d19-9d60-EXAMPLE08b51",
        "insightDetails": {
            "state": "End",
            "eventSource": "ssm.amazonaws.com",
            "eventName": "UpdateInstanceInformation",
            "insightType": "ApiCallRateInsight",
            "insightContext": {
                "statistics": {
                    "baseline": {
                        "average": 74.156423842
                    },
                    "insight": {
                        "average": 657
                    },
                    "insightDuration": 1
                }
            }
        },
        "eventCategory": "Insight"
    }]
}
```

CloudTrail 処理ライブラリを使用する

CloudTrail 処理ライブラリは、 AWS CloudTrail ログを簡単に処理できる Java ライブラリです。CloudTrail SQS キューに関する設定の詳細を指定し、イベントを処理するコードを記述します。

CloudTrail 残りは処理ライブラリが行います。Amazon SQS キューのポーリング、キューメッセージの読み取りと解析、 CloudTrail ログファイルのダウンロード、ログファイル内のイベントの解析、イベントを Java オブジェクトとしてコードに渡します。

CloudTrail 処理ライブラリは拡張性が高く、耐障害性があります。ログファイルの並列処理を行うため、必要な数だけのログを処理することができます。ネットワークタイムアウトや、アクセスできないリソースに関するネットワーク障害に対応します。

次のトピックでは、 CloudTrail 処理ライブラリを使用して Java CloudTrail プロジェクトのログを処理する方法を示します。

このライブラリは Apache ライセンスのオープンソースプロジェクトとして提供されており、以下で利用できます。 GitHub https://github.com/aws/aws-cloudtrail-processing-libraryライブラリソースには、独自のプロジェクトのベースとして使用できるサンプルコードが含まれます。

トピック

最小要件

CloudTrail 処理ライブラリを使用するには、以下のものが必要です。

- AWS SDK for Java 1.11.830
- Java 1.8 (Java SE 8)

処理ログ CloudTrail

Java CloudTrail アプリケーションのログを処理するには:

1. CloudTrail 処理ライブラリをプロジェクトに追加する。
2. CloudTrail 処理ライブラリの設定
3. イベントプロセッサを実装する
4. 処理エグゼキューターをインスタンス化して実行する

CloudTrail 処理ライブラリをプロジェクトに追加する。

CloudTrail 処理ライブラリを使用するには、Java プロジェクトのクラスパスに追加します。

目次

Apache Ant プロジェクトにライブラリを追加する

CloudTrail 処理ライブラリを Apache Ant プロジェクトに追加するには

1. CloudTrail GitHub処理ライブラリのソースコードを以下からダウンロードまたは複製します。
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 「README」で説明されているように、ソースから .jar ファイルを構築します。

```
mvn clean install -Dgpg.skip=true
```

3. 作成された .jar ファイルをプロジェクトにコピーし、プロジェクトの `build.xml` ファイルに追加します。以下はその例です。

```
<classpath>
  <pathelement path="${classpath}"/>
  <pathelement location="lib/aws-cloudtrail-processing-library-1.6.1.jar"/>
</classpath>
```

Apache Maven プロジェクトにライブラリを追加する

CloudTrail プロセッシングライブラリは Apache Maven で利用可能です。プロジェクトの `pom.xml` ファイルに依存関係を 1 つ書くことで、プロジェクトに追加できます。

CloudTrail 処理ライブラリーを Maven プロジェクトに追加するには:

- Maven プロジェクトの `pom.xml` ファイルを開き、次の依存関係を追加します。

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-cloudtrail-processing-library</artifactId>
    <version>1.6.1</version>
</dependency>
```

Eclipse プロジェクトにライブラリを追加する

CloudTrail 処理ライブラリーを Eclipse プロジェクトに追加するには:

1. CloudTrail 処理ライブラリーのソースコードを以下からダウンロードまたは複製します。 GitHub
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 「README」で説明されているように、ソースから .jar ファイルを構築します。

```
mvn clean install -Dgpg.skip=true
```

3. ビルドした aws-cloudtrail-processing-library -1.6.1.jar をプロジェクト内のディレクトリ (通常は) にコピーします。`lib`
4. Eclipse の [Project Explorer] でプロジェクト名を右クリックし、[Build Path]、[Configure] の順に選択します。
5. [Java Build Path] ウィンドウで、[Libraries] タブを選択します。
6. 「JAR を追加...」を選択します。 aws-cloudtrail-processing-library-1.6.1.jar をコピーしたパスに移動します。
7. [OK] を選択すると、プロジェクトに `.jar` が追加されます。

IntelliJ プロジェクトにライブラリを追加する

CloudTrail 処理ライブラリを IntelliJ プロジェクトに追加するには

1. CloudTrail GitHub処理ライブラリのソースコードを以下からダウンロードまたは複製します。
   - https://github.com/aws/ aws-cloudtrail-processing-library
2. 「README」で説明されているように、ソースから .jar ファイルを構築します。

```
mvn clean install -Dgpg.skip=true
```

3. [File] で、[Project Structure] を選択します。
4. [Modules]、[Dependencies] の順に選択します。
5. [+ JARS or Directories] を選択し、構築した `aws-cloudtrail-processing-library-1.6.1.jar` のパスに移動します。
6. [Apply]、[OK] の順に選択すると、プロジェクトに `.jar` が追加されます。

CloudTrail 処理ライブラリの設定

CloudTrail 処理ライブラリは、実行時にロードされるクラスパスプロパティファイルを作成するか、`ClientConfiguration`オブジェクトを作成してオプションを手動で設定することで設定できます。

プロパティファイルを提供する

アプリケーションに設定オプションを提供するクラスパスプロパティファイルを作成できます。次のサンプルファイルでは、設定できるオプションを示します。

```
# AWS access key. (Required)
accessKey = your_access_key

# AWS secret key. (Required)
secretKey = your_secret_key

# The SQS URL used to pull CloudTrail notification from. (Required)
sqsUrl = your_sqs_queue_url

# The SQS end point specific to a region.
sqsRegion = us-east-1

# A period of time during which Amazon SQS prevents other consuming components
# from receiving and processing that message.
visibilityTimeout = 60

# The S3 region to use.
s3Region = us-east-1

# Number of threads used to download S3 files in parallel. Callbacks can be
# invoked from any thread.
```

```
threadCount = 1

# The time allowed, in seconds, for threads to shut down after
# AWSCloudTrailEventProcessingExecutor.stop() is called. If they are still
# running beyond this time, they will be forcibly terminated.
threadTerminationDelaySeconds = 60

# The maximum number of AWSCloudTrailClientEvents sent to a single invocation
# of processEvents().
maxEventsPerEmit = 10

# Whether to include raw event information in CloudTrailDeliveryInfo.
enableRawEventInfo = false

# Whether to delete SQS message when the CloudTrail Processing Library is unable to
 process the notification.
deleteMessageUponFailure = false
```

以下のパラメータは必須です。

- sqsUrl— 通知を取得する URL を指定します。 CloudTrailこの値を指定しない場合、AWSCloudTrailProcessingExecutor が IllegalStateException をスローします。
- accessKey – アカウントの一意の識別子 (AKIAIOSFODNN7EXAMPLE など)。
- secretKey— bPxRfi wJalrXUtnFEMI l/K7MDeng/ CYEXAMPLEKEY など、アカウント固有の識別子。

accessKeyおよびパラメータはライブラリへの認証情報を提供し、ライブラリがユーザーに代わってアクセスできるようにします。secretKey AWS AWS

他のパラメータのデフォルト値は、ライブラリによって設定されます。詳細については、「AWS CloudTrail Processing Library リファレンス」を参照してください。

の作成 ClientConfiguration

クラスパスプロパティでオプションを設定する代わりに、次の例のように、ClientConfiguration オブジェクトでオプションを初期化して設定することにより、AWSCloudTrailProcessingExecutor にオプションを提供できます。

```
ClientConfiguration basicConfig = new ClientConfiguration(
    "http://sqs.us-east-1.amazonaws.com/123456789012/queue2",
```

```
    new DefaultAWSCredentialsProviderChain());

basicConfig.setEnableRawEventInfo(true);
basicConfig.setThreadCount(4);
basicConfig.setnEventsPerEmit(20);
```

イベントプロセッサを実装する

CloudTrail ログを処理するには、EventsProcessor CloudTrail ログデータを受信するを実装する必要があります。以下に実装例を示します。

```
public class SampleEventsProcessor implements EventsProcessor {

    public void process(List<CloudTrailEvent> events) {
        int i = 0;
        for (CloudTrailEvent event : events) {
            System.out.println(String.format("Process event %d : %s", i++,
 event.getEventData()));
        }
    }
}
```

を実装するときはEventsProcessor、process()AWSCloudTrailProcessingExecutor CloudTrail がイベントの送信に使用するコールバックを実装します。イベントは、CloudTrailClientEvent オブジェクトのリストで提供されます。

CloudTrailClientEventこのオブジェクトには、CloudTrailEventCloudTrailEventMetadata CloudTrail イベントや配信情報の読み取りに使用できるバンドが用意されています。

この簡単な例では、SampleEventsProcessor に渡された各イベントのイベント情報が表示されます。実際の実装では、必要に応じてログを処理できます。AWSCloudTrailProcessingExecutor は、送信するイベントがあり、実行している限りは、EventsProcessor へのイベントの送信を続けます。

処理工グゼキューターをインスタンス化して実行する

CloudTrail Processing Library の設定値を (ClientConfigurationプロパティーファイルまたはクラスを使用して) EventsProcessor 記述して設定すると、これらの要素を使用してを初期化し、使用できます。AWSCloudTrailProcessingExecutor

AWSCloudTrailProcessingExecutor CloudTrail イベントの処理に使用するには:

1. AWSCloudTrailProcessingExecutor.Builder オブジェクトをインスタンス化します。Builder のコンストラクタは、EventsProcessor オブジェクトとクラスパスのプロパティファイル名を受け取ります。
2. Builder の build() ファクトリメソッドを呼び出し、AWSCloudTrailProcessingExecutor オブジェクトを設定して取得します。
3. start()stop()とメソッドを使用して、 CloudTrail イベント処理を開始および終了します。AWSCloudTrailProcessingExecutor

```
public class SampleApp {
  public static void main(String[] args) throws InterruptedException {
    AWSCloudTrailProcessingExecutor executor = new
      AWSCloudTrailProcessingExecutor.Builder(new SampleEventsProcessor(),
        "/myproject/cloudtrailprocessing.properties").build();

    executor.start();
    Thread.sleep(24 * 60 * 60 * 1000); // let it run for a while (optional)
    executor.stop(); // optional
  }
}
```

高度なトピック

トピック

- 処理するイベントのフィルタリング
- データイベントの処理
- 進行状況のレポート
- エラー処理

処理するイベントのフィルタリング

デフォルトでは、Amazon SQS キューの S3 バケット内のすべての口グと、それに含まれるすべてのイベントが、EventsProcessor に送信されます。 CloudTrail Processing Library には、CloudTrail ログの取得に使用するソースをフィルタリングしたり、処理したいイベントをフィルタリングしたりするためのオプションインターフェースが用意されています。

SourceFilter

SourceFilter インターフェイスを実装して、提供されたソースからの口グを処理するかどうかを選択できます。SourceFilter で 1 つだけ宣言されているコールバックメソッド filterSource() は、CloudTrailSource オブジェクトを受け取ります。ソースからのイベントが処理されないようにするには、filterSource() から false を返します。

CloudTrail 処理ライブラリは、ライブラリが Amazon SQS filterSource() キューの口グをポーリングした後にメソッドを呼び出します。これは、ライブラリがイベントのフィルタリングまたは口グの処理を開始する前に発生します。

以下に実装例を示します。

```
public class SampleSourceFilter implements SourceFilter{
  private static final int MAX_RECEIVED_COUNT = 3;

  private static List<String> accountIDs ;
  static {
    accountIDs = new ArrayList<>();
    accountIDs.add("123456789012");
    accountIDs.add("234567890123");
  }

  @Override
  public boolean filterSource(CloudTrailSource source) throws CallbackException {
    source = (SQSBasedSource) source;
    Map<String, String> sourceAttributes = source.getSourceAttributes();

    String accountId = sourceAttributes.get(
      SourceAttributeKeys.ACCOUNT_ID.getAttributeKey());

    String receivedCount = sourceAttributes.get(
      SourceAttributeKeys.APPROXIMATE_RECEIVE_COUNT.getAttributeKey());

    int approximateReceivedCount = Integer.parseInt(receivedCount);

    return approximateReceivedCount <= MAX_RECEIVED_COUNT &&
 accountIDs.contains(accountId);
  }
}
```

独自の SourceFilter を提供しない場合に使用される DefaultSourceFilter では、すべてのソースの処理が許可されます (常に true を返します)。

EventFilter

EventFilterインターフェイスを実装して、 CloudTrailイベントをに送信するかどうかを選択できます。EventsProcessor EventFilterオブジェクトを受け取るコールバックメソッドを 1 つ宣言します。filterEvent( ) CloudTrailEventイベントが処理されないようにするには、filterEvent( ) から false を返します。

CloudTrail 処理ライブラリは、ライブラリが Amazon SQS キューのログをポーリングした後、filterEvent( )およびソースフィルタリング後にメソッドを呼び出します。これは、ライブラリがログのイベント処理を開始する前に発生します。

次の実装例を参照してください。

```
public class SampleEventFilter implements EventFilter{

  private static final String EC2_EVENTS = "ec2.amazonaws.com";

  @Override
  public boolean filterEvent(CloudTrailClientEvent clientEvent) throws
 CallbackException {
    CloudTrailEvent event = clientEvent.getEvent();

    String eventSource = event.getEventSource();
    String eventName = event.getEventName();

    return eventSource.equals(EC2_EVENTS) && eventName.startsWith("Delete");
  }
}
```

独自の EventFilter を提供しない場合に使用される DefaultEventFilter では、すべてのイベントの処理が許可されます (常に true を返します)。

データイベントの処理

CloudTrail データイベントを処理すると、整数 (int) でも A float (10 進数を含む数値) でも、数値が元の形式で保持されます。データイベントのフィールドに整数が含まれるイベントでは、CloudTrail これまではこれらの数値を浮動小数点数として処理していました。現在、 CloudTrail これらのフィールドの数値は元の形式を維持したまま処理されます。

ベストプラクティスとして、オートメーションが壊れないように、 CloudTrail データイベントの処理やフィルターに使用するコードやオートメーションには柔軟に対応し、intfloat両方の数値とフォーマット済みの数値を許可するようにしてください。最良の結果を得るには、処理ライブラリのバージョン 1.4.0 以降を使用してください。 CloudTrail

次のス二ペット例ではデータイベントの ResponseParameters ブロックの desiredCount パラメータ用にフォーマットされた float の数値、2.0 を示しています。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2.0
...
```

次のス二ペット例ではデータイベントの ResponseParameters ブロックの desiredCount パラメータ用にフォーマットされた int の数値、2 を示しています。

```
"eventName": "CreateService",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "000.00.00.00",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clientToken": "EXAMPLE",
        "cluster": "default",
        "desiredCount": 2
...
```

進行状況のレポート

ProgressReporter CloudTrail 処理ライブラリの進行状況のレポートをカスタマイズするインターフェースを実装してください。 ProgressReporterreportStart()と 2 つのメソッドを宣言します。これらのメソッドはreportEnd()、以下の操作の開始時と終了時に呼び出されます。

- Amazon SQS からのメッセージのポーリング
- Amazon SQS からのメッセージの解析
- Amazon SQS CloudTrail ソースのログの処理

- Amazon SQS からのメッセージの削除
- CloudTrail ログファイルのダウンロード
- CloudTrail ログファイルの処理

どちらの方法でも、実行されたオペレーションに関する情報が含まれる ProgressStatus オブジェクトを受信します。progressState メンバーは ProgressState 列挙のメンバーを保持し、それによって現在のオペレーションが識別されます。このメンバーには、progressInfo メンバーの追加情報を含めることができます。さらに、reportStart() から返す任意のオブジェクトが reportEnd() に渡されるので、イベントが処理を開始した時刻などのコンテキスト情報を提供できます。

次に示す実装の例では、操作が完了するまでにかかった時間についての情報を提供しています。

```
public class SampleProgressReporter implements ProgressReporter {
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public Object reportStart(ProgressStatus status) {
    return new Date();
  }

  @Override
  public void reportEnd(ProgressStatus status, Object startDate) {
    System.out.println(status.getProgressState().toString() + " is " +
      status.getProgressInfo().isSuccess() + " , and latency is " +
      Math.abs(((Date) startDate).getTime()-new Date().getTime()) + "
      milliseconds.");
  }
}
```

独自の ProgressReporter を実装しない場合に使用される DefaultExceptionHandler では、実行されている状態の名前が表示されます。

エラー処理

ExceptionHandler インターフェイスを使用すると、ログ処理中に例外が発生したときに特別な処理を提供できます。ExceptionHandler で 1 つだけ宣言されている handleException() メソッドは、発生した例外についてのコンテキストを含む ProcessingLibraryException オブジェクトを受け取ります。

渡された ProcessingLibraryException の getStatus() メソッドを使用して、例外発生時に実行された操作を明らかにし、操作のステータスに関する追加情報を取得できます。ProcessingLibraryException は Java の標準的な Exception クラスから派生しているので、いずれかの Exception メソッドを呼び出して例外に関する情報を取得することもできます。

次の実装例を参照してください。

```
public class SampleExceptionHandler implements ExceptionHandler{
  private static final Log logger =
    LogFactory.getLog(DefaultProgressReporter.class);

  @Override
  public void handleException(ProcessingLibraryException exception) {
    ProgressStatus status = exception.getStatus();
    ProgressState state = status.getProgressState();
    ProgressInfo info = status.getProgressInfo();

    System.err.println(String.format(
      "Exception. Progress State: %s. Progress Information: %s.", state, info));
  }
}
```

独自の ExceptionHandler を提供しない場合に使用される DefaultExceptionHandler は、標準エラーメッセージを表示します。

> **Note**
>
> deleteMessageUponFailureパラメータがの場合true、 CloudTrail 処理ライブラリは一般的な例外を処理エラーと区別しないため、キューメッセージを削除する可能性があります。
>
> 1. 例えば、SourceFilter を使用して、タイムスタンプでメッセージをフィルタリングします。
> 2. ただし、 CloudTrail ログファイルを受け取る S3 バケットにアクセスするのに必要な権限がありません。必要なアクセス権限がないため、AmazonServiceException がスローされます。 CloudTrail 処理ライブラリはこれをにまとめます。CallBackException
> 3. DefaultExceptionHandler はこれを口グとして記録しますが、必要なアクセス権限がないという根本原因を特定することはありません。 CloudTrail 処理ライブラリはこれ

を処理エラーと見なし、 CloudTrail メッセージに有効なログファイルが含まれていてもメッセージを削除します。

メッセージを `SourceFilter` でフィルタリングするには、`ExceptionHandler` がサービスの例外を処理エラーから区別できることを確認します。

追加リソース

CloudTrail 処理ライブラリについて詳しくは、以下を参照してください。

- CloudTrail GitHub CloudTrail 処理ライブラリアプリケーションの実装方法を示すサンプルコードを含む処理ライブラリープロジェクト。
- CloudTrail 処理ライブラリ Java Package ドキュメント。

のセキュリティ AWS CloudTrail

AWS クラウドセキュリティは最優先事項です。 AWS 顧客は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

AWS セキュリティはお客様とお客様との間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS AWS AWS クラウド内でサービスを実行するインフラストラクチャを保護する責任があります。 AWS また、安全に使用できるサービスも提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。に適用されるコンプライアンスプログラムについて詳しくは AWS CloudTrail、「AWS コンプライアンスプログラム別の対象サービス」を参照してください。
- クラウドにおけるセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、利用時に責任分担モデルを適用する方法を理解するのに役立ちます CloudTrail。以下のトピックでは、 CloudTrail セキュリティとコンプライアンスの目標を満たすように構成する方法を示しています。また、 AWS CloudTrail リソースの監視と保護に役立つ他のサービスの使い方についても学びます。

トピック

でのデータ保護 AWS CloudTrail

のデータ保護には、 AWS https://aws.amazon.com/compliance/shared-responsibility-model/ AWS CloudTrail。このモデルで説明したように、 AWS は、 AWS クラウドすべてを稼働させるグローバルインフラストラクチャを保護する責任があります。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービスのセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

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

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

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、コンソール、API、 CloudTrail または SDK を操作する場合や、 AWS のサービス その他の方法でコンソール、API、SDK を使用する場合も含まれます。 AWS CLI AWS 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

デフォルトでは、 CloudTrail イベントログファイルは Amazon S3 サーバー側暗号化 (SSE) を使用して暗号化されます。ログファイルを () AWS Key Management Service キーで暗号化することもできます。AWS KMSバケットにログファイルを任意の期間、保存することができます。また、Amazon S3 ライフサイクルのルールを定義して、自動的にログファイルをアーカイブまたは削除することもできます。ログファイルの配信と確認に関する通知が必要な場合は、Amazon SNS 通知を設定できます。

以下のセキュリティ上のベストプラクティスもデータ保護に対応しています。 CloudTrail

- CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)
- の Amazon S3 バケットポリシー CloudTrail
- CloudTrail ログファイルの整合性の検証
- CloudTrail AWS アカウント間でのログファイルの共有

CloudTrail ログファイルは Amazon S3 の 1 つまたは複数のバケットに保存されるため、Amazon Simple Storage Service ユーザーガイドのデータ保護情報も確認する必要があります。詳細については、「Amazon S3 のデータ保護」を参照してください。

Identity and Access Management AWS CloudTrail

AWS Identity and Access Management (IAM) は、 AWS のサービス AWS 管理者がリソースへのアクセスを安全に制御できるようにするものです。IAM 管理者は、リソースの使用を認証 (サインイン) および許可 (権限の付与) できるユーザーを制御します。 CloudTrail IAM AWS のサービス は追加料金なしで使用できるアプリです。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- IAM AWS CloudTrail との連携の仕組み
- の ID ベースのポリシーの例 AWS CloudTrail
- AWS CloudTrail リソースベースのポリシーの例
- の Amazon S3 バケットポリシー CloudTrail

- CloudTrail レイククエリ結果の Amazon S3 バケットポリシー
- の Amazon SNS トピックポリシー CloudTrail
- AWS CloudTrail ID とアクセスのトラブルシューティング
- サービスにリンクされたロールを使用する AWS CloudTrail
- AWS の管理ポリシー AWS CloudTrail

対象者

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

サービスユーザー — CloudTrail サービスを使用して業務を行う場合、管理者は必要な認証情報と権限を提供します。 CloudTrail 作業に使用する機能が増えるにつれて、追加の権限が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。の機能にアクセスできない場合は CloudTrail、を参照してくださいAWS CloudTrail ID とアクセスのトラブルシューティング。

サービス管理者 — CloudTrail 会社でリソースを担当している場合は、おそらくへのフルアクセス権を持っているはずです CloudTrail。 CloudTrail サービスユーザーがどの機能やリソースにアクセスすべきかを決めるのはあなたの仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM をどのように使用できるかについての詳細は CloudTrail、「」を参照してくださいIAM AWS CloudTrail との連携の仕組み。

IAM 管理者 — IAM 管理者の場合は、アクセスを管理するポリシーを作成する方法の詳細を知りたいと思うかもしれません。 CloudTrailIAM CloudTrail で使用できるアイデンティティベースのポリシーの例については、を参照してください。の ID ベースのポリシーの例 AWS CloudTrail

アイデンティティを使用した認証

認証とは、ID AWS 認証情報を使用してサインインする方法です。IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) する必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーション ID AWS としてサインインできます。 AWS IAM Identity Center フェデレーテッド ID の例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google や Facebook の認証情報などがあります。フェデ

レーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。 AWS フェデレーションを使用してアクセスすると、間接的にロールを引き継ぐことになります。

ユーザーのタイプによっては、 AWS Management Console AWS またはアクセスポータルにサインインできます。へのサインインについて詳しくは AWS、『AWS サインイン ユーザーガイド』の「AWS アカウントにサインインする方法」を参照してください。

AWS プログラムでアクセスする場合は、認証情報を使用してリクエストに暗号署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨方法を使用して自分でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「 AWS API リクエストへの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、アカウントのセキュリティを強化するために多要素認証 (MFA) AWS を使用することを推奨しています。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

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

フェデレーティッドアイデンティティ

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

フェデレーテッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、Identity Center ディレクトリのユーザー、または ID AWS のサービス ソースを通じて提供された認証情報を使用してアクセスする任意のユーザーです。 AWS Directory Serviceフェデレーテッ

ド ID がアクセスすると AWS アカウント、そのユーザーがロールを引き受け、そのロールが一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自のアイデンティティソース内のユーザーやグループに接続して同期し、すべてのアプリケーションで使用できるようにすることもできます。 AWS アカウント IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定の権限を持つ社内の AWS アカウント ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

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

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

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用してロールを引き受けることができます。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、ロールをプロキシとして使用する代わりに AWS のサービス、ポリシーをリソースに直接アタッチできるものもあります。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — AWS のサービス AWS のサービス他の機能を使用するものもあります。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、あなたはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 AWS のサービス を呼び出すプリンシパルの権限をリクエスト元と組み合わせて使用して AWS のサービス、ダウンストリームサービスにリクエストを行います。FASリクエストは、AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細に

ついては、『IAM ユーザーガイド』の「AWS のサービスに権限を委任するロールの作成」を参照してください。

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

- Amazon EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールをそのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされるインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

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

ポリシーを使用したアクセスの管理

AWS ポリシーを作成して AWS ID またはリソースにアタッチすることで、アクセスを制御します。ポリシーとは、ID またはリソースに関連付けると権限を定義するオブジェクトです。 AWS AWS プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON AWS ドキュメントとして保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

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

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザは AWS Management Console、、 AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント管理ポリシーには、 AWS 管理ポリシーと顧客管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS あまり一般的ではないポリシータイプもサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) — SCP は、組織または組織単位 (OU) の最大権限を指定する JSON ポリシーです。 AWS Organizations AWS Organizations は、 AWS アカウント 企業が所有する複数のものをグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、メンバーアカウントのエンティティ (各エンティティを含む) の権限を制限します。 AWS アカウントのルートユーザー Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。 AWS 複数のポリシータイプが関係している場合にリクエストを許可するかどうかを決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

IAM AWS CloudTrail との連携の仕組み

IAM を使用してアクセスを管理する前に CloudTrail、どの IAM 機能が使用できるかを確認してください。 CloudTrail

で使用できる IAM 機能 AWS CloudTrail

IAM 機能	CloudTrail サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	部分的
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サポート固有)	いいえ
ACL	No
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	はい
転送アクセスセッション (FAS)	はい
サービスロール	あり
サービスリンクロール	はい

AWS その他のサービスがほとんどの IAM CloudTrail 機能でどのように機能するかを大まかに把握するには、IAM ユーザーガイドの「IAM AWS と連携するサービス」を参照してください。

の ID ベースのポリシー CloudTrail

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

の ID ベースのポリシーの例 CloudTrail

CloudTrail ID ベースのポリシーの例については、を参照してください。の ID ベースのポリシーの例 AWS CloudTrail

内のリソースベースのポリシー CloudTrail

リソースベースのポリシーのサポート	部分的

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはを含めることができます。 AWS のサービス

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス権限も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパ

ルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

CloudTrail 外部のイベントソースとの CloudTrail Lake 統合に使用されるチャネルに関するリソースベースのポリシーをサポートします。 AWSチャネルのリソースベースのポリシーでは、チャネル上で `PutAuditEvents` を呼び出して送信先のイベントデータストアにイベントを送信できるプリンシパルエンティティ (アカウント、ユーザー、ロール、フェデレーションユーザー) を定義します。Lake CloudTrail とのインテグレーションの作成について詳しくは、を参照してください。外部のイベントソースとの統合を作成 AWS

例

CloudTrail リソースベースのポリシーの例については、を参照してください。AWS CloudTrail リソースベースのポリシーの例

のポリシーアクション CloudTrail

ポリシーアクションに対するサポート	はい

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

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションは通常、関連する AWS API オペレーションと同じ名前です。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

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

CloudTrail アクションのリストについては、『サービス認証リファレンス』 AWS CloudTrailの「定義するアクション」を参照してください。

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

