ユーザーガイド

AWS Health

AWS Health: ユーザーガイド

Table of Contents

AWS Health の概要

AWS Health は、リソースのパフォーマンスと、AWS サービス のアカウントの可用性を継続的に可視化します。AWS Health イベントを使用して、サービスおよびリソースの変更が AWS で実行されているアプリケーションにどのように影響するかを確認できます。AWS Health は、進行中のイベントを管理するのに役立つ関連情報をタイムリーに提供します。また、AWS Health は、計画されたアクティビティを確認して準備するうえでも役立ちます。このサービスでは、AWS リソースのヘルス状態が変化したときにアラートや通知がトリガーされ、ほぼ瞬時にイベントが可視化されます。また、表示されるガイダンスに沿って対処することでトラブルシューティングの時間を短縮できます。

すべてのお客様は、AWS Health API を利用したAWS Healthダッシュボード を使用できます。ダッシュボードのセットアップは必要ありません。認証済みの AWS ユーザーは、すぐに使い始めることができます。その他の主なサービスについては、AWS Health [ダッシュボード詳細]ページを参照してください。

AWS Health の基本およびサービスの使用方法については、AWS Health を初めてお使いになる方向けの情報を参照してください。

AWS Health の使用時に表示される用語の一覧については、の概念 AWS Healthを参照してください。

> **メモ**
>
> - AWS Healthダッシュボードは、すべてのAWSお客様に追加料金なしでご利用いただけます。
> - すべてのAWSお客様は、Amazon EventBridge を通じて追加料金なしでAWS Healthイベントを受信できます。
> - ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートプランをお持ちのお客様は、AWS Health API を使用して社内システムおよびサードパーティーのシステムと統合することもできます。詳細については、「AWS Health API リファレンス」を参照してください。
> - 使用できるAWS Supportプランの詳細については、AWS Supportを参照してください。

AWS Health を初めてお使いになる方向けの情報

AWS Health を初めて使用する場合は、最初に以下のセクションをお読みください。

- AWS Health の概要 - このセクションでは、基盤となるデータモデル、サポートしているオペレーション、サービスとのやり取りに利用できる AWS SDK について説明します。
- の概念 AWS Health – AWS Health の基本と、サービスの利用時に使用される用語について説明します。
- AWS Health ダッシュボードの開始方法 – アカウントのヘルス — イベントや影響を受けるエンティティを表示し、高度なフィルタ処理を行います。このダッシュボードには、アカウントや組織に固有のイベントが含まれます。
- AWS Health ダッシュボード — サービスの状態— AWS アカウントがない場合は、それぞれの AWS リージョンに対するAWS サービスのヘルスとステータスに関する情報を表示できます。
- Amazon による AWS Health イベントのモニタリング EventBridge— Amazon EventBridge を使用して、AWS Healthからプッシュ通知を受け取ることができます。
- AWS Health API へのアクセス – AWS Health API セクションでは、イベントやエンティティの情報を取得するオペレーションについて説明します。

AWS Health では、すべてのお客様が AWS Health ダッシュボードと呼ばれるコンソールを利用できます。ダッシュボードをセットアップするためのコードの記述やアクションの実行は不要です。

Amazon EventBridge AWS Health でイベントを受信するようにEventBridge ルールを設定できます。これにより、アクションを実行するための Amazon EventBridge ルールを作成することで、プッシュ通知を使用してAWS Healthイベント管理を自動化できます。

ビジネスサポートプラン、エンタープライズオンランプサポートプラン、またはエンタープライズサポートプランがある場合は、ダッシュボードに表示される情報にプログラムでアクセスできます。AWS Command Line Interface (AWS CLI) を使用するか、コードを記述してリクエストを作成することができます。そのためには、REST API を直接使用するか AWS SDK を使用します。

Amazon EventBridge での AWS Health イベントの使用方法の詳細については、Amazon による AWS Health イベントのモニタリング EventBridge を参照してください。AWS CLI での AWS Health の使用の詳細については、AWS Health の AWS CLI リファレンスを参照してください。AWS CLI のインストール方法については、「AWS Command Line Interface インターフェイスのインストール」を参照してください。

の概念 AWS Health

の AWS Health 概念について学び、 サービスを使用して 内のアプリケーション、サービス、リソースの正常性を維持する方法を理解します AWS アカウント。

トピック

AWS Health イベント

AWS Health イベントは、ヘルスイベントとも呼ばれ、 が他の AWS サービスに代わって AWS Health 送信する通知です。これらのイベントを使用して、アカウントに影響する可能性のある今後の変更や予定された変更について知ることができます。例えば、 (IAM) が AWS Identity and Access Management 管理ポリシーを非推奨に AWS Config する場合、またはマネージドルールを非推奨にする場合、 はイベントを送信 AWS Health できます。 は、 にサービスの可用性の問題がある場合 AWS Health にもイベントを送信します AWS リージョン。イベントの説明を確認して、問題を理解し、影響を受けるリソースを特定して、推奨されるアクションを実行できます。