```
cloudtrail
```

たとえば、ListTags API オペレーションを使用して証跡のタグを一覧表示する権限を付与するには、ポリシーに cloudtrail:ListTags アクションを含めます。ポリシーステートメントには、Action または NotAction 要素を含める必要があります。 CloudTrail このサービスで実行できるタスクを説明する独自のアクションセットを定義します。

単一ステートメントに複数アクションを指定するには、次のようにカンマで区切ります:

```
"Action": [
      "cloudtrail:AddTags",
      "cloudtrail:ListTags",
      "cloudtrail:RemoveTags
```

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

```
"Action": "cloudtrail:Get*"
```

のポリシーリソース CloudTrail

ポリシーリソースに対するサポート	はい

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

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

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

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

CloudTrail リソースタイプとその ARN の一覧については、『サービス認証リファレンス』の「Resources Defined by AWS CloudTrail」を参照してください。どのアクションで各リソースの

ARN を指定できるかについては、「AWS CloudTrailで定義されるアクション」を参照してください。

には CloudTrail、トレイル、イベントデータストア、チャネルの 3 つのリソースタイプがあります。リソースにはそれぞれ、一意の Amazon リソースネーム (ARN) が関連付けられています。ポリシーでは、ARN を使用してポリシーが適用されるリソースを識別します。 CloudTrail 現在のところ、サブリソースと呼ばれることもある他のリソースタイプはサポートされていません。

CloudTrail トレイルリソースには、次の ARN があります。

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

CloudTrail イベントデータストアリソースには、次の ARN があります。

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

CloudTrail チャネルリソースには、次の ARN があります。

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

ARN の形式の詳細については、「Amazon リソースネーム (ARN) AWS とサービス名前空間」を参照してください。

たとえば、ID が *123456789012* の場合、 AWS アカウント ステートメントで米国東部 (オハイオ) リージョンに存在する *My-Trail* という名前のトレイルを指定するには、次の ARN を使用します。

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-Trail"
```

その中の特定のアカウントに属するトレイルをすべて指定するには、ワイルドカード (*) を使用します。 AWS リージョン

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

CloudTrail リソースを作成するアクションなど、特定のリソースでは実行できないアクションもあります。このような場合は、ワイルドカード (*) を使用する必要があります。

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

CloudTrail 多くの API アクションには複数のリソースが含まれます。例えば、CreateTrail にはログファイルを保存するための Amazon S3 バケットが必要です。したがって、ユーザーにはそのバケットへ書き込みするためのアクセス許可が必要です。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
      "resource1",
      "resource2"
```

のポリシー条件キー CloudTrail

サービス固有のポリシー条件キーのサポート	いいえ

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

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

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 AWS OR論理演算を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS グローバル条件キーとサービス固有の条件キーをサポートします。 AWS すべてのグローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

CloudTrail 独自の条件キーは定義していませんが、一部のグローバル条件キーの使用はサポートされています。 AWS すべてのグローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

CloudTrail 条件キーのリストについては、『サービス認証リファレンス』の AWS CloudTrail「条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「アクション定義者」を参照してください AWS CloudTrail。

の ACL CloudTrail

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ABACと CloudTrail

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) AWS や多くのリソースにタグを付けることができます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

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

CloudTrail リソースにはタグを付けることができますが、CloudTrail Lake CloudTrail イベントデータストアとチャネルへのアクセスの制御はタグに基づいてのみサポートされます。タグに基づいて証跡へのアクセスを制御することはできません。

CloudTrail リソースにタグを付けることも、へのリクエストでタグを渡すこともできます CloudTrail。 CloudTrail リソースへのタグ付けの詳細については、「」証跡の作成 と を使用した証跡の作成、更新、管理 AWS CLI「」を参照してください。

での一時認証情報の使用 CloudTrail

一時的な認証情報のサポート	はい

AWS のサービス 一時的な認証情報を使用してサインインすると機能しないものもあります。 AWS のサービス 一時的な認証情報で機能するものなど、追加情報については、『IAM ユーザーガイド』の「IAM と連携する」を参照してくださいAWS のサービス 。

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

または API を使用して一時的な認証情報を手動で作成できます。 AWS CLI AWS その後、その一時的な認証情報を使用してアクセスできます AWS。 AWS 長期アクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをおすすめします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

アクセスセッションを転送する CloudTrail

フォワードアクセスセッション (FAS) をサポート	はい

IAM ユーザーまたはロールを使用してでアクションを実行する場合 AWS、そのユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FASは、を呼び出したプリンシパルの権限と

AWS のサービス、 AWS のサービス ダウンストリームサービスにリクエストを行うリクエストを組み合わせて使用します。FASリクエストは、 AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

CloudTrail のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、『IAM ユーザーガイド』の「AWS のサービスに権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの権限を変更すると、 CloudTrail 機能しなくなる可能性があります。サービスロールの編集は、 CloudTrail ガイダンスが提供されている場合にのみ行ってください。

のサービスにリンクされたロール CloudTrail

サービスリンクロールのサポート	はい

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

CloudTrail との統合のためのサービスにリンクされたロールをサポートします。 AWS Organizations このロールは、組織証跡またはイベントデータストアの作成に必要です。組織記録とイベントデータには、 AWS アカウント 組織内のすべてのイベントのログが格納されます。 CloudTrailサービスにリンクされたロールの作成または管理の詳細については、を参照してください。サービスにリンクされたロールを使用する AWS CloudTrail

の ID ベースのポリシーの例 AWS CloudTrail

デフォルトでは、 CloudTrailユーザーとロールにはリソースを作成または変更する権限がありません。また、 AWS Management Console、 AWS Command Line Interface (AWS CLI)、 AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARN の形式など CloudTrail、で定義されるアクションとリソースタイプの詳細については、『サービス認証リファレンス』の「アクション、リソース、および条件キー」を参照してください。 AWS CloudTrail

トピック

- ポリシーのベストプラクティス
- 例: 指定した証跡の許可および拒否アクション
- 例: 特定の証跡に対するアクションのポリシーの作成と適用
- 例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否
- CloudTrail コンソールを使用する
- ユーザーが自分の許可を表示できるようにする
- ユーザーへのカスタム権限の付与 CloudTrail

ポリシーのベストプラクティス

ID ベースのポリシーは、 CloudTrail アカウント内のリソースを誰かが作成、アクセス、削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーから始めて、最小権限の権限に移行する — ユーザーとワークロードへの権限の付与を開始するには、AWS 多くの一般的なユースケースで権限を付与する管理ポリシーを使用してください。これらのポリシーは、で利用できます。 AWS アカウント AWS ユースケースに固有のカスタマー管理ポリシーを定義して、権限をさらに減らすことをお勧めします。詳細について

は、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。

- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。サービスアクションがなどの特定の用途で使用された場合は AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) が必要 — IAM ユーザーまたは root ユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA をオンにしてください。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、『IAM ユーザーガイド』の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

CloudTrail ポリシーステートメントの要素に使用できるサービス固有のコンテキストキーはありません。`Condition`

例: 指定した証跡の許可および拒否アクション

次の例では、ポリシーを持つユーザーが証跡のステータスと設定を表示し、*`My-First-Trail`* という名前の証跡の口グ記録を開始および停止できるようにするポリシーを示します。*`############ (####) ##### (########) # ID 123456789012 AWS ##### #########`*

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

```
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "cloudtrail:StartLogging",
              "cloudtrail:StopLogging",
              "cloudtrail:GetTrail",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:GetEventSelectors"
          ],
          "Resource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

#####My-First-Trail CloudTrail ##

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Deny",
          "Action": [
              "cloudtrail:*"
          ],
          "NotResource": [
              "arn:aws:cloudtrail:us-east-2:123456789012:trail/My-First-Trail"
          ]
      }
  ]
}
```

例: 特定の証跡に対するアクションのポリシーの作成と適用

権限とポリシーを使用して、ユーザーがトレイルで特定のアクションを実行できるかどうかを制御できます。 CloudTrail

たとえば、社内のデベロッパーグループのユーザーが、特定の証跡の口グ記録を開始または停止しないようにしようとする場合です。ただし、証跡でDescribeTrailsおよびGetTrailStatusアクションを実行する権限を付与しようと思う場合もあります。また、デベロッパーグループのユーザー

自らが管理する証跡では、StartLogging アクションまたは StopLogging アクションを実行する必要があります。

2 つのポリシーステートメントを作成し、それらを IAM に作成するデベロッパーグループにアタッチすることができます。IAM のグループの詳細については、IAM ユーザーガイドの「IAM グループ」を参照してください。

最初のポリシーでは、指定する証跡 ARN の StartLogging アクションと StopLogging アクションを拒否します。次の例で、証跡 ARN は arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446057698000",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-Trail"
            ]
        }
    ]
}
```

2 つ目のポリシーでは、DescribeTrailsGetTrailStatus CloudTrail およびアクションがすべてのリソースで許可されています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1446072643000",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrail",
                "cloudtrail:GetTrailStatus"
            ],
```

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

デベロッパーグループのユーザーが、最初のポリシーに指定された証跡に対してログ記録を開始または終了しようとした場合、そのユーザーはアクセス拒否の例外を受け取ります。デベロッパーグループのユーザーは、自らが作成して管理する証跡のログ記録を開始および停止することはできます。

以下の例は、 AWS CLI という名前のプロファイルに設定された開発者グループを示していますdevgroup。最初に、devgroup のユーザーが describe-trails コマンドを実行します。

```
$ aws --profile devgroup cloudtrail describe-trails
```

コマンドは以下の出力で正常に完了しました。

```
{
    "trailList": [
        {
            "IncludeGlobalServiceEvents": true,
            "Name": "Default",
            "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Example-
Trail",
            "IsMultiRegionTrail": false,
            "S3BucketName": "myS3bucket ",
            "HomeRegion": "us-east-2"
        }
    ]
}
```

次に、このユーザーは、最初のポリシーに指定された証跡に対する get-trail-status コマンドを実行します。

```
$ aws --profile devgroup cloudtrail get-trail-status --name Example-Trail
```

コマンドは以下の出力で正常に完了しました。

```
{
    "LatestDeliveryTime": 1449517556.256,
```

```
    "LatestDeliveryAttemptTime": "2015-12-07T19:45:56Z",
    "LatestNotificationAttemptSucceeded": "",
    "LatestDeliveryAttemptSucceeded": "2015-12-07T19:45:56Z",
    "IsLogging": true,
    "TimeLoggingStarted": "2015-12-07T19:36:27Z",
    "StartLoggingTime": 1449516987.685,
    "StopLoggingTime": 1449516977.332,
    "LatestNotificationAttemptTime": "",
    "TimeLoggingStopped": "2015-12-07T19:36:17Z"
}
```

さらに、devgroup グループのユーザーが同じ証跡に対して stop-logging コマンドを実行します。

```
$ aws --profile devgroup cloudtrail stop-logging --name Example-Trail
```

このコマンドでは次のようなアクセス拒否の例外が返されます。

```
A client error (AccessDeniedException) occurred when calling the StopLogging operation:
 Unknown
```

このユーザーは同じ証跡に対して start-logging コマンドを実行します。

```
$ aws --profile devgroup cloudtrail start-logging --name Example-Trail
```

再びこのコマンドでは次のようなアクセス拒否の例外が返されます。

```
A client error (AccessDeniedException) occurred when calling the StartLogging
 operation: Unknown
```

例: タグに基づいたイベントデータストアを作成または削除するためのアクセスの拒否

次のポリシー例では、次の条件のうち少なくとも 1 つが満たされない場合
は、CreateEventDataStoreでイベントデータストアを作成する権限が拒否されます。

- イベントデータストア自体にはstageのタグキーが適用されていません
- ステージタグの値はalpha、beta、gamma、またはprodのいずれでもありません。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "cloudtrail:CreateEventDataStore",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/stage": [
                        "alpha",
                        "beta",
                        "gamma",
                        "prod"
                    ]
                }
            }
        }
    ]
}
```

以下のポリシー例では、イベントデータストアに prod の値の stage タグがある場合、DeleteEventDataStoreのイベントデータストアを削除するアクセス許可は拒否されます。このようなポリシーで、イベントデータストアが誤って削除されないように保護することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "cloudtrail:DeleteEventDataStore",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

CloudTrail コンソールを使用する

AWS CloudTrail コンソールにアクセスするには、最低限の権限が必要です。これらの権限により、CloudTrail 内のリソースの詳細を一覧表示したり表示したりできる必要があります AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

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

CloudTrail 管理権限の付与

IAM ロールまたはユーザーがトレイル、イベントデータストア、 CloudTrail チャネルなどのリソースを管理できるようにするには、タスクに関連するアクションを実行する権限を明示的に付与する必要があります。 CloudTrail ほとんどの場合、 AWS 事前定義された権限を含む管理ポリシーを使用できます。

> **Note**
>
> CloudTrail 管理タスクを実行するためにユーザーに付与する権限は、Amazon S3 バケットにログファイルを配信したり、Amazon SNS CloudTrail トピックに通知を送信したりするために必要な権限とは異なります。これらのアクセス許可の詳細については、「の Amazon S3 バケットポリシー CloudTrail」を参照してください。
> Amazon Logs との統合を設定する場合は、Amazon CloudWatch Logs CloudTrail CloudWatch ロググループにイベントを配信するために引き受けられるロールも必要です。CloudTrail を使用するロールを作成する必要があります。詳細については、「コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与」および「CloudWatch ログへのイベントの送信」を参照してください。

AWS 以下の管理ポリシーを使用できます CloudTrail。

- AWSCloudTrail_FullAccess— このポリシーは、トレイル、イベントデータストア、 CloudTrail CloudTrail チャネルなどのリソースに対するアクションへのフルアクセスを提供します。このポリシーは、 CloudTrail トレイル、イベントデータストア、チャンネルの作成、更新、削除に必要な権限を付与します。

  このポリシーは、Amazon S3 バケット、ログのロググループ、 CloudWatch およびトレイル用の Amazon SNS トピックを管理するためのアクセス権限も提供します。ただし、`AWSCloudTrail_FullAccess`管理ポリシーには Amazon S3 バケット、 CloudWatch Logs のロググループ、または Amazon SNS トピックを削除するアクセス権限は提供されません。その他の管理ポリシーについては AWS のサービス、『AWS 管理ポリシーリファレンスガイド』を参照してください。

  > **Note**
  >
  > AWSCloudTrail_FullAccessこのポリシーは、組織全体で広く共有されることを意図したものではありません。 AWS アカウントこのロールを持つユーザーは、 AWS アカウントで最も機密かつ重要な監査機能を無効にしたり、再設定したりすることができます。このため、このポリシーはアカウント管理者にのみ適用する必要があります。このポリシーの使用を厳重に管理および監視する必要があります。

- AWSCloudTrail_ReadOnlyAccess— このポリシーは、最近のイベントやイベント履歴など、CloudTrail コンソールを閲覧する権限を付与します。また、このポリシーにより、既存の証跡、イベントデータストア、およびチャネルを表示することもできます。このポリシーが適用されているロールとユーザーはイベント履歴をダウンロードできますが、証跡、イベントデータストア、またはチャンネルを作成または更新することはできません。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- 以下のユーザーおよびグループ AWS IAM Identity Center:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。

- IAM ユーザー:

- ユーザーが担当できるロールを作成します。手順については、「IAM ユーザーガイド」の「IAM ユーザー用ロールの作成」を参照してください。
- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。詳細については、「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

追加リソース

IAM を使用してユーザーやロールなどの ID にアカウント内のリソースへのアクセスを許可する方法の詳細については、IAM ユーザーガイドの「IAM AWS の設定とリソースのアクセス管理」を参照してください。

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

ユーザーが自分の許可を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、またはまたは API を使用してこのアクションをプログラムで実行するための権限が含まれています。 AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

ユーザーへのカスタム権限の付与 CloudTrail

CloudTrail ポリシーは、 CloudTrailで作業するユーザーにアクセス権限を付与します。ユーザーに異なるアクセス権限を付与する必要がある場合は、IAM CloudTrail グループまたはユーザーにポリシーをアタッチできます。ポリシーを編集して、特定のアクセス許可を含めたり除外したりすることができます。独自のカスタムポリシーを作成することもできます。ポリシーとは、ユーザーが実行を許可されているアクションと、ユーザーが実行を許可されているアクションの対象となるリソースを定義する JSON ドキュメントです。個別の例については、「例: 指定した証跡の許可および拒否アクション」および「例: 特定の証跡に対するアクションのポリシーの作成と適用」を参照してください。

目次

読み取り専用アクセス

以下の例は、 CloudTrail トレイルへの読み取り専用アクセスを許可するポリシーを示しています。これはマネージドポリシー AWSCloudTrail_ReadOnlyAccess に相当します。これによってユーザーに付与されるアクセス許可は証跡の情報を見るためのもので、証跡を作成または更新することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:Get*",
                "cloudtrail:Describe*",
                "cloudtrail:List*",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

このポリシーステートメントの Effect 要素で、アクションが許可されるか拒否されるかを指定します。Action 要素には、ユーザーによる実行を許可する特定のアクションを指定します。Resourceこのエレメントには、 AWS ユーザーがそれらのアクションを実行できるリソースが一覧表示されます。 CloudTrail アクションへのアクセスを制御するポリシーの場合、Resource要素は通常「すべてのリソース」を意味するワイルドカードに設定されます。*

Action 要素の値は、サービスがサポートする API に対応しています。アクションの前には、cloudtrail: CloudTrail アクションを指すことを示す文字が付いています。次の例に示すように、* ワイルドカード文字を Action 要素で使用できます。

- "Action": ["cloudtrail:*Logging"]

  これにより、「Logging」(StartLogging,StopLogging) CloudTrail で終わるすべてのアクションが許可されます。

- "Action": ["cloudtrail:*"]

  これにより、 CloudTrail すべてのアクションが許可されますが、 AWS 他のサービスのアクションは許可されません。

- "Action": ["*"]

  これにより、 AWS すべてのアクションが許可されます。このアクセス許可は、アカウントの AWS 管理者として行動するユーザーに適しています。

読み取り専用ポリシーでは、CreateTrail、UpdateTrail、StartLogging、StopLogging の各アクションのアクセス許可はユーザーに付与されません。このポリシーを持つユーザーは、証跡の作成、証跡の更新、ログ記録のオンとオフの切り替えを行うことはできません。 CloudTrail アクションのリストについては、AWS CloudTrail API リファレンスをご覧ください。

フル アクセス

次の例は、へのフルアクセスを許可するポリシーを示しています CloudTrail。これはマネージドポリシー AWSCloudTrail_FullAccess に相当します。 CloudTrail すべてのアクションを実行する権限をユーザーに付与します。また、ユーザーは Amazon S3 のデータイベントをログに記録したり AWS Lambda、Amazon S3 バケット内のファイルを管理したり、Logs CloudWatch CloudTrail がログイベントをモニタリングする方法を管理したり、ユーザーが関連付けられているアカウントの Amazon SNS トピックを管理したりできます。

> **Important**
>
> AWSCloudTrail_FullAccessポリシーまたは同等の権限は、アカウント全体で広く共有されることを意図したものではありません。 AWS このロールまたは同等のアクセス権を持つユーザーは、自分のアカウントで最も機密性が高く重要な監査機能を無効化または再設定できます。 AWS そのため、このポリシーはアカウント管理者にのみ適用され、このポリシーの使用は厳密に制御および監視する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:SetTopicAttributes",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutBucketPolicy"
            ],
            "Resource": [
                "arn:aws:s3:::aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudtrail:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-cloudtrail-logs*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudtrail.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey",
                "kms:CreateAlias",
                "kms:ListKeys",
                "kms:ListAliases"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:ListFunctions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Config コンソール上の情報を表示する権限を付与する CloudTrail

CloudTrail コンソールには、そのイベントに関連するリソースを含むイベント情報を表示できます。これらのリソースでは、 AWS Config AWS Config アイコンを選択してそのリソースのタイムラインをコンソールに表示できます。このポリシーをユーザーに添付して、 AWS Config 読み取り専用アクセスを許可してください。このポリシーでは、 AWS Configの設定を変更するアクセス許可は付与されません。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

詳細については、「AWS Configで参照されたリソースの表示」を参照してください。

コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与

十分な権限があれば、 CloudWatch CloudTrail コンソールでログへのイベントの配信を表示して設定できます。これらの権限は、 CloudTrail管理者に付与されている権限を超える場合があります。CloudWatch Logs CloudTrail との統合を設定および管理する管理者にこのポリシーを添付してください。このポリシーでは、Logs CloudTrail CloudWatch 内またはログ内の権限を直接付与するのではなく、 CloudWatch Logs CloudTrail グループにイベントを正常に配信するために必要となるロールの作成と設定に必要な権限を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy",
            "iam:AttachRolePolicy",
            "iam:ListRoles",
```