Health イベントには 2 つのタイプがあります。

目次

アカウント固有のイベント

アカウント固有のイベントは、 AWS アカウント または組織内の アカウントのいずれかにローカルです AWS 。例えば、使用するリージョンで Amazon Elastic Compute Cloud (Amazon EC2) インスタンスタイプに問題がある場合、 はイベントと影響を受けるリソースの名前に関する情報 AWS Health を提供します。

アカウント固有のイベントは、AWS Health Dashboard 、 AWS Health API から検索するか、Amazon CloudWatch Events を使用して通知を受信できます。

パブリックイベント

パブリックイベントは、アカウント固有ではない、レポートされたサービスイベントです。例えば、米国東部 (オハイオ) リージョンで Amazon Simple Storage Service (Amazon S3) のサービスに問題がある場合、 は、そのサービスを使用していない場合や、そのリージョンに S3 バケットがある場合でも、イベントに関する情報 AWS Health を提供します。それらに対してアクションを実行する前に、パブリック通知を確認することをお勧めします。

パブリックイベントは、 AWS Health ダッシュボードと AWS Health ダッシュボード – サービスの状態から確認できます。

アカウントをお持ちの場合は、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

アカウントをお持ちでない場合は、「AWS Health ダッシュボード — サービスの状態」を参照してください。

AWS Health ダッシュボード

がある場合 AWS アカウント、 AWS Health ダッシュボードにはパブリックイベントとアカウント固有のイベントの両方が表示されます。

AWS Health ダッシュボードを使用して、リージョン内のサービスの今後のメンテナンス問題など、一般的な認識を提供するイベントについて確認することをお勧めします。 AWS Health Dashboard を使用して、アカウントの非推奨リソースなど、ユーザーに直接影響する可能性のあるイベントについて確認することもできます。

にサインイン AWS Management Console すると、https://health.aws.amazon.com/health/home で AWS Health Dashboard を表示できます。

詳細については、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

AWS Health ダッシュボード — サービスの状態

アカウントをお持ちでない場合は、https://health.aws.amazon.com/health/status の AWS Health Dashboard – Service Health を使用して、パブリックイベントを表示できます。パブリックイベントは、サービスの可用性に関する情報を得ることのできる、 AWS についてレポートされるサービス問題です。このウェブサイトでは、どのアカウントでも固有ではないパブリックイベントのみが表示されます。このページを閲覧するために、各メンバーアカウントにサインインする必要はありません。

詳細については、「AWS Health ダッシュボード — サービスの状態」を参照してください。

イベントタイプのコード

Health イベントに表示されるイベントタイプのコードには、影響を受けるサービスとイベントのタイプが含まれています。例えば、AWS_EC2_SYSTEM_MAINTENANCE_EVENT イベントタイプのコードを含む Health イベントを受け取った場合、影響を及ぼす可能性のあるメンテナンスイベントがサービスで予定されていることを意味します。この情報を使用して、事前に計画を立てたり、アカウントに対してアクションを実行したりすることができます。

イベントタイプのカテゴリ

すべての Health イベントには、関連するイベントタイプのカテゴリがあります。一部のイベントでは、イベントタイプのカテゴリがイベントタイプのコードに表示される場合があります (AWS_RDS_MAINTENANCE_SCHEDULED コードなど)。この例では、カテゴリは scheduled です。この情報を使用して、イベントのカテゴリを大まかに確認できます。

すべてのイベントタイプのカテゴリをモニタリングすることをお勧めします。各カテゴリは、異なるタイプのイベントに対して表示されます。DescribeEventType API オペレーションを使用して、イベントタイプのカテゴリを検索することもできます。

アカウント通知

これらのイベントは、アカウントとサービスの管理またはセキュリティに関する情報を提供します。これらのイベントは情報提供のみの場合もありますが、緊急の処置が必要になる場合もあります。これらのタイプのイベントに注意を払い、推奨されるアクションをすべて確認することをお勧めします。

アカウント通知のイベントタイプのコードの例を次に示します。

- AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION — パブリックアクセスを許可する可能性のある Amazon S3 バケットがあります。
- AWS_BILLING_SUSPENSION_NOTICE — アカウントには未払いの料金があり、一時停止されているか、アカウントが非アクティブ化されました。
- AWS_WORKSPACES_OPERATIONAL_NOTIFICATION – Amazon のサービスに問題がありますWorkSpaces。

問題

これらのイベントは、 AWS サービスまたはリソースに影響する予期しないイベントです。このカテゴリの一般的なイベントには、サービスの低下を引き起こしているオペレーション上の問題、またはユーザーの認識用にローカライズされたリソースレベルの問題に関する通信が含まれます。

次に、問題に関するイベントタイプのコードの例を示します。

- AWS_EC2_OPERATIONAL_ISSUE — サービス使用時の遅延など、サービスのオペレーション上の問題。
- AWS_EC2_API_ISSUE — API オペレーションのレイテンシーの増加など、サービスの API のオペレーション上の問題。
- AWS_EBS_VOLUME_ATTACHMENT_ISSUE — Amazon Elastic Block Store (Amazon EBS) のリソースに影響を及ぼす可能性がある、ローカライズされたリソースレベルの問題。
- AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT — このイベントは、アクションを実行しなければ、アカウントが停止される可能性があることを意味します。

予定された変更

これらのイベントは、サービスおよびリソースへの今後の変更に関する情報を提供します。これらのイベントには、さまざまなバージョンの end-of-support 通知や自動アップグレードなどの計画されたライフサイクルイベントが含まれます。サービスの中断を避けるためにアクションを実行することを推奨するイベントもあれば、ユーザー側のアクションなしで自動的に発生するイベントもあります。予定された変更アクティビティの間、リソースが一時的に利用できないことがあります。このカテゴリのイベントはすべて、アカウント固有のイベントです。

次に、予定された変更に関するイベントタイプのコードの例を示します。

- AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED — Amazon EC2 インスタンスで再起動が必要です。
- AWS_SAGEMAKER_SCHEDULED_MAINTENANCE - SageMaker サービスの問題の修正などのメンテナンスイベントが必要です。

- AWS_RDS_PLANNED_LIFECYCLE_EVENT — Amazon RDS は、いずれかのバージョンのイベントなど、計画されたライフサイクル end-of-support イベントをスケジュールしています。これには、顧客のアクションが必要です。

> **Tip**
>
> AWS Health API または AWS Command Line Interface（ AWS CLI) を使用してイベントの詳細を返す場合、 Event オブジェクトには ACCOUNT_SPECIFIC 値を含む eventScopeCodeフィールドが含まれます。詳細については、「APIリファレンスAWS Health」を参照してください。

イベントステータス

イベントステータスは、Health イベントがオープン、クローズ、または将来のいずれであるかを示します。 AWS Health ダッシュボードまたは AWS Health API でヘルスイベントを最大 90 日間表示できます。

影響を受けるエンティティ

影響を受けるエンティティは、イベントによって影響を受ける可能性のある AWS リソースです。例えば、アカウントで使用している特定のインスタンスタイプについて Amazon EC2 メンテナンスの予定されたイベントを受信した場合、Health イベントを使用して、影響を受けるインスタンスの ID を判別できます。この情報を使用して、リソースの作成や非推奨など、潜在的なサービスの問題に対処します。

AWS Health Amazon での イベント EventBridge

アカウントに Amazon EventBridge ルールを設定して、適切な AWS Health イベントがアカウントによって受信された後にアクションを自動化できます。これには、予定されているすべてのライフサイクルイベントメッセージをチャットインターフェイスに送信するなど、一般的なアクションの場合もあります。また、IT サービス管理ツールでワークフローを起動するなど、特定のアクションの場合もあります。

詳細については、「Amazon による AWS Health イベントのモニタリング EventBridge」を参照してください。

AWS Health API

AWS Health API を使用して、次のような AWS Health Dashboard に表示される情報にプログラムでアクセスできます。

- AWS サービスやリソースに影響を与える可能性のあるイベントに関する情報を取得する
- AWS 組織の組織ビュー機能を有効または無効にする
- 特定のサービス、イベントタイプのカテゴリ、イベントタイプのコードでイベントをフィルタリングする

詳細については、「APIリファレンスAWS Health」を参照してください。

> **Note**
>
> AWS Health API AWS Supportを使用するには、 から Business、Enterprise On-Ramp、または Enterprise Support プランが必要です。Business、Enterprise On-Ramp、または Enterprise Support プランがないアカウントから AWS Health API を呼び出すと、`SubscriptionRequiredException`エラーが発生します。

組織ビュー

この機能を使用して、 の AWS アカウントのすべてのヘルスイベントを AWS Organizations AWS Health ダッシュボードの 1 つのビューに集約できます。その後、組織の管理アカウントにサインインするか、 AWS Health API を使用して、さまざまなアカウントとリソースに影響を与える可能性のあるすべてのイベントを表示できます。この機能は、 AWS Health コンソールまたは API から有効にできます。詳細については、「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。

AWS Health ダッシュボード — サービスの状態

AWS Health ダッシュボード – サービスのヘルスを使用して、すべての の状態を表示できます AWS サービス。このページには、 AWS リージョンにわたるサービスについて報告されたサービスイベントが表示されます。 AWS Health ダッシュボード – サービスヘルスページにアクセスするには AWS アカウント 、サインインしたり、 を持っている必要はありません。

> **Tip**
>
> このウェブサイトには、 に固有ではないパブリックイベントのみが表示されます AWS アカウント。アカウントを既にお持ちの場合は、サインインして AWS Health ダッシュボードを表示し、アカウントとサービスに影響を与える可能性のあるイベントについて常に把握しておくことをお勧めします。詳細については、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