```
            "iam:GetRolePolicy",
            "iam:GetUser"
        ],
        "Resource": "*"
    }]
}
```

詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。

追加情報

IAM を使用してユーザーやロールなどの ID にアカウント内のリソースへのアクセスを許可する方法の詳細については、IAM ユーザーガイドの「はじめに」と「AWS リソースのアクセス管理」を参照してください。

AWS CloudTrail リソースベースのポリシーの例

CloudTrail Lake CloudTrail インテグレーションに使用されるチャンネルのリソースベースのアクセス権限ポリシーをサポートします。 CloudTrail Lake CloudTrail とのインテグレーションの作成について詳しくは、を参照してください。外部のイベントソースとの統合を作成 AWS

ポリシーに必要な情報は、統合タイプによって決まります。

- CloudTrail ディレクション統合では、ポリシーにパートナーの AWS アカウント ID を含める必要があり、パートナーから提供された固有の外部 ID を入力する必要があります。 CloudTrail CloudTrail コンソールを使用してインテグレーションを作成すると、パートナーの AWS アカウント ID がリソースポリシーに自動的に追加されます。 AWS アカウント ポリシーに必要な番号を取得する方法については、パートナーのドキュメントを参照してください。
- ソリューション統合では、プリンシパルとして少なくとも 1 つの AWS アカウント ID を指定する必要があります。また、代理人の混乱を防ぐために任意で外部 ID を入力することもできます。

リソースベースのポリシーの要件は次のとおりです。

- ポリシーで定義されているリソース ARN は、ポリシーがアタッチされているチャネル ARN と一致する必要があります。
- ポリシーには、 1 つのアクションのみを含めます。`cloudtrail-data:PutAuditEvents`

- ポリシーには、少なくとも 1 つのステートメントを含めます。ポリシーには、最大 20 個のステートメントを記述できます。
- 各ステートメントには、少なくとも 1 つのプリンシパルを含めます。1 つのステートメントには、最大 50 個のプリンシパルを記述できます。

所有者によるリソースへのアクセスがポリシーで拒否されていない限り、チャネル所有者はチャネルで PutAuditEvents API を呼び出すことができます。

トピック

- 例: プリンシパルへのチャネルアクセス権の付与
- 例: 外部 ID を使用して混乱した代理問題を防止する

例: プリンシパルへのチャネルアクセス権の付与

次の例では、ARN を持つプリンシパル にarn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root、および arn:aws:iam::123456789012:root ARN CloudTrail を持つチャネルで PutAuditEventsAPI を呼び出す権限を付与します。arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b"
```

```
        }
    ]
}
```

例: 外部 ID を使用して混乱した代理問題を防止する

次の例では、外部 ID を使用して混乱した代理問題に対処し防止しています。混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。

統合パートナーはポリシーで使用する外部 ID を作成します。次に、統合の作成の一環として、統合パートナーは外部 ID を提供します。値は、パスフレーズやアカウント番号など、一意であればどんな文字列でもかまいません。

この例では、ARN を持つプリンシパル にarn:aws:iam::111122223333:rootarn:aws:iam::444455556666:root、および PutAuditEventsAPI arn:aws:iam::123456789012:root への呼び出しにポリシーで定義された外部 ID CloudTrail 値が含まれる場合にチャネルリソースで PutAuditEvents API を呼び出す権限を付与します。

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Sid": "ChannelPolicy",
            "Effect": "Allow",
            "Principal":
            {
                "AWS":
                [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root",
                    "arn:aws:iam::123456789012:root"
                ]
            },
            "Action": "cloudtrail-data:PutAuditEvents",
            "Resource": "arn:aws:cloudtrail:us-east-1:777788889999:channel/
EXAMPLE-80b5-40a7-ae65-6e099392355b",
            "Condition":
            {
                "StringEquals":
```

```
                {
                    "cloudtrail:ExternalId": "uniquePartnerExternalID"
                }
            }
        }
    ]
}
```

の Amazon S3 バケットポリシー CloudTrail

デフォルトでは、Amazon S3 バケットとオブジェクトはプライベートです。リソース所有者 (バケットを作成した AWS アカウント) のみが、バケットとそれに含まれるオブジェクトにアクセスできます。リソース所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

Amazon S3 バケットを作成または変更して組織の証跡のログファイルを受け取れるようにするには、バケットポリシーを変更する必要があります。詳細については、「を使用して組織の証跡を作成する AWS Command Line Interface」を参照してください。

ログファイルを S3 CloudTrail バケットに配信するには、必要な権限が必要で、リクエスタ支払いバケットとして設定することはできません。

CloudTrail 以下のフィールドをポリシーに自動的に追加します。

- 許可された SID。
- バケット名。
- のサービスプリンシパル名 CloudTrail
- バケット名、プレフィックス (指定した場合)、 AWS アカウント ID を含む、ログファイルが保存されているフォルダーの名前

セキュリティのベストプラクティスとして、`aws:SourceArn` 条件キーを Amazon S3 バケットポリシーに追加します。IAM `aws:SourceArn` グローバル条件キーを使用すると、特定の 1 つまたは複数の証跡についてのみ S3 CloudTrail バケットに書き込むことができます。`aws:SourceArn` の値は常に、ログを格納するためにバケットを使用している証跡の ARN (または証跡 ARN の配列) になります。既存の証跡の S3 バケットポリシーに `aws:SourceArn` 条件キーを必ず追加してください。

以下のポリシーでは、 CloudTrail サポートされているバケットにログファイルを書き込むことができます。 AWS リージョ

ン*myBucketName*、*[OptionalPrefix]/*、*myAccountId#region#TrailName* を、設定に適した値に置き換えてください。

S3 バケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

の詳細については、を参照してください。 AWS リージョンCloudTrail サポートされているリージョン

目次

CloudTrail ログ配信用の既存のバケットを指定する

ログファイル配信の保存場所として既存の S3 バケットを指定した場合は、 CloudTrail バケットへの書き込みを許可するポリシーをバケットにアタッチする必要があります。

> **Note**
>
> ベストプラクティスとして、 CloudTrail ログ専用の S3 バケットを使用してください。

CloudTrail 必要なポリシーを Amazon S3 バケットに追加するには

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. CloudTrail ログファイルを配信するバケットを選択し、[アクセス権] を選択します。
3. [編集] を選択します。
4. S3 bucket policy を [Bucket Policy Editor] ウィンドウにコピーします。イタリック体のプレースホルダーを、バケット、プレフィックス、アカウント番号の名前に置き換えます。証跡の作成時にプレフィックスを指定した場合は、ここに含めます。プレフィックスは、バケットにフォルダのような組織を作成する S3 オブジェクトキーへのオプションの追加です。

   > **Note**
   >
   > 既存のバケットにすでに 1 つ以上のポリシーがアタッチされている場合は、 CloudTrail そのポリシーへのアクセスに関するステートメントを追加します。バケットにアクセスするユーザーに適していることを確認するために、作成したアクセス権限のセットを評価します。

他のアカウントからログファイルを受信

CloudTrail AWS 複数のアカウントのログファイルを 1 つの S3 バケットに配信するように設定できます。詳細については、「CloudTrail 複数のアカウントからのログファイルの受信」を参照してください。

組織の証跡のログファイルを保存するために使用する Amazon S3 バケットを作成または更新する

組織の証跡のログファイルを受信するには、Amazon S3 バケットを指定する必要があります。このバケットには、 CloudTrail 組織のログファイルをバケットに入れることを許可するポリシーが必要です。

以下は、*myOrganizationBucket*組織の管理アカウントが所有するという名前の Amazon S3 バケットのポリシーの例です。*#####myOrganizationBucket*、*####### ID#######0-0-0-OrganizationID ##################*。

このバケットには、3 つのステートメントがあります。

- 最初のステートメントでは CloudTrail 、Amazon S3 バケットで Amazon S3 `GetBucketAcl` アクションを呼び出すことができます。
- 2 番目のステートメントでは、証跡が組織の証跡からそのアカウントの証跡にのみ変更された場合にログに記録することを許可します。
- 3 番目のステートメントでは、組織証跡をログに記録することが可能になります。

ポリシー例には、Amazon S3 バケットポリシーの `aws:SourceArn` 条件キーが含まれています。IAM `aws:SourceArn` グローバル条件キーは、特定の 1 つまたは複数の証跡についてのみ S3 CloudTrail バケットに書き込まれるようにするのに役立ちます。組織の証跡の場合、`aws:SourceArn` の値は管理アカウントで保持され、管理アカウント ID を使用する証跡の ARN である必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
```

```
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myOrganizationBucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/managementAccountID/
*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailOrganizationWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::myOrganizationBucket/AWSLogs/o-organizationID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
```

```
                    "aws:SourceArn":
  "arn:aws:cloudtrail:region:managementAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

このポリシー例では、メンバーアカウントのユーザーが組織用に作成されたログファイルにアクセスすることを許可していません。デフォルトでは、組織のログファイルは管理アカウントにのみアクセスできます。メンバーアカウントの IAM ユーザーに対して Amazon S3 バケットへの読み取りアクセスを許可する方法については、「CloudTrail AWS アカウント間でのログファイルの共有」を参照してください。

Amazon S3 バケットポリシーのトラブルシューティング

以下のセクションでは、S3 バケットポリシーをトラブルシューティングする方法について説明します。

一般的な Amazon S3 ポリシー設定のエラー

証跡の作成または更新の一環として新しいバケットを作成すると、 CloudTrail必要な権限がバケットにアタッチされます。バケットポリシーでは"cloudtrail.amazonaws.com"、 CloudTrail すべてのリージョンにログを配信できるサービスプリンシパル名を使用します。

あるリージョンのログを配信していない場合は CloudTrail 、 CloudTrail バケットに各リージョンのアカウント ID を指定する古いポリシーが適用されている可能性があります。このポリシーでは、CloudTrail指定されたリージョンにのみログを配信する権限が付与されます。

ベストプラクティスとして、 CloudTrail サービスプリンシパルの権限を使用するようにポリシーを更新してください。これを行うには、アカウント ID ARN をサービスプリンシパル名 "cloudtrail.amazonaws.com" に置き換えます。これにより、 CloudTrail 現在のリージョンと新しいリージョンのログを配信する権限が付与されます。セキュリティのベストプラクティスとして、Amazon S3 バケットポリシーに aws:SourceArn または aws:SourceAccount 条件キーを追加します。これにより、S3 バケットへの不正なアカウントアクセスを防止できます。既存の証跡がある場合は、必ず 1つまたは複数の条件キーを追加してください。次の例は、推奨されるポリシーの設定を示しています。*[optionalPrefix]/*、*myAccountId######TrailName* を、設定に適した値に置き換えてください*myBucketName*。

Example サービスプリンシパル名を使用したバケットポリシーの例

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailWrite20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:PutObject",
            "Resource":
 "arn:aws:s3:::myBucketName/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {"StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

既存のバケットのプレフィックスを変更する

証跡からログを受け取る S3 バケットのログファイルプレフィックスを追加、変更、または削除しようとすると、次のエラー「There is a problem with the bucket policy (バケットバケットポリシーに問題があります) 」が表示されることがあります。その場合、バケットポリシーに問題があります。誤ったプレフィックスを使用しているバケットポリシーは、証跡がログをバケットに配信されないようにすることができます。この問題を解決するには、Amazon S3 コンソールを使用してバケットポ

リシーのプレフィックスを更新し、 CloudTrailコンソールを使用してトレイルのバケットに同じプレフィックスを指定します。

Amazon S3 バケットのログファイルプレフィックスを更新するには

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. プレフィックスを変更するバケットを選択し、[Permissions] (アクセス許可) を選択します。
3. [編集] を選択します。
4. バケットポリシーで、`s3:PutObject` アクションの下で、`Resource` エントリを編集して、必要に応じてログファイル*`prefix/`* を追加、変更、削除します。

```
"Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*",
```

5. [保存] を選択します。
6. https://console.aws.amazon.com/cloudtrail/ CloudTrail でコンソールを開きます。
7. 証跡を選択し、Storage location の場合は鉛筆アイコンをクリックして、バケットの設定を編集します。
8. S3 バケット の場合は、変更するプレフィックスを持つバケットを選択します。
9. Log file prefix の場合は、バケットポリシーに入力したプレフィックスに一致するようにプレフィックスを更新します。
10. [Save] (保存) を選択します。

追加リソース

S3 バケットポリシーの詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットポリシーの使用」を参照してください。

CloudTrail レイククエリ結果の Amazon S3 バケットポリシー

デフォルトでは、Amazon S3 バケットとオブジェクトはプライベートです。リソース所有者 (バケットを作成した AWS アカウント) のみが、バケットとそれに含まれるオブジェクトにアクセスできます。リソース所有者は、アクセスポリシーを記述することで他のリソースおよびユーザーにアクセス権限を付与することができます。

CloudTrail Lake クエリの結果を S3 CloudTrail バケットに配信するには、必要な権限が必要で、リクエスタ支払いバケットとして設定することはできません。

CloudTrail 以下のフィールドをポリシーに自動的に追加します。

- 許可された SID。
- バケット名。
- のサービスプリンシパル名 CloudTrail

セキュリティのベストプラクティスとして、aws:SourceArn 条件キーを Amazon S3 バケットポリシーに追加します。IAM aws:SourceArn グローバル条件キーは、S3 CloudTrail バケットへの書き込みがイベントデータストア専用であることを保証するのに役立ちます。

以下のポリシーでは、 CloudTrail AWS リージョンサポート対象外のバケットにクエリ結果を配信できます。*myBucketName*、*myAccountId*、*myQueryRunning#########################*。*myAccountId* AWS はに使用されるアカウント ID であり CloudTrail、S3 AWS バケットのアカウント ID と同じではない場合があります。

> **Note**
>
> バケットポリシーが KMS キーに関するステートメントを含む場合には、完全修飾 KMS キー ARN を使用することをお勧めします。代わりに KMS キーエイリアスを使用すると、 AWS KMS リクエスタのアカウント内のキーが解決されます。この動作により、バケット所有者ではなく、リクエスタに属する KMS キーでデータが暗号化される可能性があります。
> これが組織のイベントデータストアである場合は、そのイベントデータストアの ARN に、管理アカウントの AWS アカウント ID が含まれている必要があります。これは、管理アカウントがすべての組織リソースの所有権を保持しているためです。

S3 バケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::myBucketName",
                "arn:aws:s3:::myBucketName/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::myBucketName",
            "Condition": {
                "StringLike": {
                    "aws:sourceAccount": "myAccountID",
                    "aws:sourceArn":
 "arn:aws:cloudtrail:myQueryRunningRegion:myAccountID:eventdatastore/*"
                }
            }
        }
    ]
}
```

目次

Lake のクエリ結果に既存のバケットを指定する CloudTrail

CloudTrail Lake クエリ結果の配信の保存場所として既存の S3 バケットを指定した場合は、CloudTrail クエリ結果をバケットに配信することを許可するポリシーをバケットにアタッチする必要があります。

> **Note**
>
> ベストプラクティスとして、 CloudTrail Lake のクエリ結果には専用の S3 バケットを使用してください。

CloudTrail 必要なポリシーを Amazon S3 バケットに追加するには

1. https://console.aws.amazon.com/s3/でAmazon S3 コンソールを開きます。
2. Lake CloudTrail クエリの結果を配信するバケットを選択し、[アクセス権] を選択します。
3. [編集] を選択します。
4. S3 bucket policy for query results を [Bucket Policy Editor] ウィンドウにコピーします。イタリック体のプレースホルダーを、バケット、リージョン、アカウント ID の名前に置き換えます。

> **Note**
>
> 既存のバケットにすでに 1 つ以上のポリシーがアタッチされている場合は、 CloudTrail そのポリシーへのアクセスに関するステートメントを追加します。バケットにアクセスするユーザーに適していることを確認するために、作成したアクセス権限のセットを評価します。

追加リソース

S3 バケットポリシーの詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットポリシーの使用」を参照してください。

の Amazon SNS トピックポリシー CloudTrail

SNS CloudTrail トピックに通知を送信するには、必要な権限が必要です。 CloudTrailコンソールでの証跡の作成または更新の一部として Amazon SNS トピックを作成すると、必要なアクセス権限がトピックに自動的にアタッチされます。 CloudTrail

> **Important**
>
> セキュリティのベストプラクティスとして、SNS トピックへのアクセスを制限するために、SNS 通知を送信する証跡を作成または更新した後、SNS トピックにアタッチされている IAM ポリシーを手動で編集して条件キーを追加することを強くお勧めします。詳細につい

ては、このトピックの「the section called “SNS トピックポリシーのセキュリティのベストプラクティス”」を参照してください。

CloudTrail 以下のフィールドを含む次のステートメントをポリシーに追加します。

- 許可された SID。
- のサービスプリンシパル名 CloudTrail。
- SNS トピック (リージョン、アカウント ID、およびトピック名を含む)。

以下のポリシーでは、 CloudTrail サポートされている地域からのログファイル配信に関する通知の送信を許可しています。詳細については、「CloudTrail サポートされているリージョン」を参照してください。これは、証跡を作成または更新し、SNS 通知を有効にするときに新規または既存の SNS トピックポリシーにアタッチされるデフォルトのポリシーです。

SNS トピックポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:region:SNSTopicOwnerAccountId:SNSTopicName"
        }
    ]
}
```

AWS KMS暗号化された Amazon SNS トピックを使用して通知を送信するには、のポリシーに次のステートメントを追加して、イベントソース (CloudTrail) と暗号化されたトピック間の互換性を有効にする必要もあります。 AWS KMS key

KMS キーポリシー

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

詳細については、「AWS サービスからのイベントソースと暗号化されたトピック間の互換性を有効にする」を参照してください。

目次

SNS トピックポリシーのセキュリティのベストプラクティス

デフォルトでは、Amazon SNS CloudTrail トピックにアタッチされる IAM ポリシーステートメントにより、 CloudTrail サービスプリンシパルは ARN で識別される SNS トピックに公開できます。攻撃者が SNS トピックにアクセスして、 CloudTrail トピックの受信者に代わって通知を送信するのを防ぐには、SNS トピックポリシーを手動で編集して CloudTrail 、によって添付されたポリシーステートメントに条件キーを追加します。`aws:SourceArn` CloudTrailこのキーの値は、証跡の ARN、または SNS トピックを使用している証跡 ARN の配列です。特定の証跡 ID と証跡を所有するアカウント ID の両方が含まれているため、SNS トピックへのアクセスは証跡を管理するアクセス許可を持つアカウントのみに制限されます。SNS トピックポリシーに条件キーを追加する前に、コンソールのトレイル設定から SNS トピック名を取得してください。 CloudTrail

aws:SourceAccount 条件キーもサポートされていますが、推奨されません。

aws:SourceArn 条件キーを SNS トピックポリシーに追加するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. 証跡設定に表示される SNS トピックを選択し、[編集] を選択します。
4. [アクセスポリシー] を展開します。
5. アクセスポリシー JSON エディタで、次の例のようなブロックを探します。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 次の例に示すように、条件 aws:SourceArn 用の新しいブロックを追加します。の値aws:SourceArnは、SNS に通知を送信するトレイルの ARN です。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail/Trail3"
        }
      }
    }
```

7. SNS トピックポリシーの編集が終了したら、[変更の保存] を選択します。

aws:SourceAccount 条件キーを SNS トピックポリシーに追加するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. 証跡設定に表示される SNS トピックを選択し、[編集] を選択します。
4. [アクセスポリシー] を展開します。
5. アクセスポリシー JSON エディタで、次の例のようなブロックを探します。

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496"
    }
```

6. 次の例に示すように、条件 aws:SourceAccount 用の新しいブロックを追加します。aws:SourceAccountの値はトレイルを所有するアカウントの ID です。 CloudTrail この例では、SNS トピックへのアクセスを、アカウント 123456789012 にサインインできるユーザーのみに制限しています。 AWS

```
    {
      "Sid": "AWSCloudTrailSNSPolicy20150319",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-west-2:111122223333:aws-cloudtrail-
logs-111122223333-61bbe496",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
```

7. SNS トピックポリシーの編集が終了したら、[変更の保存] を選択します。

通知の送信用に既存のトピックを指定する

Amazon SNS トピックのアクセス権限を Amazon SNS コンソールのトピックポリシーに手動で追加し、コンソールでトピックを指定できます。 CloudTrail

SNS トピックポリシーを手動で更新するには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. [Topics] を選択し、トピックを選択します。
3. [編集] を選択し、[アクセスポリシー] までスクロールします。
4. リージョン、アカウント ID、SNS topic policyトピック名に適切な値を含むステートメントを追加します。
5. トピックが暗号化されたトピックの場合は、 CloudTrail `kms:GenerateDataKey*kms:Decrypt`権限を持つことを許可する必要があります。詳細については、「Encrypted SNS topic KMS key policy」を参照してください
6. [変更の保存] を選択します。
7. CloudTrail コンソールに戻り、トレイルのトピックを指定します。

SNS トピックポリシーのトラブルシューティング

以下のセクションでは、SNS トピックポリシーをトラブルシューティングする方法について説明します。

シナリオ:

- CloudTrail リージョンの通知を送信していない
- CloudTrail 組織のメンバーアカウントには通知を送信していません

CloudTrail リージョンの通知を送信していない

トレイルの作成または更新の一環として新しいトピックを作成すると、 CloudTrail 必要な権限がトピックにアタッチされます。トピックポリシーでは`"cloudtrail.amazonaws.com"`、 CloudTrail すべてのリージョンに通知を送信できるサービスプリンシパル名を使用します。

CloudTrail あるリージョンの通知が送信されない場合、 CloudTrail トピックに各リージョンのアカウント ID を指定する古いポリシーが適用されている可能性があります。このポリシーでは、CloudTrail 指定された地域にのみ通知を送信する権限が付与されます。

以下のトピックポリシーでは、 CloudTrail 指定した 9 つのリージョンのみに通知を送信できます。

Example アカウント ID を使用したトピックポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"AWS": [
            "arn:aws:iam::903692715234:root",
            "arn:aws:iam::035351147821:root",
            "arn:aws:iam::859597730677:root",
            "arn:aws:iam::814480443879:root",
            "arn:aws:iam::216624486486:root",
            "arn:aws:iam::086441151436:root",
            "arn:aws:iam::388731089494:root",
            "arn:aws:iam::284668455005:root",
            "arn:aws:iam::113285607260:root"
        ]},
        "Action": "SNS:Publish",
        "Resource": "aws:arn:sns:us-east-1:123456789012:myTopic"
    }]
}
```

このポリシーでは、 CloudTrail 個々のアカウント ID に基づく権限を使用します。新しいリージョンの口グを配信するには、 CloudTrailそのリージョンのアカウント ID を含むようにポリシーを手動で更新する必要があります。たとえば、米国東部 (オハイオ) CloudTrail リージョンのサポートが追加されたため、ポリシーを更新してそのリージョンのアカウント ID ARN を追加する必要があります。`"arn:aws:iam::475085895292:root"`

ベストプラクティスとして、 CloudTrail サービスプリンシパルの権限を使用するようにポリシーを更新してください。これを行うには、アカウント ID ARN をサービスプリンシパル名 `"cloudtrail.amazonaws.com"` に置き換えます。

これにより、 CloudTrail 現在のリージョンと新しいリージョンに通知を送信する権限が付与されます。以下に示しているのは、以前のポリシーの最新バージョンです。

Example サービスプリンシパル名を使用したトピックポリシー

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AWSCloudTrailSNSPolicy20131101",
        "Effect": "Allow",
        "Principal": {"Service": "cloudtrail.amazonaws.com"},
        "Action": "SNS:Publish",
        "Resource": "arn:aws:sns:us-west-2:123456789012:myTopic"
    }]
}
```

ポリシーの値が正しいことを確認します。

- [Resource] フィールドに、トピックの所有者のアカウント番号を指定します。自分で作成したトピックについては、自分のアカウント番号を指定します。
- リージョンと SNS トピック名の適切な値を指定します。

CloudTrail 組織のメンバーアカウントには通知を送信していません

AWS Organizations 組織の記録を持つメンバーアカウントが Amazon SNS 通知を送信していない場合、SNS トピックポリシーの設定に問題がある可能性があります。 CloudTrail リソースの検証に失敗した場合でも、たとえば組織記録の SNS トピックにすべてのメンバーアカウント ID が含まれていない場合など、メンバーアカウントに組織証跡が作成されます。SNS トピックポリシーが正しくないと、認証が失敗します。

トレイルの SNS トピックポリシーに承認エラーがあるかどうかを確認するには:

- CloudTrail コンソールから、トレイルの詳細ページを確認します。認証に失敗すると、詳細ページには警告が表示されSNS authorization failed、SNS トピックポリシーを修正するよう指示されます。
- から AWS CLI、get-trail-statusコマンドを実行します。認証に失敗した場合、LastNotificationErrorコマンド出力には値がのフィールドが含まれますAuthorizationError。

追加リソース

Amazon SNS トピックおよびそのサブスクライブの詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

AWS CloudTrail ID とアクセスのトラブルシューティング

IAM CloudTrail を操作する際に発生する可能性のある一般的な問題の診断と修正に役立つ情報は次のとおりです。

トピック

私にはアクションを実行する権限がありません。 CloudTrail

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なcloudtrail:*GetWidget* アクセス許可を持っていない場合に発生するものです。

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

この場合、cloudtrail:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

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

AWS Management Console 操作を実行する権限がないと表示された場合は、管理者に連絡して支援を求める必要があります。管理者とは、サインイン認証情報を提供した担当者です。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用してトレイルの詳細を表示しようとしても、 CloudTrail 自分のアカウントに適切な管理ポリシー (AWSCloudTrail_FullAccessまたはAWSCloudTrail_ReadOnlyAccess) または同等の権限が適用されていない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 cloudtrail:GetTrailStatus on resource: My-Trail
```

この場合、マテオは管理者に自分のポリシーを更新して、コンソール内の証跡情報とステータスにアクセスできるようにするよう依頼します。

AWSCloudTrail_FullAccess管理ポリシーまたは同等の権限を持つ IAM ユーザーまたはロールでサインインし、証跡と Amazon CloudWatch Logs AWS Config の統合を設定できない場合、それらのサービスとの統合に必要なアクセス権限がない可能性があります。詳細については、「AWS Config コンソール上の情報を表示する権限を付与する CloudTrail 」および「コンソールで Amazon CloudWatch Logs CloudTrail 情報を表示および設定する権限の付与」を参照してください。

`iam:PassRole` を実行する権限がない

`iam:PassRole`アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新してロールを渡せるようにする必要があります。 CloudTrail

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。そのためには、サービスにロールを渡す権限が必要です。

以下のエラー例は、という名前の IAM `marymajor` ユーザーがコンソールを使用してアクションを実行しようとしたときに発生します。 CloudTrailただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

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

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

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

AWS アカウント CloudTrail 自分以外の人にも私のリソースへのアクセスを許可したい

ロールを作成して、 CloudTrail 複数のユーザー間で情報を共有できます AWS アカウント。詳細については、「 CloudTrail AWS アカウント間でのログファイルの共有」を参照してください。

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセス制御リスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- CloudTrail これらの機能をサポートするかどうかについては、を参照してくださいIAM AWS CloudTrail との連携の仕組み。
- AWS アカウント 所有しているリソース全体のリソースへのアクセスを提供する方法については、『IAM ユーザーガイド』の「AWS アカウント 所有する別の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスを第三者に提供する方法については AWS アカウント、IAM ユーザーガイドの「AWS アカウント 第三者が所有するリソースへのアクセスの提供」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

`iam:PassRole` を実行する権限がない

`iam:PassRole`アクションを実行する権限がないというエラーが表示された場合は、ロールをに渡せるようにポリシーを更新する必要があります。 CloudTrail

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。そのためには、サービスにロールを渡す権限が必要です。

以下のエラー例は、という名前の IAM `marymajor` ユーザーがコンソールを使用してアクションを実行しようとしたときに発生します。 CloudTrailただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

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

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

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

組織の証跡またはイベントデータストアを作成しようとすると NoManagementAccountSLRExistsException 例外が発生する

NoManagementAccountSLRExistsException 例外は、サービスにリンクされたロールが管理アカウントにない場合に発生します。 AWS Organizations AWS CLI または API オペレーションを使用して委任管理者を追加する場合、サービスにリンクされたロールが存在しない場合は作成されません。

組織の管理アカウントを使用して委任管理者を追加したり、 CloudTrail コンソールで組織の記録データストアやイベントデータストアを作成したり、 AWS CLI または CloudTrail API CloudTrail を使用したりすると、管理アカウントのサービスにリンクされたロールがまだ存在しない場合は自動的に作成されます。

委任管理者を追加していない場合は、 CloudTrail AWS CLI コンソールまたは CloudTrail API を使用して委任管理者を追加します。委任管理者の追加について詳しくは、「 CloudTrail 委任された管理者を追加するおよび RegisterOrganizationDelegatedAdmin(API)」を参照してください。

委任管理者をすでに追加している場合は、 CloudTrail 管理アカウントを使用してコンソールに組織記録またはイベントデータストアを作成するか、または API を使用します。 AWS CLI CloudTrail 組織記録の作成について詳しくは、コンソールで組織の証跡を作成するを使用して組織の証跡を作成する AWS Command Line Interface、および CreateTrail(API) を参照してください。

サービスにリンクされたロールを使用する AWS CloudTrail

AWS CloudTrail AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用する。サービスにリンクされたロールは、に直接リンクされるユニークなタイプの IAM ロールです。 CloudTrailサービスにリンクされたロールは、 CloudTrail サービスがユーザーに代わって他のユーザーを呼び出すために必要なすべての権限によって事前定義されており、その権限が含まれています。 AWS のサービス

サービスにリンクされたロールでは、必要な権限を手動で追加する必要がないため、 CloudTrail 設定が簡単になります。 CloudTrail サービスにリンクされたロールの権限を定義し、特に定義されていない限り、 CloudTrail そのロールを引き受けることしかできません。定義されたアクセス許可に

は、信頼ポリシーとアクセス権限ポリシーが含まれ、そのアクセス権限ポリシーを他の IAM エンティティに適用することはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携するAWSサービス」を参照して、サービスにリンクされたロール 列が [はい]になっているサービスを見つけてください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

サービスにリンクされたロールの権限 CloudTrail

CloudTrail という名前のサービスにリンクされたロールを使用 AWSServiceRoleForCloudTrail— このサービスにリンクされたロールは、組織の記録や組織のイベントデータストアをサポートするために使用されます。

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

- `cloudtrail.amazonaws.com`

このロールは、 CloudTrail での組織トレイルと CloudTrail Lake 組織イベントデータストアの作成と管理を支援するために使用されます。 CloudTrail詳細については、「組織の証跡の作成」を参照してください。

CloudTrailServiceRolePolicyロールに添付されたポリシーにより CloudTrail 、指定されたリソースに対して以下のアクションを実行できます。

- CloudTrail すべてのリソースに対するアクション:
  - `All`
- AWS Organizations 全リソースに対するアクション:
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- CloudTrail サービスプリンシパルが組織の委任管理者を一覧表示するためのすべてのOrganizationsリソースに対するアクション:
  - `organizations:ListDelegatedAdministrators`
- 組織のイベントデータストアで Lake フェデレーションを無効にするアクション:

- glue:DeleteTable
- lakeformation:DeRegisterResource

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

サービスにリンクされたロールの作成 CloudTrail

サービスリンクロールを手動で作成する必要はありません。組織記録や組織イベントデータストアを作成したり、 CloudTrail コンソールで委任管理者を追加したり、 AWS CLI または API CloudTrail 操作を使用したりすると、サービスにリンクされたロールがまだ存在しない場合は自動的に作成されます。

このサービスリンクロールを削除した後に再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。組織記録データストアまたは組織イベントデータストアを作成したり、 CloudTrail 委任管理者を追加したりすると、サービスにリンクされたロールが再び作成されます。

のサービスにリンクされたロールの編集 CloudTrail

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

のサービスにリンクされたロールを削除する CloudTrail

ロールを手動で削除する必要はありません。 AWSServiceRoleForCloudTrail がOrganizations AWS アカウント 組織から削除されると、AWSServiceRoleForCloudTrailそのロールはその組織から自動的に削除されます AWS アカウント。組織の管理アカウントの AWSServiceRoleForCloudTrail サービスリンクロールからポリシーをデタッチまたは削除するには、組織からアカウントを削除する必要があります。

IAM コンソール、、 AWS CLI または AWS API を使用して、サービスにリンクされたロールを手動で削除することもできます。そのためにはまず、サービスにリンクされたロールのリソースをクリーンアップする必要があります。その後で、そのロールを手動で削除できます。

> **Note**
>
> CloudTrail サービスがロールを使用していたときにリソースを削除しようとすると、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

AWSServiceRoleForCloudTrail ロールで使用されているリソースを削除するには、以下のいずれかの処理を行うことができます。

- 「Organizations」 AWS アカウント 内の組織からを削除します。
- 証跡を更新し、組織の証跡を停止させる必要があります。詳細については、「証跡の更新」を参照してください。
- イベントデータストアを組織のイベントデータストアではなくなるように更新します。詳細については、「コンソールでイベントデータストアを更新する」を参照してください。
- 証跡を削除します。詳細については、「証跡の削除」を参照してください。
- イベントデータストアを削除します。詳細については、「コンソールでイベントデータストアを削除する」を参照してください。

サービスにリンクされたロールを IAM で手動削除するには

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

サービスにリンクされたロールがサポートされているリージョン CloudTrail

CloudTrail は、 AWS リージョン CloudTrail 利用可能なすべての場所とOrganizations でのサービスにリンクされたロールの使用をサポートします。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。

AWS の管理ポリシー AWS CloudTrail

ユーザー、グループ、ロールにアクセス権限を追加するには、 AWS 自分でポリシーを作成するよりも管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに始めるには、 AWS 管理ポリシーを使用できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、IAM ユーザーガイドの「AWS 管理ポリシー」を参照してください。

AWS AWS サービスは管理ポリシーを維持および更新します。 AWS 管理ポリシーの権限は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。 AWS サービスは管理ポリシーから権限を削除しないため、ポリシーを更新しても既存の権限が損なわれることはありません。

さらに、 AWS 複数のサービスにまたがるジョブ機能の管理ポリシーもサポートされます。たとえば、ReadOnlyAccess AWS AWS 管理ポリシーはすべてのサービスとリソースへの読み取り専用アクセスを提供します。サービスが新しい機能を起動すると、 AWS 新しい操作やリソースに対する読み取り専用権限が追加されます。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「AWS のジョブ機能のマネージドポリシー」を参照してください。

AWS 管理ポリシー:**AWSCloudTrail_ReadOnlyAccess**

AWSCloudTrail_ReadOnlyAccessロールにポリシーがアタッチされたユーザ ID は、、トレイル CloudTrail、 CloudTrail Lake イベントデータストア`Get*`、`List*`、Lake `Describe*` クエリに対するアクションなど、読み取り専用のアクションを実行できます。

AWS 管理ポリシー:**AWSServiceRoleForCloudTrail**

CloudTrailServiceRolePolicyこのポリシーでは AWS CloudTrail 、ユーザーに代わって組織記録や組織イベントデータストアに対してアクションを実行することが許可されています。このポリシーには、 AWS Organizations 組織内の組織アカウントと委任管理者を記述および一覧表示するために必要な権限が含まれています。 AWS Organizations

このポリシーには、組織のイベントデータストアで Lake Federation AWS GlueAWS Lake Formation を無効にするために必要な権限と権限も含まれています。

このポリシーは、AWSServiceRoleForCloudTrail CloudTrail ユーザーに代わってアクションを実行できるサービスにリンクされたロールに添付されています。ユーザー、グループおよびロールにこのポリシーはアタッチできません。

CloudTrail AWS 管理ポリシーの更新

AWS の管理ポリシーの更新に関する詳細を表示します CloudTrail。このページへの変更に関する自動アラートを受け取るには、ページの RSS CloudTrail ドキュメント履歴 フィードを購読してください。

変更	説明	日付
CloudTrailServiceRolePolicy - 既存ポリシーへの更新	フェデレーションが無効になっている場合でも、組織のイベントデータストアで以下のアクションを実行できるように、ポリシーを更新しました。 • glue:DeleteTable • lakeformation:DeregisterResource	2023 年 11 月 26 日
AWSCloudTrail_ReadOnlyAccess – 既存ポリシーへの更新	CloudTrail AWSCloudTrailReadOnlyAccess ポリシーの名前をに変更しました。AWSCloudTrail_ReadOnlyAccess また、 CloudTrail ポリシー内の権限の範囲はアクションに限定されました。Amazon S3、 AWS KMS、AWS Lambda またはアクションのアクセス権限は含まれなくなりました。	2022 年 6 月 6 日
CloudTrail 変更の追跡を開始しました。	CloudTrail AWS 管理ポリシーの変更の追跡を開始しました。	2022 年 6 月 6 日

のコンプライアンス検証 AWS CloudTrail

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

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポート

されているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。

- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

のレジリエンス AWS CloudTrail

AWS AWS グローバルインフラストラクチャはリージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンには、物理的に分離され隔離された複数のアベイラビリティーゾーンがあり、低レイテンシー、高スループット、冗長性の高いネットワークで接続されています。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。 CloudTrail 地理的に離れた場所で特にログファイルを複製する必要がある場合は、トレイルの Amazon S3 バケットにクロスリージョンレプリケーションを使用できます。これにより、異なるリージョンのバケット間でオブジェクトを自動的に非同期コピーできます。 AWS

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

CloudTrail には、 AWS グローバルインフラストラクチャの他に、データの復元力とバックアップのニーズをサポートするいくつかの機能があります。

すべてのリージョンのイベントを記録するトレイルとイベントデータストア AWS

AWS すべてのリージョンに証跡を適用すると、 CloudTrail AWS リージョン AWS 作業中のパーティション内の他のすべてのリージョンに同じ構成の証跡が作成されます。 AWS 新しいリージョンを追加すると、そのトレイル設定は新しいリージョンに自動的に作成されます。

マルチリージョンイベントデータストアを作成すると、 CloudTrail AWS リージョン アカウント内のすべてのイベントが収集されます。

ログデータのバージョン管理、ライフサイクル設定、オブジェクトロック保護 CloudTrail

Amazon S3 CloudTrail バケットを使用してログファイルを保存するため、Amazon S3 が提供する機能を使用してデータの耐障害性とバックアップのニーズに対応することもできます。詳細については、「Amazon S3 の耐障害性」を参照してください。

のインフラストラクチャセキュリティ AWS CloudTrail

マネージドサービスとして、 AWS CloudTrail AWS グローバルネットワークセキュリティによって保護されています。 AWS AWS セキュリティサービスとインフラストラクチャの保護方法については、「AWS Cloud Security」を参照してください。 AWS インフラストラクチャセキュリティのベストプラクティスを使用して環境を設計するには、「Security Pillar AWS Well-Architected Framework におけるインフラストラクチャ保護」を参照してください。

AWS 公開されている API CloudTrail 呼び出しを使用してネットワーク経由でアクセスします。クライアントは以下をサポートする必要があります:

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

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

以下のセキュリティベストプラクティスでは、におけるインフラストラクチャのセキュリティにも対応しています CloudTrail。

- 証跡アクセス用の Amazon VPC エンドポイントを検討してください。
- Amazon S3 バケットアクセス用の Amazon VPC エンドポイントの検討 詳細については、「バケットポリシーによる VPC エンドポイントからのアクセスの制御」を参照してください。
- CloudTrail ログファイルを含むすべての Amazon S3 バケットを特定して監査します。タグを使用して、 CloudTrail CloudTrailトレイルとログファイルを含む Amazon S3 バケットの両方を識別することを検討してください。そうすれば、リソースとしてリソースグループを使用できます。CloudTrail 詳細については、「AWS Resource Groups」を参照してください。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましによって、混乱した代理人問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐために、 AWS には、アカウント内のリソースへのアクセス権が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールが用意されています。

aws:SourceArnaws:SourceAccountリソースポリシーではグローバル条件コンテキストキーとグローバル条件コンテキストキーを使用して、 AWS CloudTrail リソースに別のサービスを付与する権限を制限することをおすすめします。クロスサービスアクセスにリソースを 1 つだけ関連付けたい場合は、aws:SourceArn を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、aws:SourceAccount を使用します。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合は、aws:SourceArn グローバルコンテキスト条件キーを使用して、ARN の未知部分をワイルドカード (*) で表します。例えば、"arn:aws:cloudtrail:*:*AccountID*:trail/*" のように指定します。ワイルドカードを含める場合は、StringLike 条件演算子も使用する必要があります。

aws:SourceArn の値は、リソースを使用している証跡、イベントデータストア、またはチャネルの ARN でなければなりません。

次の例は、aws:SourceArnaws:SourceAccountおよびグローバル条件コンテキストキーを使用して、 CloudTrail 混乱を招く代理問題を防ぐ方法を示しています CloudTrail レイククエリ結果の Amazon S3 バケットポリシー。

のセキュリティ・ベスト・プラクティス AWS CloudTrail

AWS CloudTrail には、独自のセキュリティポリシーを策定して実装する際に考慮すべきセキュリティ機能が数多く用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお

客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

トピック

- CloudTrail 探偵セキュリティのベストプラクティス
- CloudTrail 予防的セキュリティのベストプラクティス

CloudTrail 探偵セキュリティのベストプラクティス

証跡の作成

AWS アカウント内のイベントを継続的に記録するには、証跡を作成する必要があります。追跡記録を作成しなくても、管理イベントの 90 CloudTrail 日間のイベント履歴情報がコンソールに表示されますが CloudTrail 、これは永続的な記録ではなく、発生する可能性のあるすべての種類のイベントに関する情報を提供するわけでもありません。進行中のレコード、および指定したすべてのイベントタイプを含むレコードの場合は、指定した Amazon S3 バケットにログファイルを配信する証跡を作成する必要があります。

CloudTrail データの管理に役立つように、管理イベントをすべて記録する証跡を 1 つ作成し AWS リージョン、Amazon S3 AWS Lambda バケットのアクティビティや関数など、リソースの特定のイベントタイプを記録する証跡を追加で作成することを検討してください。

以下に示しているのは、実行できるいくつかのステップです。

- AWS アカウントの証跡を作成します。
- 組織の証跡を作成します。

すべてに証跡を適用してください。 AWS リージョン

AWS アカウント内の IAM ID またはサービスによって取得されたイベントの完全な記録を取得するには、すべてのイベントをログに記録するように各トレイルを設定する必要があります。 AWS リージョンすべてのイベントをログに記録することで AWS リージョン、 AWS 発生したリージョンに関係なく、 AWS アカウントで発生したすべてのイベントが確実に記録されます。これには、AWS そのサービス固有のリージョンに記録されるグローバルサービスイベントのロギングが含まれます。すべてのリージョンに適用される証跡を作成すると、 CloudTrail 各リージョンのイベントを記録し、指定した S3 CloudTrail バケットにイベントログファイルを配信します。すべてのリージョンに適用される証跡を作成した後に AWS リージョンを追加すると、その新しいリージョンは自動的に追加

され、そこでのイベントはログに記録されます。 CloudTrail これはコンソールで証跡を作成するときのデフォルトオプションです。

以下に示しているのは、実行できるいくつかのステップです。

- AWS アカウントの証跡を作成します。
- 既存の証跡を更新して すべての AWS リージョンでイベントを記録します。
- の multi-region-cloud-trail-enabled ルールを使用して、作成されるすべての証跡が確実にイベントを記録できるように、継続的な検出制御を実装します。 AWS リージョン AWS Config

ログファイルの整合性を有効にする CloudTrail

検証されたログファイルは、セキュリティおよびフォレンシック調査で特に重要です。たとえば、検証されたログファイルを使用すると、ログファイル自体が変更されていないこと、または特定の IAM ID の認証情報が特定の API アクティビティを実行したことを確実にアサートできます。 CloudTrail ログファイルの整合性検証プロセスでは、ログファイルが削除または変更されたかどうかを確認したり、特定の期間にログファイルがアカウントに配信されなかったことを確認したりすることもできます。 CloudTrail ログファイルの整合性検証では、業界標準のアルゴリズムを使用します。ハッシュには SHA-256、デジタル署名には RSA で SHA-256 を使用します。そのため、ログファイルを検出せずに変更、削除、または偽造することは計算上不可能です。 CloudTrail詳細については、「検証の有効化とファイルの検証」を参照してください。

Amazon CloudWatch ログと統合

CloudWatch ログを使用すると、によってキャプチャされた特定のイベントを監視し、 CloudTrailアラートを受信できます。 CloudWatch ログに送信されるイベントは、トレイルによって記録されるように設定されているイベントなので、監視したいイベントタイプ (管理イベントやデータイベント) を記録するように 1 つまたは複数のトレイルを設定していることを確認してください。

たとえば、主要なセキュリティイベントやネットワーク関連の管理イベント (AWS Management Console サインイン失敗イベントなど) を監視できます。

以下に示しているのは、実行できるいくつかのステップです。

- CloudWatchの ログ統合の例を確認してください。 CloudTrail
- CloudWatch Logs にイベントを送信するようにトレイルを設定します。
- の cloud-trail-cloud-watch-logs-enabled ルールを使用して、 CloudWatch すべてのトレイルが監視対象のイベントをログに送信するように継続的な検出制御を実施することを検討してください。 AWS Config

Amazon 使用 GuardDuty

Amazon GuardDuty は、アカウント、コンテナ、ワークロード、 AWS および環境内のデータを保護するのに役立つ脅威検出サービスです。機械学習 (ML) モデルと異常/脅威検出機能を使用して、GuardDuty さまざまなログソースを継続的に監視し、環境内の潜在的なセキュリティリスクや悪意のあるアクティビティを特定し、優先順位を付けます。

たとえば、 GuardDuty インスタンス起動ロールを通じて Amazon EC2 インスタンス専用に作成された認証情報が、内部の別のアカウントから使用されていることを検出した場合、認証情報が漏洩する可能性があることを検出します。 AWS詳細については、Amazon GuardDuty ユーザーガイドを参照してください。

使用アイテム AWS Security Hub

を使用してAWS Security Hub、 CloudTrail セキュリティのベストプラクティスに関連するの使用状況を監視してください。Security Hub は、検出セキュリティコントロールを使用してリソース設定とセキュリティ標準を評価し、お客様がさまざまなコンプライアンスフレームワークに準拠できるようサポートします。Security Hub CloudTrail を使用してリソースを評価する方法について詳しくは、『AWS Security Hub ユーザーガイド』の「AWS CloudTrail コントロール」を参照してください。

CloudTrail 予防的セキュリティのベストプラクティス

以下のベストプラクティスは、セキュリティインシデントの防止に役立ちます。 CloudTrail

専有および一元化された Amazon S3 バケットへのログ

CloudTrail ログファイルは IAM ID AWS またはサービスによって実行されたアクションの監査ログです。これらのログの整合性、完全性、および可用性は、フォレンジックおよび監査目的にとって非常に重要です。専有および一元化された Amazon S3 バケットにログに記録することで、厳格なセキュリティ管理、アクセス、および役割分担を実施できます。

以下に示しているのは、実行できるいくつかのステップです。

- AWS ログアーカイブアカウントとして別のアカウントを作成します。を使用する場合は AWS Organizations、このアカウントを組織に登録し、AWS 組織内のすべてのアカウントのデータを記録する組織証跡を作成することを検討してください。
- OrOrganizations izationsを使用していないが、 AWS 複数のアカウントのデータを記録したい場合は、このログアーカイブアカウントにアクティビティを記録するためのトレイルを作成します。こ

のアカウントへのアクセスを、アカウントおよび監査データへのアクセス権限を有する信頼された管理ユーザーだけに制限します。

- 証跡の作成の一環として、それが組織の証跡であろうと、 AWS 単一アカウントの証跡であろうと、この証跡のログファイルを保存する専用の Amazon S3 バケットを作成します。
- 複数のアカウントのアクティビティを記録する場合は、 AWS AWS アカウントアクティビティを記録したいすべてのアカウントのログファイルの記録と保存を許可するようにバケットポリシーを変更します。 AWS
- 組織証跡を使用していない場合は、ログアーカイブアカウントで Amazon S3 バケットを指定して、すべての AWS アカウントで証跡を作成します。

AWS KMS マネージドキーによるサーバー側の暗号化を使用してください。

デフォルトでは、S3 CloudTrail バケットに配信されるログファイルは KMS キーによるサーバー側の暗号化 (SSE-KMS) を使用して暗号化されます。で SSE-KMS を使用するには CloudTrail、KMS キーとも呼ばれるキーを作成して管理します。AWS KMS key

> **Note**
>
> SSE-KMS とログファイルの検証を使用していて、SSE-KMS で暗号化されたファイルのみを許可するように Amazon S3 バケットポリシーを変更した場合は、次の例のポリシー行に示すように、バケットポリシーを AES256 暗号化を特に許可するように変更しない限り、そのバケットを活用する証跡を作成することはできません。
>
> ```
> "StringNotEquals": { "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"] }
> ```

以下に示しているのは、実行できるいくつかのステップです。

- SSE-KMS を使用してログファイルを暗号化する利点を確認します。
- ログファイルの暗号化に使用する KMS を作成します。
- 証跡のログファイル暗号化を設定します。
- のルールを使用して、すべてのトレイルが SSE-KMS でログファイルを暗号化できるように、継続的な検出制御を実装することを検討してください。cloud-trail-encryption-enabled AWS Config

デフォルトの Amazon SNS トピックポリシーに条件キーを追加する

Amazon SNS に通知を送信するようにトレイルを設定すると、SNS CloudTrail トピックへのコンテンツの送信を許可するポリシーステートメントが SNS CloudTrail トピックアクセスポリシーに追加されます。セキュリティのベストプラクティスとして、ポリシーステートメントに aws:SourceArn (またはオプションでaws:SourceAccount) 条件キーを追加することをお勧めします。 CloudTrail これにより、SNS トピックへの不正なアカウントアクセスを防止できます。詳細については、「の Amazon SNS トピックポリシー CloudTrail」を参照してください。

ログファイルを保存する Amazon S3 バケットへの最小特権のアクセス権限を実装する

CloudTrail 指定した Amazon S3 バケットにログイベントを追跡します。これらのログファイルには、IAM ID とサービスによって実行されたアクションの監査ログが含まれます。 AWS これらのログファイルの整合性と完全性は、監査とフォレンジック用に非常に重要です。整合性を確保するために、 CloudTrail ログファイルの保存に使用される Amazon S3 バケットへのアクセスを作成または変更するときは、最小権限の原則に従う必要があります。