AWS Health ダッシュボード – サービスの状態を表示するには

1. https://health.aws.amazon.com/health/status ページに移動します。

   > **Note**
   >
   > 既に AWS アカウント、 ページにサインインしている場合は、AWS Health ダッシュボード – アカウントのヘルスページにリダイレクトされます。

2. [サービスヘルス]で[未解決と最近の問題]を選択すると、最近報告されたイベントが表示されます。イベントに関する以下の情報を見ることができます。

   - イベント名と影響を受ける地域。たとえば、運用上の問題 — Amazon Elastic Compute Cloud (バージニア北部)
   - サービス名
   - イベントの重要度 (情報や機能低下など)
   - イベントの最新更新のタイムライン
   - このイベントの AWS サービス 影響を受ける のリスト

> **Note**
>
> イベントはローカルタイムゾーンまたは UTC で表示できます。詳細については、「タイムゾーンの設定」を参照してください。

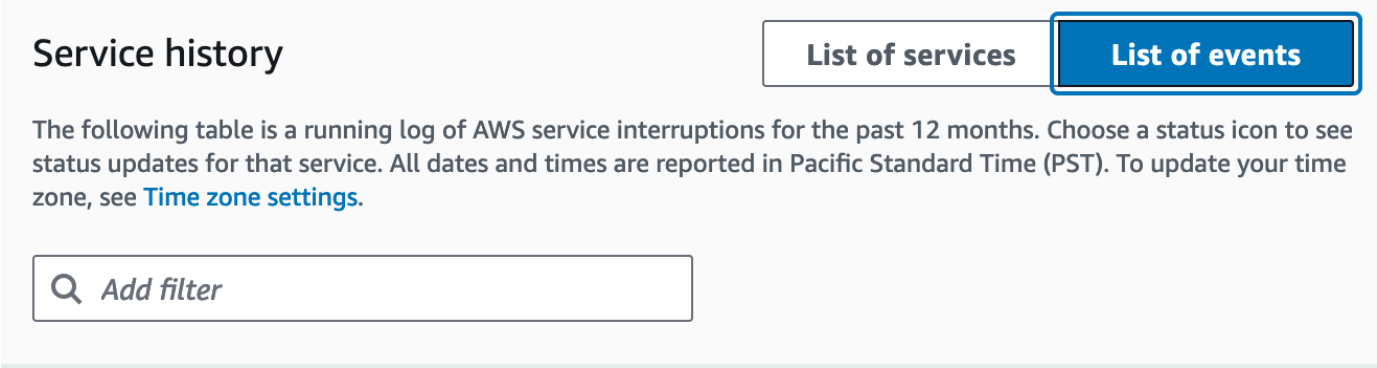
3. (オプション) イベントの横にある[RSS] を選択すると、このイベントの RSS フィードを購読できます。指定された で、この特定のサービスに関する通知を受け取ります AWS リージョン。
4. [サービス履歴]を選択すると、[サービス履歴]テーブルが表示されます。この表は、過去 12 か月間のすべての AWS サービス 中断を示しています。

> **Tip**
>
> サービス、AWS リージョン、日付でフィルタリングできます。

5. 進行中のサービスイベントの横にあるステータスアイコン

   ( )

   を選択すると、そのイベントに関する詳細情報が表示されます。
6. (オプション) これを履歴イベントのリストとして表示するには、イベントのリストボタンを選択します。イベント列で任意のイベントを選択すると、ポップアップサイドパネルにその特定のイベントに関する詳細情報が表示されます。



> **Note**
>
> 2023 年 9 月以降にパブリックイベントを選択すると、ブラウザの URL にそのパブリック AWS Health イベントへのリンクが入力されます。このリンクを選択したら、そのイベントポップアップを含むイベントビューのリストに移動します。

7. (オプション) RSS フィードを購読するには、[RSS]を選択します。この特定のサービスに関する通知が、指定した AWS リージョンに届きます。
8. (オプション) ローカルタイムゾーンと UTC を切り替えてイベントを見ることもできます。詳細については、「タイムゾーン設定」を参照してください。
9. (オプション) アカウントをお持ちの場合は、[アカウントの状態を開く]を選択してサインインしてください。サインインすると、アカウントに固有のイベントを表示できます。詳細については、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

の計画されたライフサイクルイベント AWS Health

の計画されたライフサイクルイベントについて説明します AWS Health。

トピック

計画的ライフサイクルイベントとは？

AWS Health は、アプリケーションの可用性に影響する重要な変更を通知します。責任 AWS 共有モデルでは、 AWS は、 リソースをサポートする基盤となるハードウェアとインフラストラクチャを最新かつ安全に保つためのアクションを取ります。ただし、一部の変更では、アプリケーションへの影響を避けるために、お客様の対応や調整が必要になります。 AWS Health は次のような重要な変更を事前に通知します。