次のステップを実行します。

- ログファイルを保存するすべてのバケットの Amazon S3 バケットポリシーを確認し、必要に応じてそれを調整して不要なアクセスを削除します。このバケットポリシーは、 CloudTrail コンソールを使用して証跡を作成すると自動的に生成されますが、手動で作成して管理することもできます。
- セキュリティのベストプラクティスとして、バケットポリシーに aws:SourceArn 条件キーを手動で追加してください。 詳細については、「の Amazon S3 バケットポリシー CloudTrail」を参照してください。
- 同じ Amazon S3 バケットを使用して複数のアカウントのログファイルを保存する場合は、 AWS 複数のアカウントのログファイルを受信するためのガイダンスに従ってください。
- 組織証跡を使用している場合は、組織証跡のガイダンスに従っていることを確認し、を使用して組織の証跡を作成する AWS Command Line Interface の組織証跡の Amazon S3 バケットのポリシー例を確認してください。
- Amazon S3 セキュリティのドキュメントとバケットを保護するためのチュートリアルの例を確認してください。

ログファイルを保存する Amazon S3 バケットで MFA Delete を有効にする

多要素認証 (MFA)を設定すると、バケットのバージョニング状態を変更しようとしたり、バケット内のオブジェクトのバージョンを削除しようとすると、追加の認証が必要になります。これにより、ユーザーが Amazon S3 オブジェクトを永続的に削除する権限を持つ IAM ユーザーのパスワードを取得した場合でも、ログ ファイルを危険にさらす可能性のある操作を防止できます。

以下に示しているのは、実行できるいくつかのステップです。

- Amazon Simple Storage Service ユーザーガイドの MFA Delete のガイダンスを確認します。
- MFA を要求する Amazon S3 バケットポリシーの追加します

> **Note**
>
> ライフサイクル設定で MFA 削除を使用することはできません。ライフサイクル設定と、これを使用して他の設定を操作する方法の詳細については、Amazon Simple Storage Service ユーザーガイドの「ライフサイクルとその他のバケット設定」を参照してください。

ログファイルを保存する Amazon S3 バケットにオブジェクトライフサイクル管理を設定する

CloudTrail 証跡のデフォルトでは、記録用に設定された Amazon S3 バケットにログファイルを無期限に保管します。Amazon S3 オブジェクトライフサイクル管理ルールを使用して、独自の保持ポリシーを定義し、ビジネスおよび監査のニーズをより適切に満たせるようになります。たとえば、1 年以上経過しているログファイルを Amazon Glacier にアーカイブしたり、一定の時間が経過した後にログファイルを削除できます。

> **Note**
>
> 多要素認証 (MFA) が有効なバケットのライフサイクル設定はサポートされていません。

ポリシーへのアクセスを制限してください。 AWSCloudTrail_FullAccess

AWSCloudTrail_FullAccessこのポリシーを適用したユーザーは、アカウント内の最も機密性が高く重要な監査機能を無効にしたり、再構成したりできます。 AWS このポリシーは、アカウント内の IAM ID に共有されたり、広く適用されたりすることを意図したものではありません。 AWS このポリシーの適用は、アカウント管理者として行動する予定のできるだけ少数の個人に限定してください。 AWS

CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)

デフォルトでは、 CloudTrail バケットに配信されるログファイルは KMS キーによるサーバー側の暗号化 (SSE-KMS) を使用して暗号化されます。SSE-KMS 暗号化を有効にしない場合、ログは SSE-S3 暗号化を使用して暗号化されます。

> **Note**
>
> サーバー側の暗号化を有効にすると SSE-KMS、を使用してログファイルが暗号化されますが、ダイジェストファイルは暗号化されません。ダイジェストファイルは、Amazon S3 で管理された暗号化キー (SSE-S3) を使用して暗号化されます。
> S3 バケット Key で既存の S3 バケットを使用している場合、 CloudTrail アクションとを使用するにはキーポリシーでアクセス権限を許可する必要があります。 AWS KMS `GenerateDataKey` `DescribeKey`もし `cloudtrail.amazonaws.com` にキーポリシーの許可が与えられていない場合、証跡の作成や更新は行なえません。

で SSE-KMS を使用するには CloudTrail、KMS キー (とも呼ばれます) を作成して管理します。AWS KMS keyどのユーザーがログファイルの暗号化と復号化にキーを使用できるかを決定するポリシーをキーにアタッチします。 CloudTrail 復号は、S3 を通じてシームレスです。 CloudTrail キーの権限を持つユーザーがログファイルを読み取ると、S3 が復号化を管理し、権限のあるユーザーは暗号化されていない形式のログファイルを読み取ることができます。

このアプローチには以下の利点があります。

- KMS キー暗号化キーを自分で作成して管理することができます。
- 単一の KMS キーを使用して、すべてのリージョンの複数のアカウントのログファイルを暗号化および復号できます。
- ログファイルの暗号化と復号に誰がキーを使用できるかを制御できます。 CloudTrail 要件に応じて、組織のユーザーにキーのアクセス権限を割り当てることができます。
- セキュリティが強化されました。この機能では、ログファイルを読み取るために、次のアクセス許可が必要です。
  - ユーザーには、ログファイルを含むバケットに対する S3 の読み取り権限が必要です。
  - ユーザーには、KMS キーポリシーによるアクセス許可の復号化を許可するポリシーまたは役割も適用する必要があります。

- S3 は KMS キーの使用を許可されたユーザーからのリクエストに応じてログファイルを自動的に復号化するため、ログファイルの SSE-KMS 暗号化は、 CloudTrail ログデータを読み取るアプリケーションと下位互換性があります。 CloudTrail

> **Note**
>
> 選択する KMS キーは、ログファイルを受け取る Amazon S3 AWS バケットと同じリージョンで作成する必要があります。例えば、ログファイルが 米国東部 (オハイオ) リージョンのバケットに保存される場合は、そのリージョンで作成された KMS キーを作成または選択する必要があります。Amazon S3 バケットのリージョンを確認するには、Amazon S3 コンソールでそのプロパティを調べます。

ログファイルの暗号化を有効にする

> **Note**
>
> CloudTrail コンソールで KMS キーを作成すると、必要な KMS CloudTrail キーポリシーセクションが自動的に追加されます。IAM AWS CLI コンソールでキーを作成した場合や、必要なポリシーセクションを手動で追加する必要がある場合は、以下の手順に従ってください。

CloudTrail ログファイルの SSE-KMS 暗号化を有効にするには、以下の大まかな手順を実行します。

1. KMS キーを作成します。

   - で KMS キーを作成する方法については AWS Management Console、『開発者ガイド』の「キーの作成」を参照してください。AWS Key Management Service
   - を使用して KMS キーを作成する方法については AWS CLI、「create-key」を参照してください。

   > **Note**
   >
   > 選択する KMS キーは、ログファイルを受け取る S3 バケットと同じリージョンにある必要があります。S3 バケットのリージョンを確認するには、S3 コンソールでバケットのプロパティを調べます。

2. CloudTrail ログファイルの暗号化とユーザーによる復号化を有効にするポリシーセクションをキーに追加します。

   - ポリシーに含める内容の詳細については、「AWS KMS の主要ポリシーの設定 CloudTrail」を参照してください。

     > **Warning**
     >
     > ログファイルを読み取る必要があるすべてのユーザーに対して、ポリシーに復号のアクセス権限を含めるようにしてください。証跡の設定にキーを追加する前にこの手順を実行しない場合、復号のアクセス権限のないユーザーは、それらにアクセス権限を付与するまで暗号化されたファイルを読み取ることができません。

   - IAM コンソールを使用したポリシーの編集の詳細については、AWS Key Management Service デベロッパーガイドの「キーポリシーの編集」を参照してください。
   - を使用して KMS キーにポリシーをアタッチする方法については、を参照してください。 AWS CLIput-key-policy

3. ポリシーを変更した KMS キーを使用するようにトレイルを更新してください。 CloudTrail

   - CloudTrail コンソールを使用してトレイル設定を更新するには、を参照してくださいKMS キーを使用するようにリソースを更新する。
   - を使用してトレイル設定を更新するには AWS CLI、を参照してください CloudTrail による口グファイルの暗号化の有効化と無効化 AWS CLI。

CloudTrail AWS KMS マルチリージョンキーもサポートしています。マルチリージョンキーの詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

次のセクションでは、KMS キーポリシーと併用する必要があるポリシーセクションについて説明します。 CloudTrail

KMS キーを作成するためのアクセス許可の付与

`AWSKeyManagementServicePowerUser`ポリシーを使用して作成する権限をユーザーに付与できます。 AWS KMS key

KMS キーを作成するためのアクセス許可を付与するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 権限を付与するグループまたはユーザーを選択します。
3. [Permissions]、[Attach Policy] の順に選択します。
4. AWSKeyManagementServicePowerUser を検索し、ポリシーを選択して、[ポリシーのアタッチ] を選択します。

   これで、ユーザーは KMS キーを作成するアクセス許可を持つようになりました。ポリシー作成の詳細については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

AWS KMS の主要ポリシーの設定 CloudTrail

は次の 3 AWS KMS key つの方法で作成できます。

- CloudTrail コンソール
- AWS 管理コンソール
- は AWS CLI

> **Note**
>
> CloudTrail コンソールで KMS キーを作成すると、必要な KMS CloudTrail キーポリシーが自動的に追加されます。ポリシーステートメントを手動で追加する必要はありません。「コンソールで作成されたデフォルト KMS キーポリシー CloudTrail 」を参照してください。

AWS 管理またはで KMS キーを作成する場合は AWS CLI、キーにポリシーセクションを追加して使用できるようにする必要があります。 CloudTrailポリシーでは、 CloudTrail キーを使用してログファイルとイベントデータストアを暗号化し、指定したユーザが暗号化されていない形式のログファイルを読み取れるようにする必要があります。

以下のリソースを参照してください。

- を使用して KMS キーを作成する方法については AWS CLI、「create-key」を参照してください。
- の KMS キーポリシーを編集するには CloudTrail、『開発者ガイド』の「キーポリシーの編集」を参照してください。AWS Key Management Service

- CloudTrail 使用方法の技術的な詳細については AWS KMS、『AWS Key Management Service 開発者ガイド』 AWS KMSの「AWS CloudTrail 使用方法」を参照してください。

で使用するために必要な KMS キーポリシーセクション CloudTrail

AWS 管理コンソールまたはで KMS キーを作成した場合 AWS CLI、KMS キーポリシーを使用するには、少なくとも KMS キーポリシーに次のステートメントを追加する必要があります。 CloudTrail

トピック

- 証跡用の KMS キーポリシーの必須要素
- イベントデータストア用の KMS キーポリシーの必須要素

証跡用の KMS キーポリシーの必須要素

1. CloudTrail ログ暗号化権限を有効にします。暗号化権限の付与 を参照してください。
2. CloudTrail ログ復号権限を有効にします。復号の権限を付与する を参照してください。S3 バケットキーで既存の S3 バケットを使用している場合は、SSE-KMS 暗号化を有効にした証跡を作成または更新するために、`kms:Decrypt` アクセス許可が必要です。
3. KMS CloudTrail キープロパティを記述できるようにします。KMS CloudTrail キープロパティを記述できるようにする を参照してください。

セキュリティのベストプラクティスとして、KMS キーポリシーに `aws:SourceArn` 条件キーを追加します。IAM `aws:SourceArn` グローバル条件キーは、特定の 1 つまたは複数のトレイルにのみ KMS CloudTrail キーを使用するようにするのに役立ちます。`aws:SourceArn` の値は、常に KMS キーを使用している証跡 ARN (または証跡 ARN の配列) です。既存の証跡用の KMS キーポリシーに `aws:SourceArn` 条件キーを必ず追加してください。

`aws:SourceAccount` 条件キーもサポートされていますが、推奨されません。`aws:SourceAccount` の値は、証跡の所有者のアカウント ID、または組織の証跡の場合は管理アカウント ID です。

> **Important**
>
> 新しいセクションを KMS キーポリシーに追加するときは、ポリシー内の既存のセクションを変更しないでください。

トレイルで暗号化が有効になっていて、KMS キーが無効になっているか、KMS キーポリシーが正しく設定されていないと、ログを配信できません。 CloudTrail CloudTrail

イベントデータストア用の KMS キーポリシーの必須要素

1. CloudTrail ログ暗号化権限を有効にします。暗号化権限の付与 を参照してください。
2. CloudTrail ログ復号権限を有効にします。復号の権限を付与する を参照してください。
3. KMS キーを使用してイベントデータストアデータを暗号化および復号するための許可をユーザーおよびロールに付与します。

   イベントデータストアを作成して KMS キーで暗号化する場合、または KMS キーで暗号化するイベントデータストアに対してクエリを実行する場合は、KMS キーに対する書き込みアクセス権が必要です。KMS キーポリシーには CloudTrail、イベントデータストアで操作 (クエリなど) を実行するユーザーがアクセスでき、KMS キーを管理できる必要があります。
4. KMS CloudTrail キープロパティを記述できるようにする。KMS CloudTrail キープロパティを記述できるようにする を参照してください。

`aws:SourceArn` および `aws:SourceAccount` 条件キーは、イベントデータストアの KMS キーポリシーではサポートされていません。

> **Important**
>
> 新しいセクションを KMS キーポリシーに追加するときは、ポリシー内の既存のセクションを変更しないでください。
> イベントデータストアで暗号化が有効になっていて、KMS キーが無効化または削除されている場合、または KMS キーポリシーが正しく設定されていないと CloudTrail、 CloudTrailイベントデータストアにイベントを配信できません。

暗号化権限の付与

Example CloudTrail 特定のアカウントに代わってログを暗号化することを許可する

CloudTrail KMS キーを使用して特定のアカウントに代わってログを暗号化するには、明示的な権限が必要です。アカウントを指定するには、KMS キーポリシーに次の必須のステートメントを追加して、*account-id*、*region*、および *trailName* を設定に適切な値に置き換えま

す。EncryptionContextセクションにアカウント ID を追加して、それらのアカウントが KMS CloudTrail キーを使用してログファイルを暗号化できるようにすることができます。

セキュリティのベストプラクティスとして、証跡用の KMS キーポリシーに aws:SourceArn 条件キーを追加します。IAM aws:SourceArn グローバル条件キーは、特定の 1 つまたは複数のトレイルにのみ KMS CloudTrail キーを使用するようにするのに役立ちます。

```
{
   "Sid": "Allow CloudTrail to encrypt logs",
   "Effect": "Allow",
   "Principal": {
       "Service": "cloudtrail.amazonaws.com"
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
         },
         "StringLike": {
             "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws:cloudtrail:*:account-
id:trail/*"
         }
    }
}
```

CloudTrail Lake イベントデータストアログの暗号化に使用される KMS キーのポリシーでは、条件キーまたはを使用することはできません。aws:SourceArn aws:SourceAccountイベントデータストアの KMS キーポリシーの例を次に示します。

```
{
    "Sid": "Allow CloudTrail to encrypt event data store",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

Example

次のポリシーステートメントの例は、別のアカウントが KMS キーを使用してログを暗号化する方法を示しています。 CloudTrail

シナリオ

- KMS キーは、アカウント *111111111111* にあります。
- 自分も アカウント *222222222222* も両方ともログを暗号化します。

このポリシーでは、キーで暗号化するアカウントを 1 つ以上追加します。 CloudTrail EncryptionContextこれにより、 CloudTrail キーを使用してログを暗号化できるのは、指定したアカウントのログのみに制限されます。アカウント *222222222222* のルートにログを暗号化する権限を与えると、アカウント管理者に権限を委任して、必要な権限をそのアカウント内の他のユーザーに暗号化します。アカウント管理者は、これらの IAM ユーザーに関連するポリシーを変更することでこれを行います。

セキュリティのベストプラクティスとして、KMS キーポリシーに aws:SourceArn 条件キーを追加します。IAM aws:SourceArn グローバル条件キーは、指定された証跡にのみ KMS CloudTrail キーを使用するようにするのに役立ちます。この条件は、イベントデータストアの KMS キーポリシーではサポートされていません。

KMS キーポリシーステートメント:

```
{
  "Sid": "Enable CloudTrail encrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:GenerateDataKey*",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:cloudtrail:arn": [
        "arn:aws:cloudtrail:*:111111111111:trail/*",
        "arn:aws:cloudtrail:*:222222222222:trail/*"
      ]
    },
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
```

```
    }
  }
}
```

で使用する KMS キーポリシーの編集について詳しくは CloudTrail、『開発者ガイド』の「キーポリシーの編集」を参照してください。 AWS Key Management Service

復号の権限を付与する

KMS CloudTrail キーを設定に追加する前に、復号化権限を必要とするすべてのユーザーに復号化権限を付与することが重要です。暗号化の許可はあっても、復号の許可がないユーザーは、暗号化されたログを読み取ることはできません。S3 バケットキーで既存の S3 バケットを使用している場合は、SSE-KMS 暗号化を有効にした証跡を作成または更新するために、`kms:Decrypt` アクセス許可が必要です。

ログ復号権限を有効にします CloudTrail 。

キーのユーザーには、暗号化されたログファイルを読み取るための明示的な権限を付与する必要があります。 CloudTrail ユーザーが暗号化されたログを読み取れるようにするには、次の必要なステートメントを KMS キーポリシーに追加し、`Principal` セクションを変更して、KMS キーを使用して復号できるすべてのプリンシパル のための行を追加します。

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account-id:user/username"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

以下は、 CloudTrail サービスプリンシパルがトレイルログを復号化できるようにするために必要なポリシーの例です。

```
{
```

```
      "Sid": "Allow CloudTrail to decrypt a trail",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

CloudTrail Lake イベントデータストアで使用される KMS キーの復号化ポリシーは次のようなものです。Principal の値として指定されたユーザーまたはロールの ARN には、イベントデータストアの作成または更新、クエリの実行、またはクエリ結果の取得を行うための復号許可が必要です。

```
{
      "Sid": "Enable user key permissions for event data stores"
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::account-id:user/username"
      },
      "Action": [
          "kms:Decrypt",
          "kms:GenerateDataKey"
      ],
      "Resource": "*"
  }
```

以下は、 CloudTrail サービスプリンシパルがイベントデータストアのログを復号化できるようにするために必要なポリシーの例です。

```
{
      "Sid": "Allow CloudTrail to decrypt an event data store",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

アカウントのユーザーが KMS キーで証跡ログを復号することを許可する

例

このポリシーステートメントは、アカウント内のユーザー、またはロールがキーを使用してアカウントの S3 バケットの暗号化されたログを読み取ることを許可する方法を示しています。

Example シナリオ

- KMS キー、S3 バケット、および IAM ユーザーの Bob は、アカウント *111111111111* にあります。
- IAM ユーザーの Bob に S3 CloudTrail バケット内のログを復号する権限を付与します。

キーポリシーでは、IAM ユーザー Bob CloudTrail のログ復号権限を有効にします。

KMS キーポリシーステートメント:

```
{
  "Sid": "Enable CloudTrail log decrypt permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111111111111:user/Bob"
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

他のアカウントのユーザーが KMS キーで証跡ログを復号することを許可する

他のアカウントのユーザーが KMS キーを使用して証跡ログを復号することを許可しつつ、イベントデータストアログは復号できないようにすることができます。キーポリシーに必要な変更は、S3 バケットが自分のアカウントにあるか、または別のアカウントにあるかによって異なります。

別のアカウントのバケットのユーザーがログを復号する権限を与える

例

このポリシーステートメントは、別のアカウントの IAM ユーザーまたはロールに、キーを使用して、他のアカウントの S3 バケットから暗号化されたログを読み取る権限を与える方法を示しています。

シナリオ

- KMS キーは、アカウント *111111111111* にあります。
- IAM ユーザーである Alice と S3 バケットは、アカウント *222222222222* にあります。

この場合、 CloudTrail アカウントでログを復号する権限を付与し*222222222222*、アカウントにあるキーを使用する権限を Alice の IAM ユーザーポリシーに付与します。*KeyA 111111111111*

KMS キーポリシーステートメント:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Alice の IAM ユーザーポリシーステートメント:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-west-2:111111111111:key/KeyA"
    }
  ]
}
```

別のアカウントのユーザーがバケットから証跡ログを復号することを許可する

Example

このポリシーは、S3 バケットから暗号化されたログを読み取るために、別のアカウントがキー使用する方法を示しています。

Example シナリオ

- KMS キーと S3 バケットは、アカウント *111111111111* にあります。
- バケットからログを読み取るユーザーは、アカウント *222222222222* にあります。

このシナリオを有効にするには、自分のアカウントの IAM ロールの復号化権限を有効にし、CloudTrailReadRole他のアカウントにそのロールを引き受ける権限を付与します。

KMS キーポリシーステートメント:

```
{
  "Sid": "Enable encrypted CloudTrail log read access",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::11111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRoleトラスト・エンティティ・ポリシー・ステートメント:

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "Allow CloudTrail access",
```

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::222222222222:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

で使用する KMS キーポリシーの編集については CloudTrail、『AWS Key Management Service 開発者ガイド』の「キーポリシーの編集」を参照してください。

KMS CloudTrail キープロパティを記述できるようにする

CloudTrail KMS キーのプロパティを記述できる必要があります。この機能を有効にするには、以下の必要なステートメントをそのまま KMS キーポリシーに追加します。このステートメントでは、CloudTrail 指定した他の権限以外の権限は付与されません。

セキュリティのベストプラクティスとして、KMS キーポリシーに aws:SourceArn 条件キーを追加します。IAM aws:SourceArn グローバル条件キーは、特定の 1 つまたは複数のトレイルにのみ KMS CloudTrail キーを使用するようにするのに役立ちます。

```
{
  "Sid": "Allow CloudTrail access",
  "Effect": "Allow",
  "Principal": {
    "Service": "cloudtrail.amazonaws.com"
  },
  "Action": "kms:DescribeKey",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "StringEquals": {
        "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-name"
    }
  }
}
```

KMS キーポリシーの編集の詳細については、AWS Key Management Service デベロッパーガイドの「キーポリシーの編集」を参照してください。

コンソールで作成されたデフォルト KMS キーポリシー CloudTrail

AWS KMS key CloudTrail コンソールでを作成すると、次のポリシーが自動的に作成されます。このポリシーでは、次の権限が付与されます。

- KMS キーの AWS アカウント (root) 権限を許可します。
- KMS キーのログファイルを暗号化し、KMS キーを記述できます CloudTrail 。
- 指定されたアカウント内のすべてのユーザーがログファイルを復号する権限を付与する
- 指定されたアカウント内のすべてのユーザーが KMS キーの KMS エイリアスを作成する権限を付与する
- 証跡を作成したアカウントのアカウント ID に対するクロスアカウントログ復号化を有効にします。

トピック

Lake CloudTrail イベントデータストア用のデフォルト KMS キーポリシー

以下は、 CloudTrail Lake AWS KMS key のイベントデータストアで使用する用に作成されたデフォルトポリシーです。

```
{
      "Version": "2012-10-17",
      "Id": "Key policy created by CloudTrail",
      "Statement": [
        {
          "Sid": "The key created by CloudTrail to encrypt event data stores. Created
 ${new Date().toUTCString()}",
          "Effect": "Allow",
          "Principal": {
            "Service": "cloudtrail.amazonaws.com"
          },
          "Action": [
            "kms:GenerateDataKey",
            "kms:Decrypt"
          ],
          "Resource": "*"
        },
```

```
        {
          "Sid": "Enable IAM user permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::account-id:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
            "AWS" : "arn:aws:sts::account-id:role-arn"
          },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
        }
      ]
    }
```

証跡のデフォルト KMS キーポリシー

トレイルで使用する、用に作成されたデフォルトポリシーは次のとおりです。 AWS KMS key

> **Note**
>
> このポリシーには、クロスアカウントが KMS キーを使用してログファイルを復号することを許可するステートメントが含まれています。

```
{
    "Version": "2012-10-17",
    "Id": "Key policy created by CloudTrail",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": [
                    "arn:aws:iam::account-id:root",
                    "arn:aws:iam::account-id:user/username"
                ]
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow CloudTrail to encrypt logs",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:GenerateDataKey*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:region:account-id:trail/trail-
name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow CloudTrail to describe key",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
             },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow principals in the account to decrypt log files",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": [
                "kms:Decrypt",
```

```
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
"arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        },
        {
            "Sid": "Allow alias creation during setup",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
             },
            "Action": "kms:CreateAlias",
            "Resource": "arn:aws:kms:region:account-id:key/key-id",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "ec2.region.amazonaws.com",
                    "kms:CallerAccount": "account-id"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "account-id"
                },
                "StringLike": {
```