- オープンソースソフトウェアのサポート終了 - 一部の はオープンソースバージョンのソフトウェア AWS サービス を実行します。オープンソースコミュニティがソフトウェアバージョンのサポートを終了すると、アップグレードしてアプリケーションへの影響を避けるためにアクションを実行する必要があるときに から AWS 通知されます。
  - Amazon RDS for MySQL エンジンバージョンのサポート終了
  - Amazon EKS Kubernetes バージョンのサポート終了
- アクションを必要とする可能性のある AWS所有のリソースに影響する変更。
  - Amazon RDS 認証局証明書の有効期限満了。
  - Amazon WorkDocs Companion はサポートが終了し、 は利用できなくなりました。

    > **Note**
    >
    > この基準を満たすすべての通知は、計画されたライフサイクルイベント AWS Health として を通じて報告されます。
- 動的リソースのバーンダウンとメタデータの改善: AWS Health イベントの存続期間を通じて通知を受信してから、影響を受けるリソースは、特定のエンティティステータスを持つ影響を受ける工

ンティティとして AWS Health イベントに関連付けられます。影響を受けるリソースは、該当する場合には ARN 形式で指定されます。影響を受けるリソースが顧客による対応を必要とする場合、そのリソースは「保留中」ステータスで一覧表示されます。影響を受けるリソースに必要な対応が実行されたか、リソースが削除された場合、ステータスは「解決済み」に更新されます。

> **Note**
>
> - リソース状態の更新は非同期かつ定期的に実行され、まれに最大72時間遅れることがあります。
> - 「保留中」または「解決済み」ステータスのリソースではなく、動的更新が提供されない例外では、リソースにステータスは割り当てられません。
> - リソースステータスの更新は、 AWS GovCloud (US) および中国リージョンではサポートされていません。

計画ライフサイクルイベントの通知を受け取ったら、何を予期すべきですか?

計画されたライフサイクルイベント AWS Health の経験は、チームが今後のライフサイクル変更について学習し、アクションの完了を追跡するのに役立ちます。

タイプカテゴリ:予定されている変更

イベントタイプコード: AWS_ {SERVICE} _PLANNED_LIFECYCLE_EVENT

イベント開始時間：イベント開始時間は、リソースが変更の影響を受ける最も早い日付です。

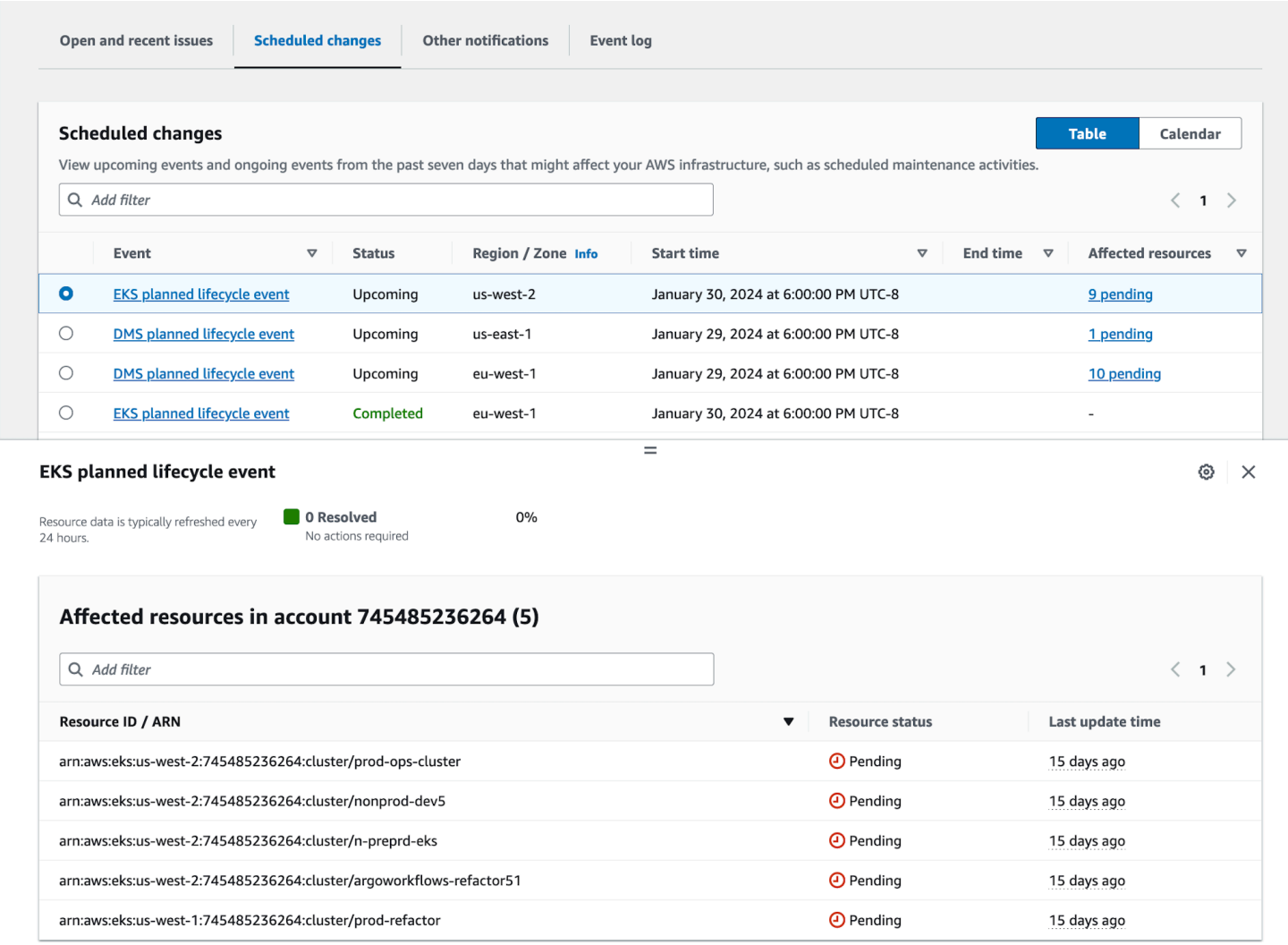
イベント終了時刻： イベント終了時刻は、すべての AWS リソースで変更が完了した日付です。終了時間は必ずしも指定されるわけではないことに注意してください。開始時間を変更日として扱うことが重要です。

> **Note**
>
> 組織は、影響を受けるリソースが存在する地域ごとにグループ化された、計画されたライフサイクルイベントごとに1つのイベント ARN を受け取ることを予期できます。ただし、組織が多数の影響を受ける AWS アカウント またはリソースを持っている場合、複数の ARNs を受け取る可能性があります。

計画されたライフサイクルイベントを早期に可視化：計画されたライフサイクルイベントは、可能な限り、メジャーバージョン / 変更では180日、マイナーバージョン / 変更では90日という最小リードタイムを設けるように設計されています。

動的リソースのバーンダウンとメタデータの改善： AWS Health イベントの存続期間を通じて通知を受信すると、影響を受けるリソースは、特定のエンティティステータスを持つ影響を受けるエンティティとして AWS Health イベントに関連付けられます。影響を受けるリソースは、該当する場合には ARN 形式で指定されます。影響を受けるリソースが顧客による対応を必要とする場合、そのリソースは「保留中」ステータスで一覧表示されます。影響を受けるリソースに必要な対応が実行されたか、リソースが削除された場合、ステータスは「解決済み」に更新されます。

> **Note**
>
> - AWS Health 通知は、 AWS GovCloud (US) および中国リージョンを除き、可能な場合はステータスを経時的に更新します。
> - リソース状態の更新は非同期かつ定期的に実行され、まれに最大72時間遅れることがあります。