```
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:account-id:trail/*"
                }
            }
        }
    ]
}
```

KMS キーを使用するようにリソースを更新する

AWS CloudTrail コンソールで、 AWS Key Management Service キーを使用するようにトレイルまたはイベントデータストアを更新します。独自の KMS キーを使用すると、 AWS KMS 暗号化と復号化にコストがかかることに注意してください。詳細については、「AWS Key Management Service の料金」を参照してください。

トピック

- KMS キーを使用するように証跡を更新する
- KMS キーを使用するようにイベントデータストアを更新する

KMS キーを使用するように証跡を更新する

変更した Trail を使用するように証跡を更新するには CloudTrail、コンソールで次の手順を実行します。 AWS KMS key CloudTrail

> **Note**
>
> 以下の手順を使用して証跡を更新すると、ログファイルが暗号化されますが、SSE-KMS を使用したダイジェストファイルは暗号化されません。ダイジェストファイルは、Amazon S3 で管理された暗号化キー (SSE-S3) を使用して暗号化されます。
> S3 バケットキーのある既存の S3 バケットを使用している場合、 CloudTrail AWS KMS `GenerateDataKey`アクションとを使用するにはキーポリシーでアクセス権限が許可されている必要がありますDescribeKey。もし `cloudtrail.amazonaws.com` にキーポリシーの許可が与えられていない場合、証跡の作成や更新は行なえません。

を使用してトレイルを更新するには AWS CLI、を参照してください CloudTrail によるログファイルの暗号化の有効化と無効化 AWS CLI。

KMS キーを使用するために証跡を更新するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ CloudTrail のコンソールを開きます。
2. [Trails] を選択し、証跡名を選択します。
3. [General details] で、[Edit] を選択します。
4. [Log file SSE-KMS encryption] (ログファイルの SSE-KMS 暗号化) で、SSE-S3 暗号化を使用する代わりに SSE-KMS 暗号化を使用してログファイルを暗号化する場合は、[Enabled] (有効) を選択します。デフォルトは [Enabled] です。SSE-KMS 暗号化を有効にしない場合、ログは SSE-S3 暗号化を使用して暗号化されます。SSE-KMS 暗号化の詳細については、「(SSE-KMS) でのサーバー側の暗号化の使用」を参照してください。 AWS Key Management Service SSE-S3 暗号化の詳細については、「Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (SSE-S3) の使用」を参照してください。

   [Existing] を選択して AWS KMS keyの証跡を更新します。ログファイルを受け取る S3 バケットと同じリージョンにある KMS キーを選択します。S3 バケットのリージョンを確認するには、S3 コンソールでそのプロパティを確認します。

   > **Note**
   >
   > 別のアカウントのキーの ARN を入力することもできます。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。キーポリシーでは、 CloudTrail キーを使用してログファイルを暗号化することを許可し、指定したユーザーが暗号化されていない形式のログファイルを読み取ることを許可する必要があります。キーポリシーを手動で編集する方法については、AWS KMS の主要ポリシーの設定 CloudTrail を参照してください。

   [AWS KMS Alias] に、 CloudTrailポリシーを変更して使用するエイリアスをという形式で指定します。`alias/`*`MyAliasName`*詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。

   エイリアス名、ARN、グローバルに一意のキー ID を入力できます。KMS キーが、別のアカウントに属している場合は、そのキーポリシーに使用可能なアクセス権限があることを確認します。値は、以下の形式のいずれかになります。

   - エイリアス名: `alias/`*`MyAliasName`*

- エイリアス ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
- キー ARN: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
- グローバルに一意のキー ID: `12345678-1234-1234-1234-123456789012`

5. [証跡の作成] を選択します。

> **Note**
>
> 選択した KMS キーが無効になっているか、削除が保留されている場合は、その KMS キーで証跡を保存することはできません。KMS キーを有効にするか、別の CMK を選択できます。詳細については、AWS Key Management Service デベロッパーガイドの「キー状態: KMS キーへの影響」を参照してください。

KMS キーを使用するようにイベントデータストアを更新する

変更したデータストアを使用するようにイベントデータストアを更新するには CloudTrail、CloudTrail コンソールで次の手順を実行します。 AWS KMS key

を使用してイベントデータストアを更新するには AWS CLI、を参照してくださいイベントデータストアを次のように更新します。 AWS CLI。

> **Important**
>
> KMS キーを無効化または削除するか、 CloudTrail キーに対する権限を削除すると、イベントデータストアにイベントを取り込むことができなくなり、キーで暗号化されたイベントデータストア内のデータをユーザーがクエリすることもできなくなります。 CloudTrail イベントデータストアを KMS キーに関連付けた後に、その KMS キーを削除または変更することはできません。イベントデータストアで使用している KMS キーを無効化または削除する前に、イベントデータストアを削除またはバックアップしてください。

KMS キーを使用するようにイベントデータストアを更新するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/ のコンソールを開きます。 CloudTrail

2. ナビゲーションペインで、[Lake] の [Event data stores] (イベントデータストア) を選択します。更新するイベントデータストアを選択します。
3. [General details] で、[Edit] を選択します。
4. [Encryption] (暗号化) で、暗号化が既に有効になっているのでなければ、[Use my own AWS KMS key] を選択して、自身の KMS キーでログファイルを暗号化します。

   KMS キーでイベントデータストアを更新するには、[Existing] (既存) を選択します。イベントデータストアと同じリージョンにある KMS キーを選択します。別のアカウントからのキーはサポートされていません。

   「Enter AWS KMS Alias」に、 CloudTrail使用するポリシーを変更したエイリアスをという形式で指定しますalias/*MyAliasName*。詳細については、「KMS キーを使用するようにリソースを更新する」を参照してください。

   エイリアスを選択するか、またはグローバルに一意のキー ID を使用することを選択できます。値は、以下の形式のいずれかになります。

   - エイリアス名: `alias/MyAliasName`
   - エイリアス ARN: `arn:aws:kms:region:123456789012:alias/MyAliasName`
   - キー ARN: `arn:aws:kms:region:123456789012:key/12345678-1234-1234-1234-123456789012`
   - グローバルに一意のキー ID: `12345678-1234-1234-1234-123456789012`
5. [変更を保存] を選択します。

> **Note**
>
> 選択した KMS キーが無効になっているか、削除が保留されている場合は、その KMS キーでイベントデータストア設定を保存することはできません。KMS キーを有効にするか、または別のキーを選択できます。詳細については、AWS Key Management Service デベロッパーガイドの「キー状態: KMS キーへの影響」を参照してください。

CloudTrail によるログファイルの暗号化の有効化と無効化 AWS CLI

このトピックでは、を使用して SSE-KMS のログファイル暗号化を有効または無効にする方法について説明します。 CloudTrail AWS CLI背景情報については、「 CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)」を参照してください。

トピック

- CloudTrail を使用してログファイルの暗号化を有効にする AWS CLI
- CloudTrail を使用してログファイルの暗号化を無効にします。 AWS CLI

CloudTrail を使用してログファイルの暗号化を有効にする AWS CLI

- 証跡のログファイル暗号化を有効にする
- イベントデータストアのログファイル暗号化を有効にする

証跡のログファイル暗号化を有効にする

1. AWS CLIを使用してキーを作成します。作成するキーは、 CloudTrail ログファイルを受け取る S3 バケットと同じリージョンにある必要があります。このステップでは、 AWS KMS create-keyコマンドを使用します。
2. 既存のキーポリシーを取得して、で使用できるように変更します CloudTrail。キーポリシーは、AWS KMS get-key-policyコマンドで取得できます。
3. ログファイルを暗号化したり、 CloudTrail ユーザーが復号したりできるように、キーポリシーに必要なセクションを追加します。ログファイルを読むすべてのユーザーに、復号許可が付与されているようにしてください。ポリシーの既存のセクションを変更しないでください。追加するポリシーセクションの詳細については、「AWS KMS の主要ポリシーの設定 CloudTrail」を参照してください。
4. コマンドを使用して、変更した JSON ポリシーファイルをキーに添付します。 AWS KMS put-key-policy
5. `--kms-key-id`パラメーターを指定して CloudTrail `create-trail` or `update-trail` コマンドを実行します。このコマンドは、ログの暗号化を有効にします。

   ```
   aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
   ```

   `--kms-key-id`このパラメーターは、ポリシーを変更したキーを指定します CloudTrail。次のいずれかの形式を指定できます。

   - エイリアス名。例: `alias/MyAliasName`
   - エイリアス ARN。例: `arn:aws:kms:us-east-2:123456789012:alias/MyAliasName`

- キー ARN。例: `arn:aws:kms:us-east-2:123456789012:key/12345678-1234-1234-1234-123456789012`
- 全体で一意のキー ID。例: `12345678-1234-1234-1234-123456789012`

以下に、応答の例を示します。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-
east-2:123456789012:key/12345678-1234-1234-1234-123456789012",
    "S3BucketName": "my-bucket-name"
}
```

KmsKeyId 要素が存在するため、ログファイルの暗号化が有効になったことがわかります。暗号化されたログファイルは約 5 分以内にバケットに表示されます。

イベントデータストアのログファイル暗号化を有効にする

1. AWS CLIを使用してキーを作成します。作成するキーは、イベントデータストアと同一のリージョンにある必要があります。このステップでは、 AWS KMS create-keyコマンドを実行します。
2. CloudTrail既存のキーポリシーを取得して編集して使用します。キーポリシーは、 AWS KMS get-key-policyコマンドを実行して取得できます。
3. ログファイルを暗号化したり、 CloudTrail ユーザーが復号したりできるように、必要なセクションをキーポリシーに追加します。ログファイルを読むすべてのユーザーに、復号許可が付与されているようにしてください。ポリシーの既存のセクションを変更しないでください。追加するポリシーセクションの詳細については、「AWS KMS の主要ポリシーの設定 CloudTrail」を参照してください。
4. コマンドを実行して、編集した JSON ポリシーファイルをキーに添付します。 AWS KMS put-key-policy
5. CloudTrail `create-event-data-store`or `update-event-data-store` コマンドを実行し、`--kms-key-id`パラメーターを追加します。このコマンドは、ログの暗号化を有効にします。

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

--kms-key-idこのパラメータは、ポリシーを変更したキーを指定します CloudTrail。次の 4 つの形式のいずれかを指定できます。

- エイリアス名。例: alias/MyAliasName
- エイリアス ARN。例: arn:aws:kms:us-east-2:123456789012:alias/MyAliasName
- キー ARN。例: arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012
- 全体で一意のキー ID。例: 12345678-1234-1234-1234-123456789012

以下に、応答の例を示します。

```
{
    "Name": "my-event-data-store",
    "ARN": "arn:aws:cloudtrail:us-east-1:12345678910:eventdatastore/
EXAMPLEf852-4e8f-8bd1-bcf6cEXAMPLE",
    "RetentionPeriod": "90",
    "KmsKeyId": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    "MultiRegionEnabled": false,
    "OrganizationEnabled": false,
    "TerminationProtectionEnabled": true,
    "AdvancedEventSelectors": [{
        "Name": "Select all external events",
        "FieldSelectors": [{
            "Field": "eventCategory",
            "Equals": [
                "ActivityAuditLog"
            ]
        }]
    }]
}
```

KmsKeyId 要素が存在するため、ログファイルの暗号化が有効になったことがわかります。暗号化されたログファイルは、約 5 分でイベントデータストアに表示されます。

CloudTrail を使用してログファイルの暗号化を無効にします。 AWS CLI

証跡でのログの暗号化を停止するには、update-trail を実行して、空の文字列を kms-key-id パラメータに渡します。

```
aws cloudtrail update-trail --name my-test-trail --kms-key-id ""
```