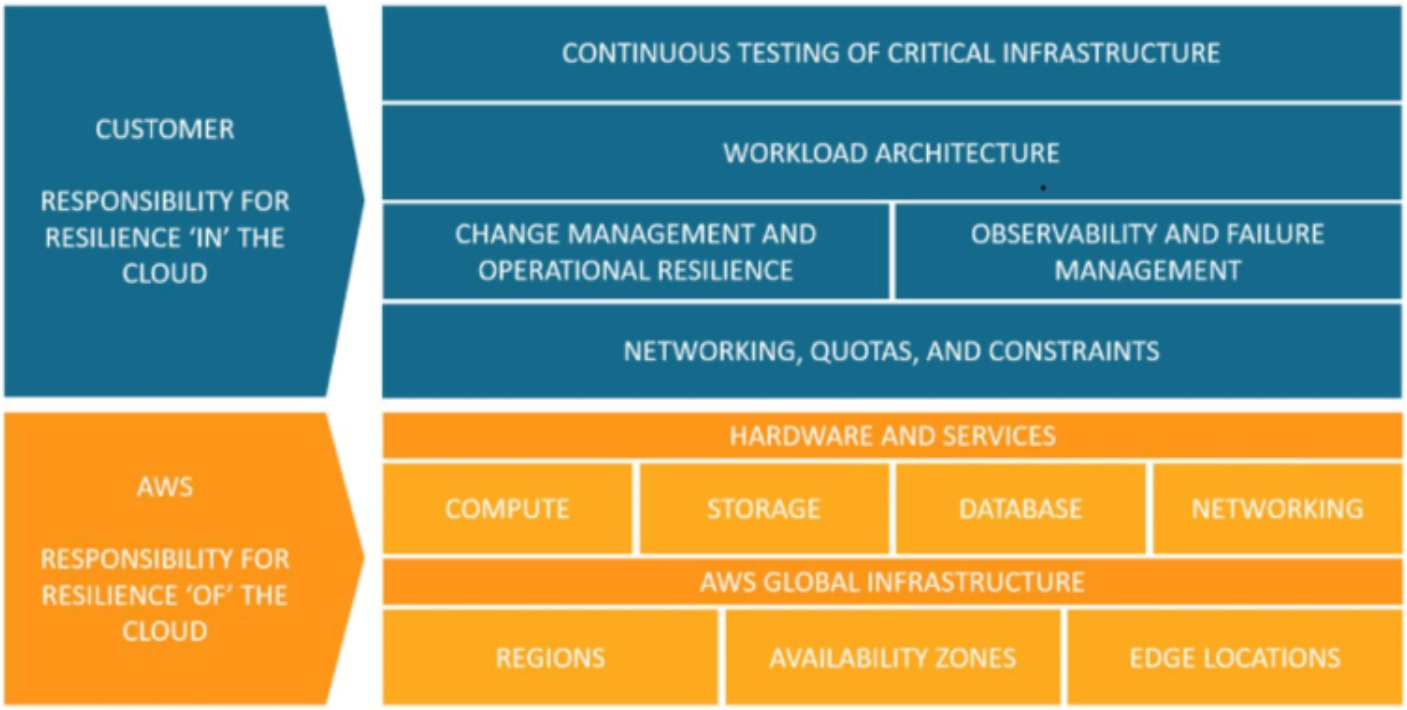
予定されているイベントの日付が過ぎると、

1. 該当する場合、サービスはイベントの開始日以降にいつでも、お客様のリソースに上記の変更を実施することがあります。
2. サポート終了日より前にすべてのリソースを解決すると、 AWS Health イベントのステータスが「クローズ」に変わります。
3. 未解決のリソースが残っていても解決されない場合、 AWS Health イベントは開始日または終了日から90日間は開いたままになります。その後、イベントは削除されます。

レジリエンス維持のための責任分担モデル

セキュリティとコンプライアンスは、 AWS と顧客間で責任を共有するものです。導入するサービスによっては、この共有モデルがお客様の運用上の負担を軽減するのに役立ちます。これは、 がホス

トオペレーティングシステムと仮想化レイヤーから、サービスが動作する施設の物理セキュリティまで、コンポーネントを AWS 運用、管理、制御するためです。お客様は、 AWSが提供するセキュリティグループファイアウォールの設定に加えて、ゲストオペレーティングシステム (更新やセキュリティパッチを含む) およびその他の関連するアプリケーションソフトウェアの責任と管理を引き受けます。詳細については、責任共有モデルを参照してください。



計画されたライフサイクルイベントへのアクセス

計画されたライフサイクルイベントには、複数のチャネルを使用してアクセスおよび監視できます。

- Amazon を使用する EventBridge
- AWS Health ダッシュボードを使用する
  - カレンダービュー
  - 「影響を受けるリソース」ビュー
- AWS Health API を使用する

AWS Health ダッシュボードの開始方法 – アカウントのヘルス

AWS Health Dashboard を使用して、 AWS Health イベントについて学習できます。これらのイベントは、 AWS サービス または AWS アカウントに影響を与える可能性があります。アカウントにサインインすると、 AWS Health Dashboard に次の方法で情報が表示されます。

- [アカウントイベント] — このページには、アカウントに固有のイベントが表示されます。未解決の変更、最近の変更、予定されている変更を表示できます。過去 90 日間のすべてのイベントを示す通知とイベントログを表示することもできます。
- [組織のイベント] — このページには、 AWS Organizationsの組織固有のイベントが表示されます。組織の未解決の変更、最近の変更、および予定されている変更を表示できます。通知だけではなく、過去 90 日間のすべての組織イベントを示すイベントログを表示することもできます。

> **Note**
>
> をお持ちでない場合は AWS アカウント、 を使用して、サービスの一般提供状況AWS Health ダッシュボード — サービスの状態を確認できます。
> アカウントをお持ちの場合は、 AWS Health Dashboard にサインインして、 のサービスとリソースに影響を与える可能性のあるイベントや今後の変更に関するより深い洞察を得ることをお勧めします。

目次

- タイムゾーン設定
- 組織のヘルス
- Amazon を設定する EventBridge
- AWS Health 対応
- AWS Health イベントのアラート

AWS Health Dashboard でアカウントイベントを表示する

アカウントにサインインすると、パーソナライズされたイベントやお勧め情報を受け取ることができます。

AWS Health ダッシュボードでアカウントイベントを表示するには

1. ホーム で AWS Health https://health.aws.amazon.com/health/Dashboard を開きます。
2. ナビゲーションペインの [アカウントの状態] で、次のオプションを選択できます。

   a. [未解決の課題と最近の問題] — 最近開いたイベントと終了したイベントを表示します。
   b. [予定されている変更] — サービスやリソースに影響する可能性のある、今後予定されているイベントを表示します。
   c. [その他の通知] — アカウントに影響する可能性のある、過去 7 日間のその他の通知や進行中のイベントをすべて表示します。
   d. [イベントログ] — 過去 90 日間のすべてのイベントを表示します。