以下に、応答の例を示します。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "Default",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/Default",
    "LogFileValidationEnabled": false,
    "S3BucketName": "my-bucket-name"
}
```

KmsKeyId の値がないため、ログファイルの暗号化が有効でなくなったことがわかります。

> **Important**
>
> イベントデータストアでのログファイル暗号化を停止することはできません。

ドキュメント履歴

次の表に、 のドキュメントに対する重要な変更点を示します AWS CloudTrail。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

- API バージョン: 2013-11-01
- ドキュメントの最終更新日: 2024-05-30

変更	説明	日付
更新版	高度なイベントセレクタを使用してデータイベントをフィルタリングする方法について説明します。詳細については、「高度なイベントセレクタを使用してデータイベントをフィルタリングする」を参照してください。	2024 年 5 月 29 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon Kinesis Data Streams ストリームとストリームコンシューマーのデータイベントをログ記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 5 月 21 日
更新版	Lake でCloudTrail サポートされているリージョンページを更新し、アジアパシフィック (ハイデラバード) リージョン (ap-south-2)、欧州 (チューリッヒ) リージョン (eu-central-2)、イスラエル (テルアビ	2024 年 5 月 16 日

	ブ) リージョン (il-central-1) を追加しました。	
追加された機能	高度な CloudTrail イベントセレクタを使用して、 AWS Step Functions ステートマシンのデータイベントをログに記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 5 月 16 日
更新版	を使用した CloudTrail コストと使用状況の表示に関するセクションを追加しました AWS Cost Explorer。詳細については、「 での CloudTrail コストと使用状況の表示」を参照してください AWS Cost Explorer。	2024 年 5 月 14 日
追加された機能	高度なイベントセレクタを使用して、Amazon Q Apps で CloudTrail データイベントをログ記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 5 月 1 日

更新版	ユーザーガイドのセクションとページタイトルの全般的な組織の改善。これには、CloudTrail ログイベントリファレンスページのタイトルを「イベントを理解する」に変更し、管理 CloudTrail イベント、データイベント、インサイトイベントの説明を追加しました。「設定」ページのタイトルを「設定の構成 CloudTrail」に変更しました。データイベントのログ記録、管理イベントのログ記録、および Insights イベントのログ記録 ページを CloudTrail イベントを理解する セクションに移動しました。CloudTrail ログファイルの例ページをCloudTrail ログファイルセクションに移動しました。 CloudTrail Lake イベントデータストア、クエリ、統合 のコマンドを AWS CLI 一覧表示する個別のページを追加しました。https://docs.aws.amazon.com/awscloudtrail/latest/userguide/lake-queries-cli.html https://docs.aws.amazon.com/awscloudtrail/latest/userguide/lake-integrations-cli.html	2024 年 4 月 10 日

更新版	Lake がCloudTrail サポートするリージョンページを更新して、欧州 (スペイン) リージョン (eu-south-2) を追加しました。	2024 年 4 月 10 日
サービスサポートを追加	このリリースでは、 AWS Control Catalog がサポートされています。詳細については、「 のAWS のサービストピック CloudTrail」および「 を使用した AWS Control Catalog API コールのログ記録 AWS CloudTrail」を参照してください。	2024 年 4 月 8 日
サービスサポートを追加	このリリースでは、Deadline Cloud AWS がサポートされています。詳細については、「 のAWS のサービス トピック CloudTrail」を参照してください。	2024 年 4 月 2 日
追加された機能	AWS CloudTrail イベントバージョンは 1.10 になりました。詳細については、CloudTrail「レコードの内容」を参照してください。	2024 年 3 月 26 日

サービスサポートを追加	このリリースでは AWS Billing Conductorがサポートされています。詳細については、「 のAWS のサービス トピック CloudTrail」および「 を使用した AWS Billing Conductor API コールのログ記録 AWS CloudTrail」を参照してください。	2024 年 3 月 12 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、 AWS X-Ray トレースと AWS Systems Manager マネージドノードのデータイベントをログに記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 3 月 7 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon Simple Workflow Service (Amazon SWF) ドメインのデータイベントをログに記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 2 月 14 日

追加された機能	CloudTrail に ListInsightsMetricData API が追加されました。ListInsightsMetricData API は、Insights を有効にした証跡の Insights メトリクスデータを返します。詳細については、 API リファレンスListInsightsMetricDataの「」を参照してください。AWS CloudTrail	2024 年 2 月 6 日
追加された機能	高度なイベントセレクタを使用して AWS IoT、、 AWS IoT SiteWise、 CloudTrail のデータイベントを口グ AWS AppConfig に記録できるようになりました。詳細については、「データイベント」を参照してください。	2024 年 1 月 4 日
追加された機能	の高度なイベントセレクタを使用して AWS IoT Greengrass 、 CloudTrail のデータイベントを口グに記録できるようになりました。詳細については、「データイベント」を参照してください。	2023 年 12 月 22 日
新しいリージョンのサポート	CloudTrail は、新しい リージョンであるカナダ西部 (カルガリー) リージョンのサポートを拡大しました。詳細については、CloudTrail「サポートされているリージョン」を参照してください。	2023 年 12 月 20 日

追加された機能	高度なイベントセレクタを使用して、Amazon Keyspaces (Apache Cassandra 向け）AWS IoT TwinMaker 、、Amazon RDS、および CloudTrail のデータイベントを口グ AWS Supply Chain に記録できるようになりました。詳細については、「データイベント」を参照してください。	2023 年 12 月 20 日
AWS 管理ポリシーの更新	フェデレーションが無効になっている場合でも、組織のイベントデータストアで `glue:DeleteTable` および `lakeformation:DeregisterResource` のアクションを実行できるように、CloudTrailServiceRolePolicy 管理ポリシーを更新しました。	2023 年 11 月 26 日

追加された機能	CloudTrail Lake イベントデータストアをフェデレートして、データカタログ内のイベントデータストアに関連付けられたメタデータを表示し、AWS Glue Amazon Athena を使用してイベントデータに対して SQL クエリを実行できるようになりました。 AWS Glue データカタログに保存されているテーブルメタデータにより、Athena クエリエンジンはクエリするデータを検索、読み取り、処理する方法を知ることができます。詳細については、「イベントデータストアをフェデレーションする」を参照してください。	2023 年 11 月 26 日
追加された機能	の高度なイベントセレクタを使用して AWS Cloud Map 、CloudTrail のデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 11 月 16 日
追加された機能	高度なイベントセレクタを使用して、Amazon SQS メッセージで CloudTrail データイベントをログ記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 11 月 16 日

追加された機能	CloudTrail Lake では、イベントデータストアに 1 年間の拡張可能な保持料金と 7 年間の保持料金の 2 つの料金オプションが提供されるようになりました。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。このリリース以前は、すべてのイベントデータストアが 7 年間の保持料金オプションを使用していました。CloudTrail コンソール 、、または API オペレーションを使用して、イベントデータストアを 7 年間の保持料金オプションの使用から 1 年間の拡張可能な保持料金の使用に切り替えることができます。 AWS CLI UpdateEventDataStore料金オプションの詳細については、「AWS CloudTrail 料金」と「イベントデータストアの料金オプション」を参照してください。	2023 年 11 月 15 日

追加された機能	CloudTrail Lake. AWS CloudTrail Insights で Insights イベントを収集できるようになりました。これにより、AWS ユーザーは CloudTrail 管理イベントを継続的に分析することで、API コールや API エラー率に関連する異常なアクティビティを特定して対応できます。 CloudTrail Lake で Insights イベントを収集するには、管理イベントを口グに記録し、Insights を有効にするソースイベントデータストアと、ソースイベントデータストア内の異常な管理イベントアクティビティに基づいて Insights イベントを収集する送信先イベントデータストアが必要です。詳細については、CloudTrail 「Insights イベント用のイベントデータストアを作成する」および「Insights イベントの口グ記録」を参照してください。	2023 年 11 月 9 日
サービスサポートを追加	このリリースでは AWS Launch Wizardがサポートされています。詳細については、「 のAWS のサービス トピック CloudTrail」および「 を使用した AWS Launch Wizard API コールの口グ記録 AWS CloudTrail」を参照してください。	2023 年 11 月 8 日

サービスサポートを追加	このリリースでは、Amazon Bedrock がサポートされています。詳細については、「 のAWS のサービス トピック CloudTrail」および「 を使用した Amazon Bedrock API コールのログ AWS CloudTrail記録」を参照してください。	2023 年 10 月 23 日
追加された機能	高度なイベントセレクタを使用して、Amazon の CodeWhisperer カスタマイズで CloudTrail データイベントを記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 10 月 18 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon Timestream データベースとテーブルのデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 9 月 28 日
追加された機能	高度なイベントセレクタを使用して、Amazon SNS トピックとプラットフォームエンドポイント CloudTrail のデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 9 月 28 日

更新版	AWS Organizations 組織内の管理アカウント、委任管理者アカウント、およびメンバーアカウントが で実行できるタスクを示す表を追加しました CloudTrail。詳細については、「Organization delegated administrator」(組織の委任された管理者) を参照してください。	2023 年 9 月 25 日
サービスサポートを追加	このリリースでは、 AWS Marketplace 契約がサポートされています。詳細については、AWS のサービス「 のトピック CloudTrail」および「 を使用した契約 API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 9 月 1 日
追加された機能	高度なイベントセレクタを使用して、Amazon Kinesis ビデオストリームと Amazon SageMaker エンドポイントで CloudTrail データイベントを記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 8 月 31 日

サービスサポートを追加	このリリースでは、 AWS アプリケーション変換サービスがサポートされています。AWS アプリケーション変換サービスは、Microservice Extractor for AWS .NET などのサービスで使用されるバックエンドサービスです。詳細については、CloudTrail「サポートされているサービスと統合」を参照してください。	2023 年 8 月 26 日
追加された機能	高度なイベントセレクタを使用して、 AWS Private CA Connector for Active Directory で CloudTrail データイベントを口グ記録できるようになりました。詳細については、「データイベントの口グ記録」を参照してください。	2023 年 8 月 24 日
更新版	を使用して、イベントデータストアの作成、 CloudTrail Lake ダッシュボードの表示、証跡イベントをイベントデータストアにコピーする方法、サンプルクエリの表示と実行、クエリ結果を Amazon S3 バケットに保存する方法を示す新しい CloudTrail Lake シナリオを追加しました AWS Management Console。詳細については、「Lake のシナリオ」を参照してください。CloudTrail	2023 年 8 月 16 日

新しいリージョンのサポート	CloudTrail は、サポートを新しい リージョンであるイスラエル (テルアビブ) リージョンに拡張しました。詳細については、CloudTrail 「サポートされているリージョン」を参照してください。	2023 年 8 月 1 日
サービスサポートを追加	このリリースでは AWS HealthImaging がサポートされています。詳細については、CloudTrail「サポートされているサービスと統合」および「 を使用した AWS HealthImaging API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 7 月 26 日
追加された機能	高度なイベントセレクタを使用して CloudTrail 、データストアで AWS HealthImaging データイベントをログ記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 7 月 26 日
追加された機能	高度なイベントセレクタを使用して、 AWS Systems Manager コントロールチャネルと Amazon Managed Blockchain ネットワークで CloudTrail データイベントをログ記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 6 月 21 日

追加された機能	aws cloudtrail verify-query-results コマンドを使用して CloudTrail Lake が保存したクエリ結果を検証できるようになりました。詳細については、「AWS CLI を使用したクエリ結果の検証」を参照してください。	2023 年 6 月 21 日
サービスサポートを追加	このリリースは Amazon Verified Permissions をサポートします。詳細については、CloudTrail「サポートされているサービスと統合」および「 を使用した Amazon Verified Permissions API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 6 月 13 日
追加された機能	CloudTrail Lake ダッシュボードを使用して、イベントデータストア内のイベントを視覚化できるようになりました。詳細については、「Lake ダッシュボードを表示する」を参照してください。	2023 年 6 月 13 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon Verified Permissions ポリシーストアのデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 6 月 13 日

追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon CodeWhisperer プロファイルのデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 6 月 6 日
追加された機能	イベントデータストアで CloudTrail イベント取り込みを開始および停止できるようになりました。コンソールを使用してイベントの取り込みを停止する方法については、「イベントデータストアからのイベントの取り込みを停止する」を参照してください。を使用してイベント取り込みを停止する方法については AWS CLI、「イベントデータストアの取り込みを停止する」を参照してください。	2023 年 6 月 2 日
追加された機能	高度なイベントセレクタを使用して、Amazon EMR ログ先行書き込みワークスペースで CloudTrail データイベントをログ記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 5 月 31 日

サービスサポートを追加	このリリースでは、Amazon Security Lake がサポートされています。詳細については、CloudTrail「サポートされているサービスと統合」および「 を使用した Amazon Security Lake API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 5 月 30 日
更新版	CloudTrail userIdentity 要素のトピックを更新し、IAM Identity Center ユーザーに代わって行われたリクエストの例とフィールドの説明を追加しました。詳細については、「CloudTrail userIdentity 要素」を参照してください。	2023 年 5 月 23 日
更新版	この更新では、Processing Library の CloudTrail次のパッチリリースがサポートされています： aws-cloudtrail-processing-library-1.6.1.jar。詳細については、「 での CloudTrail Processing Library と CloudTrail Processing Library の使用」を参照してください GitHub。	2023 年 5 月 23 日
追加された機能	CloudTrail Lake は、すべての Presto 関数と演算子をサポートするようになりました。詳細については、CloudTrail「Lake SQL 制約」を参照してください。	2023 年 5 月 9 日

追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon GuardDuty ディテクターのデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」および「 を使用した Amazon GuardDuty API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 3 月 30 日
更新版	イベントデータストア用のユーザー定義のコスト配分タグの作成に関する新しいセクションが追加されました。詳細については、「 CloudTrail Lake イベントデータストアのユーザー定義のコスト配分タグの作成」を参照してください。	2023 年 3 月 24 日
サービスサポートを追加	このリリースでは、 AWS Telco Network Builder (AWS TNB) がサポートされています。詳細については、CloudTrail「サポートされているサービスと統合」および「 を使用した AWS Telco Network Builder API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 2 月 21 日

追加された機能	高度なイベントセレクタを使用して、Amazon Cognito ID プール CloudTrail のデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2023 年 2 月 15 日
更新版	CloudTrail Lake で使用できる学習リソースに関する新しいセクションを追加しました。詳細については、「学習リソース」を参照してください。	2023 年 2 月 9 日
追加された機能	の外部でイベントソースとの CloudTrail Lake 統合を作成できるようになりましたAWS。オンプレミスやクラウドでホストされている社内アプリケーションや SaaS アプリケーション、仮想マシン、コンテナなど、ハイブリッド環境のあらゆるソースからのユーザーアクティビティデータをログに記録して保存できます。詳細については、「AWS 外のイベントソースとの統合を作成する」を参照してください。	2023 年 1 月 31 日

追加された機能	高度なイベント CloudTrail PutAuditEvents セレクタを使用して、 CloudTrail Lake チャネルのアクティビティ CloudTrail のデータイベントを口グに記録できるようになりました。詳細については、「データイベントの口グ記録」を参照してください。	2023 年 1 月 31 日
新しいリージョンのサポート	CloudTrail は、サポートを新しいリージョンであるアジアパシフィック (メルボルン) リージョンに拡張しました。詳細については、CloudTrail「サポートされているリージョン」を参照してください。	2023 年 1 月 24 日
更新版	でのデータ整合性の管理に関する新しいセクションを追加しました。 CloudTrail「 でのデータ整合性の管理 CloudTrail」を参照してください。	2023 年 1 月 18 日
追加された機能	高度な CloudTrail イベントセレクタを使用して、Amazon SageMaker 特徴量ストアのデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2022 年 12 月 27 日

サービスサポートを追加	このリリースでは Discovery AWS Marketplace がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2022 年 12 月 15 日
追加された機能	高度なイベントセレクタを使用して、Amazon SageMaker メトリクス実験トライアルコンポーネントで CloudTrail データイベントをログ記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2022 年 12 月 15 日
追加された機能	設定 AWS Config 項目を含めるイベントデータストアを作成し、イベントデータストアを使用して本番環境への非準拠の変更を調査できるようになりました。詳細については、AWS Config 「設定項目 のイベントデータストアを作成する」を参照してください。	2022 年 11 月 28 日
新しいリージョンのサポート	CloudTrail は、サポートを新しいリージョンであるアジアパシフィック (ハイデラバード) リージョンに拡張しました。詳細については、CloudTrail 「サポートされているリージョン」を参照してください。	2022 年 11 月 22 日

追加された機能	高度なイベントセレクタを使用して、 Amazon FinSpace 環境で CloudTrail データイベントを口グ記録できるようになりました。詳細については、「データイベントの口グ記録」を参照してください。	2022 年 11 月 18 日
新しいリージョンのサポート	CloudTrail は、サポートを新しいリージョンである欧州 (スペイン) リージョンに拡張しました。詳細については、CloudTrail 「サポートされているリージョン」を参照してください。	2022 年 11 月 16 日
新しいリージョンのサポート	CloudTrail は、サポートを新しいリージョンである欧州 (チューリッヒ) リージョンに拡張しました。詳細については、CloudTrail 「サポートされているリージョン」を参照してください。	2022 年 11 月 9 日
追加された機能	AWS Organizations 組織の管理アカウントで、委任された管理者を追加して、組織の CloudTrail 証跡とイベントデータストアを管理できるようになりました。詳細については、「Organization delegated administrator」(組織の委任された管理者) を参照してください。	2022 年 11 月 7 日

追加された機能	CloudTrail Lake イベントデータストアの AWS Key Management Service 暗号化を有効にできるようになりました。詳細については、「イベントデータストアを作成する」を参照してください。	2022 年 11 月 7 日
追加された機能	クエリの実行時に CloudTrail Lake クエリ結果を Amazon S3 バケットに保存できるようになりました。クエリの実行の詳細については、「クエリを実行してクエリ結果を保存する」を参照してください。クエリ結果のダウンロードの詳細については、「保存されたクエリ結果の取得とダウンロード」を参照してください。	2022 年 10 月 21 日
追加された機能	CloudTrail 証跡イベントを CloudTrail Lake イベントデータストアにコピーできるようになりました。詳細については、「証跡イベントを CloudTrail Lake にコピーする」を参照してください。	2022 年 9 月 19 日
更新版	CloudTrail Lake でサポートされている Amazon CloudWatch メトリクスのリストを追加しました。詳細については、「サポートされている CloudWatch メトリクス」を参照してください。	2022 年 9 月 16 日

追加された機能	を使用して、 CloudTrail サービスにリンクされたチャネルを表示できるようになりました AWS CLI。詳細については、「 を使用して のサービスにリンク CloudTrail されたチャネルを表示する AWS CLI」を参照してください。	2022 年 9 月 9 日
新しいリージョンのサポート	CloudTrail は、新しい リージョンである中東 (UAE) リージョンのサポートを拡張しました。詳細については、CloudTrail 「サポートされているリージョン」を参照してください。	2022 年 8 月 30 日
変更された機能	CloudTrail は、管理ポリシーの名前を `AWSCloudTrailReadOnlyAccess` に変更しました`AWSCloudTrail_ReadOnlyAccess` 。このポリシー内の許可のスコープが縮小されています。デフォルトでは、ポリシーはすべての Amazon S3 バケット、 AWS Lambda 関数、またはエイ AWS KMS リアスを一覧表示するアクセス許可を付与しなくなりました。詳細については、「読み取り専用アクセス」を参照してください。	2022 年 6 月 6 日

変更された機能	セキュリティのベストプラクティスとして、aws:SourceArn または aws:SourceAccount 条件キーを Amazon S3 バケットポリシーの s3:GetBucketAcl ACL チェッキングブロックに追加できるようになりました。詳細については、「 の Amazon S3 バケットポリシーを設定する CloudTrail」を参照してください。	2022 年 5 月 11 日
変更された機能	2022 年 2 月 24 日以降、プロキシクライアントが使用された AWS Management Console セッションから発生したイベントで、 userAgent および sourceIPAddress フィールドの値の変更 AWS CloudTrail が開始されます。これらのイベントでは、 CloudTrail はフィールドuserAgent と sourceIPAddress フィールドの値を に置き換えますAWS Internal。 CloudTrail は、すべての AWS サービスでサービスアクションの情報をログに記録する方法を標準化するために、この変更を加えました。詳細については、CloudTrail「レコードの内容」を参照してください。	2022 年 4 月 12 日

サービスサポートを追加	このリリースでは、Amazon がサポートされています GameSparks。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2022 年 3 月 24 日
サービスサポートを追加	このリリースでは、 AWS App Mesh Envoy Management Service がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2022 年 3 月 18 日
更新版	CloudTrail Lake の新しいクエリ例が追加されました。これは、イベントに対してきめ細かな複数フィールドの SQL クエリを実行できるようにする新機能です。また、新たに `BytesScanned` フィールドが、`DescribeQuery` と `GetQueryResults` オペレーションのクエリメタデータの結果に追加されました。詳細については、「 CloudTrail Lake の使用」を参照してください。	2022 年 3 月 4 日

変更された機能	CloudTrail は、次の条件の両方が満たされた場合、データイベントの `resources` ブロック内の Amazon S3 バケット所有者のアカウント ID を削除するようになりました。データイベント API コールは Amazon S3 バケット所有者とは異なる AWS アカウントから送信され、API 発信者は発信者アカウントのみに関する`AccessDenied` エラーを受信しました。詳細については、「他のアカウントでコールされたデータイベントのバケット所有者アカウント ID を秘匿化する」を参照してください。	2022 年 3 月 3 日
更新版	この更新では、 CloudTrail Processing Library の次のリリースがサポートされています。カスタム S3 マネージャーの実装のサポート、ログファイル解析関連の例外へのイベントログ記録、のオプション`errorCode` フィールドの解析のサポート`insightDetails` が追加され、非数値を受け入れるようにアカウント ID 解析正規表現が更新されました。詳細については、「 で CloudTrail 処理ライブラリとCloudTrail処理ライブラリを使用する」を参照してください GitHub。	2022 年 1 月 28 日

追加された機能	CloudTrail では、イベントに対してきめ細かな複数フィールド SQL クエリを実行できるようにする新機能である CloudTrail Lake が導入されました。イベントはイベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基いた、イベントのイミュータブルなコレクションです。詳細については、「CloudTrail Lake の使用」を参照してください。	2022 年 1 月 5 日
新しいリージョンのサポート	CloudTrail は、サポートを新しいリージョンであるアジアパシフィック (ジャカルタ) リージョンに拡張しました。詳細については、CloudTrail「サポートされているリージョン」を参照してください。	2021 年 12 月 13 日
サービスサポートを追加	このリリースでは、Amazon WorkSpaces Web がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 12 月 3 日

追加された機能	高度な CloudTrail イベントセレクタを使用して、Lake Formation によって作成された AWS Glue テーブルのデータイベントを口グに記録できるようになりました。詳細については、「データイベントの口グ記録」を参照してください。	2021 年 11 月 30 日
変更された機能	セキュリティのベストプラクティスとして、キーポリシーと Amazon S3 バケットポリシーに `aws:SourceArn` または `aws:SourceAccount` 条件 AWS KMS キーを追加できるようになりました。Amazon S3 詳細については、「 のAWS KMS キーポリシーを設定する CloudTrail」および「 の Amazon S3 バケットポリシーを設定する CloudTrail」を参照してください。	2021 年 11 月 15 日
サービスサポートを追加	このリリースでは、 AWS Resilience Hub がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 11 月 10 日

追加された機能	新しい CloudTrail Insights イベントタイプとして、エラー率 Insights イベントを使用できます。エラーレート Insights イベントは、アカウント内で呼び出された API で発生したエラーに関する異常なアクティビティをキャプチャします。詳細については、「証跡 Insights イベントのログ記録」を参照してください。	2021 年 11 月 10 日
追加された機能	高度なイベントセレクタを使用して、DynamoDB ストリーム CloudTrail のデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2021 年 9 月 22 日
追加された機能	Amazon S3 アクセスポイントのデータイベントをログに記録できるようになりました。アドバンストイベントセレクタを使用して Amazon S3 アクセスポイントデータイベントをログに記録できます。詳細については、「データイベントのログ記録」を参照してください。	2021 年 8 月 24 日

変更された機能	Amazon SNS に通知を送信するように証跡を設定すると、 は SNS トピックへのアクセスポリシーにポリシーステートメント CloudTrail を追加し、 が SNS トピック CloudTrail にコンテンツを送信できるようにします。セキュリティのベストプラクティスとして、 CloudTrail ポリシーステートメントに `aws:SourceArn` または `aws:SourceAccount` 条件キーを追加することをお勧めします。詳細については、「 の Amazon SNS トピックポリシー CloudTrail」を参照してください。	2021 年 8 月 16 日
サービスサポートを追加	このリリースでは、Amazon Route 53 アプリケーションリカバリコントローラーがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 7 月 27 日

追加された機能	EBS スナップショットで実行される Amazon EBS ダイレクト API でデータイベントを口グに記録できるようになりました。アドバンストイベントセレクタを使用して Amazon EBS ダイレクト API データイベントを口グに記録できます。詳細については、「データイベントの口グ記録」を参照してください。	2021 年 7 月 27 日
変更された機能	がデータイベント CloudTrail を処理するとき、数値は整数 (int) か かにかかわらず、元の形式で保持されますfloat。データイベントのフィールドに整数があるイベントでは、 はこれらの数値を浮動小数点数として CloudTrail 履歴的に処理しました。これで、 はデータイベントの元の形式の整数 CloudTrail を保持します。詳細については、CloudTrail 「処理ライブラリの使用」を参照してください。	2021 年 7 月 13 日
追加された機能	Amazon RDS Data API 管理イベントを証跡から除外できるようになりました。詳細については、「証跡の管理イベントのログ記録」を参照してください。	2021 年 7 月 1 日

サービスサポートを追加	このリリースでは AWS BugBust がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 6 月 24 日
サービスサポートを追加	このリリースでは、Amazon Managed Grafana と Amazon Managed Service for Prometheus がサポートされます。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 6 月 2 日
サービスサポートを追加	このリリースでは AWS App Runner がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 5 月 18 日
サービスサポートを追加	このリリースでは、 AWS Systems Manager Incident Manager がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 5 月 10 日
更新版	この更新では、 AWS Config コンフォーマンスパック、特に HIPAA や FedRAMP などのコンプライアンスフレームワークのデータイベントログ記録要件について説明します。詳細については、「データイベントのログ記録」を参照してください。	2021 年 5 月 7 日

サービスサポートを追加	このリリースでは、Service Quotas と Amazon EBS ダイレクト API がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 4 月 13 日
追加された機能	IAM 管理者が を設定するとAWS STS、 はユーザーが IAM ロールを引き受けるとき、または引き受けたロールでアクションを実行するときに、イベントに`sourceIdentity` 情報を CloudTrail ログに記録します。詳細については、「CloudTrail userIdentity 要素」を参照してください。	2021 年 4 月 13 日
更新版	この更新では、一部の CloudTrailイベントレコードフィールドのコンテンツについて、キロバイト (KB) 単位で制限されます。詳細については、CloudTrail 「レコードの内容」を参照してください。	2021 年 4 月 8 日
追加された機能	IAM 管理者が を設定するとAWS STS、 はユーザーが IAM ロールを引き受けるとき、または引き受けたロールでアクションを実行するときに、イベントに`sourceIdentity` 情報を CloudTrail ログに記録します。詳細については、「CloudTrail userIdentity 要素」を参照してください。	2021 年 4 月 6 日

追加された機能	Amazon DynamoDB テーブルのデータイベントをログに記録できるようになりました。イベントセレクタまたはアドバンストイベントセレクタを使用して、DynamoDB データイベントをログに記録できます。詳細については、「データイベントのログ記録」を参照してください。	2021 年 3 月 23 日
サービスサポートを追加	このリリースでは、Amazon Managed Workflows for Apache Airflow がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 3 月 22 日
追加された機能	アドバンストイベントセレクタを使用することを選択している場合、S3 Object Lambda アクセスポイントでデータイベントをログに記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2021 年 3 月 18 日
サービスサポートを追加	このリリースでは、 AWS Fault Injection Simulator がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 3 月 15 日

追加された機能	アドバンストイベントセレクタを使用することを選択している場合、Amazon Managed Blockchain の Ethereum ノードでデータイベントを記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2021 年 3 月 1 日
サービスサポートを追加	このリリースでは、Amazon Managed Blockchain と Managed Blockchain 用の Ethereum のプレビューがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 2 月 4 日
サービスサポートを追加	このリリースでは AWS Amplifyがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 2 月 3 日
サービスサポートを追加	このリリースでは、Amazon Lookout for Metrics がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2021 年 2 月 1 日

更新版	この更新では、 CloudTrail Processing Library の次のパッチリリースがサポートされています。 ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.4.0.jar を使用します。詳細については、「 で CloudTrail 処理ライブラリとCloudTrail処理ライブラリを使用する」を参照してください GitHub。	2021 年 1 月 12 日
追加された機能	AWS Outpostsの Amazon S3 でデータイベントを記録できるようになりました。詳細については、「データイベントのログ記録」を参照してください。	2020 年 12 月 21 日
サービスサポートを追加	このリリースでは、Amazon Lookout for Equipment AWS Well-Architected Tool、および Amazon Location Service がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 12 月 16 日
サービスサポートを追加	このリリースでは AWS IoT Greengrass V2 がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 12 月 15 日

サービスサポートを追加	このリリースでは、EKS の Amazon EMR がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 12 月 10 日
サービスサポートを追加	このリリースでは、 AWS Audit Manager と Amazon がサポートされていま す HealthLake。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 12 月 8 日
サービスサポートを追加	このリリースでは、Amazon Lookout for Vision がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 12 月 1 日
追加された機能	AWS CloudTrail イベントバージョンは 1.08 になりました。バージョン 1.08 では、 の新しいフィールドが導入されています CloudTrail。詳細については、CloudTrail 「レコードの内容」を参照してください。	2020 年 11 月 24 日

追加された機能	AWS CloudTrail では、データイベントの高度なイベントセレクタが導入されています。アドバンストイベントセレクタにより、証跡に記録するデータイベントを詳細に制御できます。特定の AWS リソースのデータイベントを含めたり除外したりし、それらのリソースの特定の APIsを選択して証跡にログを記録したりできます。詳細については、「データイベントのログ記録」を参照してください。	2020 年 11 月 24 日
サービスサポートを追加	このリリースでは、 AWS Network Firewall がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 11 月 17 日
サービスサポートを追加	このリリースでは、 AWS Trusted Advisor がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 10 月 22 日
更新版	root ユーザーのサインインイベントのイベントレコードの例を 2 つ追加しました。詳細については、「AWS コンソールのサインインイベント」を参照してください。	2020 年 10 月 13 日

変更された機能	`AWSCloudTrail_FullAccess` ポリシーのアクセス許可が絞り込まれました。このポリシーでは、Amazon SNS トピックまたは Amazon S3 バケットを削除できなくなり、`getObject` アクションは削除されました。詳細については、CloudTrail「ユーザー へのカスタムアクセス許可の付与」を参照してください。	2020 年 9 月 29 日
更新版	この更新では、 CloudTrail Processing Library の次のパッチリリースがサポートされています。 ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.3.0.jar を使用します。詳細については、「 で CloudTrail 処理ライブラリとCloudTrail処理ライブラリを使用する」を参照してください GitHub。	2020 年 8 月 28 日
サービスサポートを追加	このリリースでは AWS Outpostsがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 8 月 28 日

追加された機能	AWS CloudTrail Insights では、 CloudTrail Insights イベントの属性フィールドが導入されています。属性フィールドには、Insights イベントをトリガーする異常なアクティビティに関連付けられている上位ユーザーアイデンティティ、ユーザーエージェント、エラーコードが表示されます。比較のために、属性フィールドには、上位のユーザーアイデンティティ、ユーザーエージェント、通常のアクティビティまたはベースラインのアクティビティに関連するエラーコードも表示されます。詳細については、「証跡 Insights イベントのログ記録」を参照してください。	2020 年 8 月 13 日
追加された機能	AWS CloudTrail コンソールは、使いやすくするために設計された新しい外観になっています。 AWS CloudTrail ユーザーガイドが更新され、証跡の作成、証跡の更新、イベント履歴のダウンロードなど、コンソールでタスクを実行する方法の手順が変更されました。	2020 年 8 月 13 日

サービスサポートを追加	このリリースでは、Amazon Interactive Video Service がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 7 月 15 日
サービスサポートを追加	このリリースでは、Amazon Honeycode がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 6 月 24 日
サービスサポートを追加	このリリースは、Amazon Macie をサポートします。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 5 月 19 日
サービスサポートを追加	このリリースは、Amazon Kendra をサポートします。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 5 月 13 日
サービスサポートを追加	このリリースでは AWS IoT SiteWiseがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 4 月 29 日
リージョンサポートが追加されました	今回のリリースから新たに欧州 (ミラノ) リージョンがサポートされます。「AWS CloudTrail でサポートされているリージョン」を参照してください。	2020 年 4 月 28 日

サービスとリージョンのサポートを追加	このリリースでは、Amazon AppFlow がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。アフリカ (ケープタウン) リージョンのサポートも追加されました。「AWS CloudTrail でサポートされているリージョン」を参照してください。	2020 年 4 月 22 日
追加された機能	Encrypt、、 などのハイボリュームな AWS KMS アクションGenerateDataKey はDecrypt、読み取りイベントとして記録されるようになりました。証跡上のすべての AWS KMS イベントをログに記録し、書き込み管理イベントも口グに記録することを選択した場合、証跡はDisableDelete、、 などの関連 AWS KMS アクションを口グに記録しますScheduleKey 。	2020 年 4 月 7 日
サービスサポートを追加	このリリースでは、Amazon CodeGuru Reviewer がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 2 月 7 日

サービスサポートを追加	このリリースは、Amazon Managed Apache Cassandra サービスをサポートしています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2020 年 1 月 17 日
サービスサポートを追加	このリリースでは、Amazon Connect がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 12 月 13 日
更新版	この更新では、 CloudTrail Processing Library の次のパッチリリースがサポートされています。 ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.2.0.jar を使用します。詳細については、「 で CloudTrail 処理ライブラリとCloudTrail処理ライブラリを使用する」を参照してください GitHub。	2019 年 11 月 21 日
追加された機能	このリリースでは、 アカウントの異常なアクティビティを検出するのに役立つ AWS CloudTrail Insights がサポートされています。「証跡の Insights イベントの記録	2019 年 11 月 20 日

追加された機能	このリリースでは、証跡から AWS Key Management Service イベントをフィルタリングするオプションが追加されています。「証跡の作成」を参照してください。	2019 年 11 月 20 日
サービスサポートを追加	このリリースでは、 AWS CodeStar 通知がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 11 月 7 日
追加された機能	このリリースでは、 CloudTrail コンソールまたは API のどちらを使用するかにかかわらず CloudTrail、 で証跡を作成するときにタグの追加がサポートされています。このリリースでは、`GetTrail` と `ListTrails` の 2 つの新しい API が追加されています。	2019 年 11 月 1 日
サービスサポートを追加	このリリースでは AWS App Meshがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 10 月 17 日
サービスサポートを追加	このリリースでは、Amazon Translate がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 10 月 17 日

ドキュメントの更新	サポートされていないサービストピックが復元され、 に現在イベントを記録していない AWS サービスのみが含まれるように更新されました CloudTrail。「CloudTrail でサポートされていないサービス」を参照してください。	2019 年 10 月 7 日
ドキュメントの更新	AWSCloudTrailFullAccess ポリシーの変更にともないドキュメントが更新されました。AWSCloudTrailFullAccess と同等のアクセス権限を示すポリシー例が更新され、iam:PassRole アクションが実行できるリソースが、以下の条件ステートメント "iam:PassedToService": "cloudtrail.amazonaws.com" に一致するリソースに制限されました。「AWS CloudTrail アイデンティティベースのポリシーの例」を参照してください。	2019 年 9 月 24 日
ドキュメントの更新	ドキュメントは、予算内に収め CloudTrail る際に から必要なログデータを取得できるように、新しいトピック CloudTrail「コストの管理」で更新されました。	2019 年 9 月 3 日

サービスサポートを追加	このリリースでは AWS Control Towerがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 8 月 13 日
リージョンサポートが追加されました	今回のリリースから新たに中東 (バーレーン) リージョンがサポートされます。「AWS CloudTrail でサポートされているリージョン」を参照してください。	2019 年 7 月 29 日
ドキュメントの更新	ドキュメントが更新され、 のセキュリティに関する情報が追加されました CloudTrail。「AWS CloudTrailのセキュリティ」を参照してください。	2019 年 7 月 3 日
サービスサポートを追加	このリリースでは AWS Ground Stationがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 6 月 6 日
サービスサポートを追加	このリリースでは AWS IoT Things Graphがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 6 月 4 日
サービスサポートを追加	このリリースでは Amazon AppStream 2.0がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 4 月 25 日

リージョンサポートが追加されました	今回のリリースから新たにアジアパシフィック (香港) リージョンがサポートされます。「AWS CloudTrail でサポートされているリージョン」を参照してください。	2019 年 4 月 24 日
サービスサポートを追加	このリリースは、Amazon Managed Service for Apache Flinkをサポートしています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 3 月 22 日
サービスサポートを追加	このリリースでは AWS Backupがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 2 月 4 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています WorkLink。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 1 月 23 日
サービスサポートを追加	このリリースでは AWS Cloud9がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 1 月 21 日

サービスサポートを追加	このリリースでは AWS Elemental MediaLiveがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 1 月 19 日
サービスサポートを追加	このリリースでは、Amazon Comprehend がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2019 年 1 月 18 日
サービスサポートを追加	このリリースでは AWS Elemental MediaPackageがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 12 月 21 日
リージョンサポートが追加されました	今回のリリースから新たに欧州 (ストックホルム) リージョンがサポートされます。「AWS CloudTrail でサポートされているリージョン」を参照してください。	2018 年 12 月 11 日
ドキュメントの更新	サポートおよびサポートされていないサービスに関する情報でドキュメントが更新されました。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 12 月 3 日

サービスサポートを追加	このリリースでは、 AWS Resource Access Manager (AWS RAM) がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 11 月 20 日
更新された機能	このリリースでは、 の組織内のすべての AWS アカウントのイベントを口グ CloudTrail に記録する証跡の作成がサポートされています AWS Organizations。「組織の証跡の作成」を参照してください。	2018 年 11 月 19 日
サービスサポートを追加	このリリースでは、Amazon Pinpoint SMS と音声 API をサポートしています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 11 月 16 日
サービスサポートを追加	このリリースでは AWS IoT Greengrassがサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 10 月 29 日

更新版	この更新では、 CloudTrail Processing Library の次のパッチリリースがサポートされています。 ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.1.3.jar を使用します。詳細については、「 で CloudTrail 処理ライブラリとCloudTrail処理ライブラリを使用する」を参照してください GitHub。	2018 年 10 月 18 日
追加された機能	このリリースでは、[イベント履歴] で追加のフィルターの使用がサポートされます。コンソール での CloudTrail イベントの表示 CloudTrail を参照してください。	2018 年 10 月 18 日
追加された機能	このリリースでは、Amazon Virtual Private Cloud (Amazon VPC) を使用した、VPC と AWS CloudTrailとの間のプライベート接続の確立がサポートされています。「インターフェイス VPC エンドポイント AWS CloudTrail での の使用」を参照してください。	2018 年 8 月 9 日
サービスサポートを追加	このリリースでは、Amazon Data Lifecycle Manager がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 7 月 24 日

サービスサポートを追加	このリリースでは、Amazon MQ がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 7 月 19 日
サービスサポートを追加	このリリースでは、 AWS Mobile CLI がサポートされています。「AWS CloudTrail でサポートされるサービスと統合」を参照してください。	2018 年 6 月 29 日
AWS CloudTrail RSS フィードから入手できるドキュメント履歴通知	RSS フィードにサブスクライブすることで、 AWS CloudTrail ドキュメントの更新に関する通知を受信できるようになりました。	2018 年 6 月 29 日

以前の更新

次の表は、2018 年 6 月 29 日より AWS CloudTrail 前の のドキュメントリリース履歴を示しています。

変更	説明	リリース日
サービスサポートを追加	このリリースでは、Amazon RDS Performance Insightsがサポートされました。詳細については、CloudTrail 「サポートされているサービスと統合」を参照してください。	2018 年 6 月 21 日
追加された機能	このリリースでは、イベント履歴のすべての CloudTrail 管理イベントのログ記録がサポートされています。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。	2018 年 6 月 14 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは AWS Billing and Cost Management がサポートされています。「CloudTrail がサポートするサービスと統合」を参照してください	2018 年 6 月 7 日
サービスサポートを追加	このリリースでは、Amazon Elastic Container Service for Kubernetes (Amazon EKS) がサポートされました。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 6 月 5 日
更新版	この更新では、Processing Library の次のパッチリリースがサポートされています CloudTrail。 • ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.1.2.jar を使用します。 詳細については、 CloudTrail 処理ライブラリを使用する「」およびCloudTrail 「 の処理ライブラリ」を参照してください GitHub。	2018 年 5 月 16 日
サービスサポートを追加	このリリースでは AWS Billing and Cost Management がサポートされています。「CloudTrail がサポートするサービスと統合」を参照してください	2018 年 6 月 7 日
サービスサポートを追加	このリリースでは、Amazon Elastic Container Service for Kubernetes (Amazon EKS) がサポートされました。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 6 月 5 日

変更	説明	リリース日
更新版	この更新では、Processing Library の次のパッチリリースがサポートされています CloudTrail。 • ユーザーガイドの .jar ファイル参照を更新して、最新バージョンの aws-cloudtrail-processing-library-1.1.2.jar を使用します。 詳細については、CloudTrail 処理ライブラリを使用する「」およびCloudTrail 「 の処理ライブラリ」を参照してください GitHub。	2018 年 5 月 16 日
サービスサポートを追加	このリリースでは AWS X-Rayがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 4 月 25 日
サービスサポートを追加	このリリースでは、 AWS IoT Analytics がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 4 月 23 日
サービスサポートを追加	このリリースでは、 Secrets Manager がサポートされました。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 4 月 10 日
サービスサポートを追加	このリリースでは、Amazon Rekognition がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 4 月 6 日
サービスサポートを追加	このリリースでは AWS 、 Private Certificate Authority (PCA) がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 4 月 4 日

変更	説明	リリース日
追加された機能	このリリースでは、Amazon Athena で CloudTrail 口グファイルを簡単に検索できるようになりました。CloudTrail コンソールから直接ログをクエリするためのテーブルを自動的に作成し、それらのテーブルを使用して Athena でクエリを実行できます。詳細については、CloudTrail がサポートするサービスと統合「」および「 コンソールでの CloudTrail ログのテーブルの作成 CloudTrail」を参照してください。	2018 年 3 月 15 日
サービスサポートを追加	このリリースでは AWS AppSyncがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 2 月 13 日
リージョンサポートが追加されました	今回のリリースから新たにアジアパシフィック (大阪) (ap-northeast-3) リージョンがサポートされます。CloudTrail サポートされているリージョン を参照してください。	2018 年 2 月 12 日
サービスサポートを追加	このリリースでは AWS Shieldがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 2 月 12 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています SageMaker。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 1 月 11 日
サービスサポートを追加	このリリースでは AWS Batchがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2018 年 1 月 10 日
追加された機能	このリリースでは、 CloudTrail イベント履歴で使用できるアカウントアクティビティの量を 90 日に延長できます。列の表示をカスタマイズして、 CloudTrail イベントの表示を改善することもできます。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。	2017 年 12 月 12 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは、Amazon がサポートされています WorkMail。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 12 月 12 日
サービスサポートを追加	このリリースでは、Alexa for Business 、 AWS Elemental MediaConvert、および がサポートされています AWS Elemental MediaStore。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 12 月 1 日
機能とドキュメントの追加	このリリースでは、 AWS Lambda 関数のデータイベントのログ記録がサポートされています。 詳細については、「データイベントをログ記録する」を参照してください。	2017 年 11 月 30 日
機能とドキュメントの追加	このリリースでは、 AWS Lambda 関数のデータイベントのログ記録がサポートされています。 詳細については、「データイベントをログ記録する」を参照してください。	2017 年 11 月 30 日
機能とドキュメントの追加	このリリースでは、 CloudTrail Processing Library に対する以下の更新がサポートされています。 • 管理イベントのブール値の識別。 • CloudTrail イベントバージョンを 1.06 に更新します。 詳細については、 CloudTrail 処理ライブラリを使用する「」およびCloudTrail 「 の処理ライブラリ」を参照してください GitHub。	2017 年 11 月 30 日
サービスサポートを追加	このリリースでは AWS Glueがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 11 月 7 日

変更	説明	リリース日
新規ドキュメント	このリリースは新しいトピックを追加しています[のクォータ AWS CloudTrail]。	2017 年 10 月 19 日
更新版	このリリースでは、Amazon Athena 、、Amazon Elastic Container Registry AWS CodeBuild、および の CloudTrail イベント履歴でサポートされている APIs のドキュメントを更新します AWS Migration Hub。	2017 年 10 月 13 日
サービスサポートを追加	このリリースでは、Amazon Chime がサポートされています。[CloudTrail がサポートするサービスと統合] を参照してください。	2017 年 9 月 27 日
機能とドキュメントの追加	このリリースでは、 AWS アカウント内のすべての Amazon S3 バケットのデータイベントログ記録の設定がサポートされています。[データイベントを口グ記録する] を参照してください。	2017 年 9 月 20 日
サービスサポートを追加	このリリースでは、Amazon Lex がサポートされています。[CloudTrail がサポートするサービスと統合] を参照してください。	2017 年 8 月 15 日
サービスサポートを追加	このリリースでは、 AWS Migration Hub がサポートされています。[CloudTrail がサポートするサービスと統合] を参照してください。	2017 年 8 月 14 日
機能とドキュメントの追加	このリリースでは CloudTrail 、すべての AWS アカウントでデフォルトで有効になっています。過去 7 日間のアカウントアクティビティはイベント履歴に表示され CloudTrail、最新のイベントはコンソールダッシュボードに表示されます。API アクティビティ履歴と呼ばれていた機能は、イベント履歴に置き換えられました。	2017 年 8 月 14 日

変更	説明	リリース日
機能とドキュメントの追加	このリリースでは、API アクティビティ履歴ページの CloudTrail コンソールからのイベントのダウンロードがサポートされています。イベントは JSON または CSV 形式でダウンロードできます。 詳しくは、イベントのダウンロード を参照してください。	2017 年 7 月 27 日
追加された機能	今回のリリースでは、欧州 (ロンドン) とカナダ (中部) の 2 つのリージョンで、Amazon S3 オブジェクトレベルの API オペレーションのログ記録がサポートされました。 詳しくは、 CloudTrail ログファイルの操作 を参照してください。	2017 年 7 月 19 日
サービスサポートを追加	このリリースではAPIs アクティビティ履歴機能で Amazon CloudWatch Events の CloudTrail API を検索できます。	2017 年 6 月 27 日
機能とドキュメントの追加	このリリースでは、以下のサービスの APIs アクティビティ履歴機能で追加の CloudTrail API がサポートされています。 • AWS CloudHSM • Amazon Cognito • Amazon DynamoDB • Amazon EC2 • Kinesis • AWS Storage Gateway	2017 年 6 月 27 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは AWS CodeStarがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 6 月 14 日

機能とドキュメントの追加	このリリースでは、 CloudTrail Processing Library に対する以下の更新がサポートされています。
	• CloudTrail ログファイルを識別するために、同じ SQS キューからの SQS メッセージに対するさまざまな形式のサポートを追加します。以下の形式がサポートされています。
	  • が SNS トピック CloudTrail に送信する通知
	  • Amazon S3 が SNS トピックに送信する通知
	  • Amazon S3 が直接 SQS キューに送信する通知
	• `deleteMessageUponFailure` プロパティのサポートを追加すると、処理できなかったメッセージを削除するために使用できます。
	
	詳細については、CloudTrail 処理ライブラリを使用する「」およびCloudTrail 「 の処理ライブラリ」を参照してください GitHub。
		2017 年 6 月 1 日

サービスサポートを追加	このリリースでは、Amazon Athena がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 5 月 19 日

変更	説明	リリース日
追加された機能	このリリースでは、Amazon CloudWatch Logs へのデータイベントの送信がサポートされています。 データイベントをログに記録するように証跡を設定する方法の詳細については、データイベント を参照してください。 CloudWatch ログへのイベントの送信の詳細については、「」を参照してくださいAmazon CloudTrail CloudWatch ログによるログファイルのモニタリング。	2017 年 5 月 9 日
サービスサポートを追加	このリリースでは、 AWS Marketplace Metering Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 5 月 2 日
サービスサポートを追加	このリリースでは、Amazon がサポートされていますQuickSight。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 4 月 28 日
機能とドキュメントの追加	このリリースでは、新しい証跡を作成するためのコンソールの操作が更新されました。新しい証跡で、管理イベントとデータイベントを ログに記録するよう設定できるようになりました。詳しくは、証跡の作成 を参照してください。	2017 年 4 月 11 日

変更	説明	リリース日
ドキュメントの追加	CloudTrail が S3 バケットにログを配信していない場合、またはアカウント内の一部のリージョンから SNS 通知を送信していない場合は、ポリシーを更新する必要がある場合があります。 S3 バケットポリシーの更新の詳細については、一般的な Amazon S3 ポリシー設定のエラー を参照してください。 SNS トピックポリシーの更新の詳細については、CloudTrail リージョンの通知を送信していない を参照してください。	2017 年 3 月 31 日
サービスサポートを追加	このリリースでは AWS Organizationsがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 2 月 27 日
機能とドキュメントの追加	このリリースでは、管理イベントとデータイベントをログに記録するように証跡を設定するためのコンソールの操作が更新されました。詳しくは、CloudTrail ログファイルの操作 を参照してください。	2017 年 2 月 10 日
サービスサポートを追加	このリリースでは、Amazon Cloud Directory がサポートされました。CloudTrail がサポートするサービスと統合 を参照してください。	2017 年 1 月 26 日
機能とドキュメントの追加	このリリースでは AWS CodeCommit、 APIs アクティビティ履歴での 、Amazon GameLift、および AWS Managed Services の CloudTrail API の検索がサポートされています。	2017 年 1 月 26 日

変更	説明	リリース日
追加された機能	このリリースでは、 AWS Health Dashboardとの統合がサポートされました。 を使用して AWS Health Dashboard 、証跡が SNS トピックまたは S3 バケットにログを配信できないかどうかを特定できます。これは、S3 バケットまたは SNS トピックのポリシーに問題がある場合に発生する可能性があります。 は、影響を受ける証跡について AWS Health Dashboard 通知し、ポリシーを修正する方法を推奨します。 詳細については、『AWS Health ユーザーガイド』を参照してください。	2017 年 1 月 24 日
機能とドキュメントの追加	このリリースでは、 CloudTrail コンソールでのイベントソースによるフィルタリングがサポートされています。イベントソースには、リクエストが行われた AWS サービスが表示されます。 詳細については、「コンソールでの最近の管理イベントの表示」を参照してください。	2017 年 1 月 12 日
サービスサポートを追加	このリリースでは AWS CodeCommitがサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2017 年 1 月 11 日
サービスサポートを追加	このリリースでは、Amazon Lightsail がサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2016 年 12 月 23 日
サービスサポートを追加	このリリースでは、 AWS マネージドサービスがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 12 月 21 日
リージョンサポートが追加されました	このリリースでは、欧州 (ロンドン) リージョンがサポートされています。CloudTrail サポートされているリージョン を参照してください。	2016 年 12 月 13 日

変更	説明	リリース日
リージョンサポートが追加されました	このリリースでは、カナダ (中部) リージョンがサポートされています。CloudTrail サポートされているリージョン を参照してください。	2016 年 12 月 8 日
サービスサポートを追加	このリリースでは、 AWS CodeBuild 「」を参照してくださいCloudTrail がサポートするサービスと統合。 このリリースでは AWS Healthがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。 このリリースでは AWS Step Functionsがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 12 月 1 日
サービスサポートを追加	このリリースでは、Amazon Polly がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 11 月 30 日
サービスサポートを追加	このリリースでは AWS OpsWorks for Chef Automate がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 11 月 23 日
機能とドキュメントの追加	このリリースでは、読み取り専用、書き込み専用、またはすべてのイベントをログに記録するように証跡を設定できるようになりました。 CloudTrail は、、、 などの Amazon S3 オブジェクトレベルの API オペレーションのログ記録をサポートしますDeleteObject 。 GetObject PutObject ユーザーは、オブジェクトレベルの API オペレーションをログに記録するように証跡を設定できます。 詳しくは、 CloudTrail ログファイルの操作 を参照してください。	2016 年 11 月 21 日

変更	説明	リリース日
機能とドキュメントの追加	このリリースでは、`userIdentity` 要素の `type` フィールドに追加の値 (`AWSAccount` と `AWSService`) を指定できるようになりました。詳細については、「フィールド for `userIdentity` 」を参照してください。	2016 年 11 月 16 日
サービスサポートを追加	このリリースでは、アプリケーションの Auto Scaling がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 10 月 31 日
リージョンサポートが追加されました	このリリースでは、米国東部 (オハイオ) リージョンをサポートされています。CloudTrail サポートされているリージョン を参照してください。	2016 年 10 月 17 日
機能とドキュメントの追加	このリリースでは、API 以外の AWS サービスイベントのログ記録がサポートされています。詳細については、「AWS サービスイベント」を参照してください。	2016 年 9 月 23 日
機能とドキュメントの追加	このリリースでは、 CloudTrail コンソールを使用して、 でサポートされているリソースタイプを表示できます AWS Config。詳細については、「AWS Configで参照されたリソースの表示」を参照してください。	2016 年 7 月 7 日
サービスサポートを追加	このリリースでは AWS Service Catalogがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 7 月 6 日
サービスサポートを追加	このリリースでは、Amazon Elastic File System (Amazon EFS) がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 6 月 28 日
リージョンサポートが追加されました	今回のリリースから新たに ap-south-1 (アジアパシフィック (ムンバイ)) リージョンがサポートされます。CloudTrail サポートされているリージョン を参照してください。	2016 年 6 月 27 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは AWS Application Discovery Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 5 月 12 日
サービスサポートを追加	このリリースでは、南米 (サンパウロ) リージョンの CloudWatch ログがサポートされています。詳細については、「Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング」を参照してください。	2016 年 5 月 6 日
サービスサポートを追加	このリリースでは AWS WAFがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 4 月 28 日
サービスサポートを追加	このリリースでは AWS Supportがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 4 月 21 日
サービスサポートを追加	このリリースでは、Amazon Inspector がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 4 月 20 日
サービスサポートを追加	このリリースでは AWS IoTがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 4 月 11 日
機能とドキュメントの追加	このリリースでは、Security Assertion Markup Language AWS Security Token Service (SAML AWS STS) とウェブ ID フェデレーションを使用して行われた () API コールのログ記録がサポートされています。詳細については、「SAML とウェブ ID AWS STS フェデレーションを使用する API の値」を参照してください。	2016 年 3 月 28 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは AWS Certificate Managerがサポートされています。「CloudTrail がサポートするサービスと統合」を参照してください。	2016 年 3 月 25 日
サービスサポートを追加	このリリースでは、Amazon Data Firehose がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 3 月 17 日
サービスサポートを追加	このリリースでは、Amazon CloudWatch Logs がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 3 月 10 日
サービスサポートを追加	このリリースでは、Amazon Cognito がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 2 月 18 日
サービスサポートを追加	このリリースでは AWS Database Migration Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 2 月 4 日
サービスサポートを追加	このリリースでは、Amazon GameLift (Amazon) がサポートされています GameLift。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 1 月 27 日
サービスサポートを追加	このリリースでは、Amazon CloudWatch Events がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2016 年 1 月 16 日
リージョンサポートが追加されました	今回のリリースから新たに ap-northeast-2 (アジアパシフィック (ソウル)) リージョンがサポートされます。CloudTrail サポートされているリージョン を参照してください。	2016 年 1 月 6 日
サービスサポートを追加	このリリースでは、Amazon Elastic Container Registry (Amazon ECR) がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 12 月 21 日

変更	説明	リリース日
機能とドキュメントの追加	このリリースでは、すべてのリージョン CloudTrail でを有効にし、リージョンごとに複数の証跡をサポートできます。詳細については、「CloudTrail トレイルでの作業」を参照してください。	2015 年 12 月 17 日
サービスサポートを追加	このリリースでは、Amazon Machine Learning がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 12 月 10 日
機能とドキュメントの追加	このリリースでは、ログファイルの暗号化、ログファイルの整合性検証、およびタグ付けがサポートされました。詳細については、CloudTrail AWS KMS キーによるログファイルの暗号化 (SSE-KMS)、CloudTrail ログファイルの整合性の検証、および証跡の更新を参照してください。	2015 年 10 月 1 日
サービスサポートを追加	このリリースでは、Amazon OpenSearch Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 10 月 1 日
サービスサポートを追加	このリリースでは、Amazon S3 バケットレベルのイベントがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 9 月 1 日
サービスサポートを追加	このリリースでは AWS Device Farmがサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2015 年 7 月 13 日
サービスサポートを追加	このリリースでは、Amazon API Gateway がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 7 月 9 日
サービスサポートを追加	このリリースでは CodePipeline がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 7 月 9 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは、Amazon DynamoDB がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 5 月 28 日
サービスサポートを追加	このリリースでは、米国西部 (北カリフォルニア) リージョンで CloudWatch ログがサポートされています。CloudWatch ログモニタリング CloudTrail のサポートの詳細については、「」を参照してくださいAmazon CloudTrail CloudWatch ログによるログファイルのモニタリング。	2015 年 5 月 19 日
サービスサポートを追加	このリリースでは AWS Directory Serviceがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 5 月 14 日
サービスサポートを追加	このリリースでは、Amazon Simple Email Service (Amazon SES) がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 5 月 7 日
サービスサポートを追加	このリリースでは、Amazon Elastic Container Service がサポートされています。「CloudTrail がサポートするサービスと統合」を参照してください。	2015 年 4 月 9 日
サービスサポートを追加	このリリースでは AWS Lambdaがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 4 月 9 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています WorkSpaces。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 4 月 9 日

変更	説明	リリース日
	このリリースでは、 (CloudTrail イベント) によってCloudTrailキャプチャされた AWS アクティビティの検索がサポートされています。ユーザーは、作成、変更、削除に関連するアカウント内のイベントを参照したり、フィルタリングしたりすることができます。これらのイベントを検索するには、 CloudTrail コンソール、 AWS Command Line Interface （ AWS CLI ）、または AWS SDK を使用できます。詳細については、「 CloudTrail イベント履歴の操作」を参照してください。	2015 年 3 月 12 日
サービスサポートと新しいドキュメントの追加	このリリースでは、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京)、欧州 (フランクフルト) の各リージョンで Amazon CloudWatch Logs がサポートされています。詳細については、 CloudWatch 「 ログへのイベントの送信」を参照してください。	2015 年 3 月 5 日
新規ドキュメント	AWS Security Token Service （ AWS STS) リージョンエンドポイント CloudTrail のサポートについて説明する新しいセクションが CloudTrail 概念ページに追加されました。	2015 年 2 月 17 日
サービスサポートを追加	このリリースでは、Amazon Route 53 がサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2015 年 2 月 11 日
サービスサポートを追加	このリリースでは AWS Configがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 2 月 10 日
サービスサポートを追加	このリリースでは AWS CloudHSMがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2015 年 1 月 8 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは AWS CodeDeployがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 12 月 17 日
サービスサポートを追加	このリリースでは AWS Storage Gatewayがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 12 月 16 日
リージョンサポートが追加されました	このリリースでは、-1 (AWS GovCloud （ 米国西部)) us-gov-westリージョンが 1 つ追加されています。CloudTrail サポートされているリージョン を参照してください。	2014 年 12 月 16 日
サービスサポートを追加	このリリースは、Amazon S3 Glacier がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 12 月 11 日
サービスサポートを追加	このリリースでは AWS Data Pipelineがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 12 月 2 日
サービスサポートを追加	このリリースでは AWS Key Management Serviceがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 11 月 12 日
新規ドキュメント	新しいセクション (Amazon CloudTrail CloudWatch ログによるログファイルのモニタリング) がガイドに追加されました。Amazon CloudWatch Logs を使用して CloudTrail ログイベントをモニタリングする方法について説明します。	2014 年 11 月 10 日
新規ドキュメント	新しいセクション (CloudTrail 処理ライブラリを使用する) がガイドに追加されました。 AWS CloudTrail Processing Library を使用して Java で CloudTrail ログプロセッサを書き込む方法に関する情報を提供します。	2014 年 11 月 5 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは、Amazon Elastic Transcoder がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 10 月 27 日
リージョンサポートが追加されました	このリリースでは、1 つの追加リージョン、eu-central-1 (欧州 (フランクフルト)) がサポートされています。CloudTrail サポートされているリージョン を参照してください。	2014 年 10 月 23 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています CloudSearch。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 10 月 16 日
サービスサポートを追加	このリリースでは、Amazon Simple Notification Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 10 月 9 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています ElastiCache。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 9 月 15 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています WorkDocs。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 8 月 27 日
新しいコンテンツの追加	このリリースでは、サインインイベントのログ記録に関するトピックが追加されました。AWS Management Console サインインイベント を参照してください。	2014 年 7 月 24 日
新しいコンテンツの追加	このリリースの eventVersion 要素はバージョン 1.02 にアップグレードされ、3 つの新しいフィールドが追加されました。CloudTrail レコードの内容 を参照してください。	2014 年 7 月 18 日
サービスサポートを追加	このリリースでは、Auto Scaling がサポートされています (「CloudTrail がサポートするサービスと統合」を参照してください)。	2014 年 7 月 17 日

変更	説明	リリース日
リージョンサポートが追加されました	今回のリリースから新たに ap-southeast-1 (アジアパシフィック (シンガポール))、ap-northeast-1 (アジアパシフィック (東京))、sa-east-1 (南米 (サンパウロ)) の 3 つのリージョンがサポートされます。CloudTrail サポートされているリージョン を参照してください。	2014 年 6 月 30 日
サービスサポートの追加	このリリースでは、Amazon Redshift がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 6 月 10 日
サービスサポートを追加	このリリースでは AWS OpsWorksがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 6 月 5 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています CloudFront。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 5 月 28 日
リージョンサポートが追加されました	今回のリリースから新たに us-west-1 (米国西部 (北カリフォルニア))、eu-west-1 (欧州 (アイルランド))、ap-southeast-2 (アジアパシフィック (シドニー)) の 3 つのリージョンがサポートされます。CloudTrail サポートされているリージョン を参照してください。	2014 年 5 月 13 日
サービスサポートを追加	このリリースでは、Amazon Simple Workflow Service がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 5 月 9 日
新しいコンテンツの追加	このリリースでは、アカウント間でのログファイルの共有に関するトピックが追加されました。CloudTrail AWS アカウント間でのログファイルの共有 を参照してください。	2014 年 5 月 2 日
サービスサポートを追加	このリリースでは、Amazon がサポートされています CloudWatch。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 4 月 28 日

変更	説明	リリース日
サービスサポートを追加	このリリースでは、Amazon Kinesis がサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2014 年 4 月 22 日
サービスサポートを追加	このリリースでは AWS Direct Connectがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 4 月 11 日
サービスサポートを追加	このリリースでは、Amazon EMR がサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 4 月 4 日
サービスサポートを追加	このリリースでは、Elastic Beanstalk がサポートされています。CloudTrail がサポートするサービスと統合を参照してください。	2014 年 4 月 2 日
サービスサポートの追加	このリリースでは AWS CloudFormationがサポートされています。CloudTrail がサポートするサービスと統合 を参照してください。	2014 年 3 月 7 日
新規ガイド	このリリースでは AWS CloudTrailを導入しています。	2013 年 11 月 13 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

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