未解決の問題と最近の問題

[未解決の問題と最近の問題] タブでは、過去 7 日間に進行中のアカウントに影響する可能性のあるすべてのイベントを確認できます。

ダッシュボードでイベントを選択すると、[詳細] ペインにイベントと影響を受けるリソースのリストの情報が表示されます。詳細については、「イベントの詳細」を参照してください。

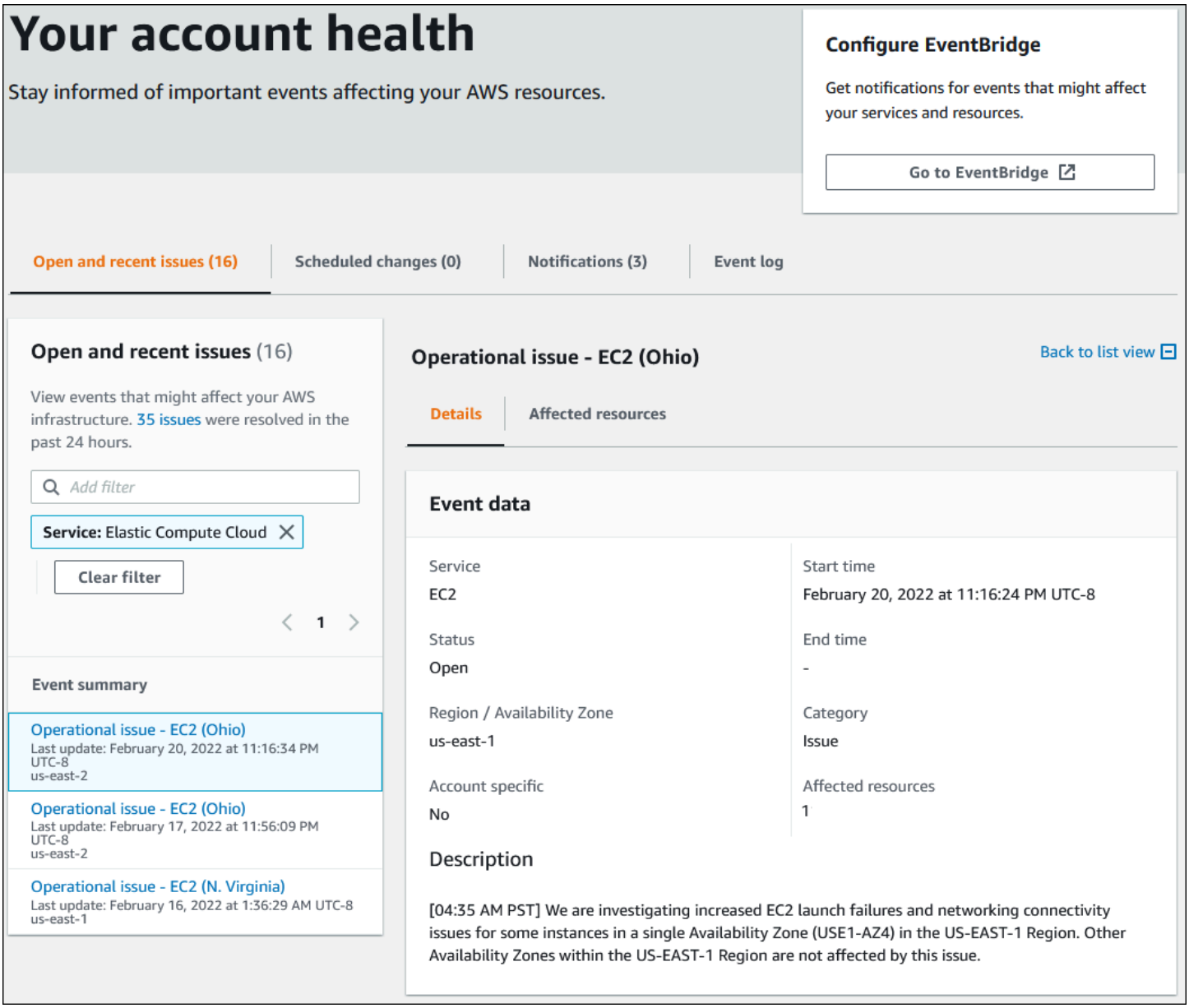
表示されたイベントは、タブを問わず、フィルタリストからオプションを選択してフィルタリングできます。例えば、結果をアベイラビリティーゾーン、リージョン、イベント終了時刻、最終更新時刻などで絞り込むことができます AWS サービス。

ダッシュボードに表示される最近のイベントだけでなく、すべてのイベントを表示するには、[イベントログ] タブを選択します。

> **Note**
>
> 現時点では、 AWS Health ダッシュボードに表示されるイベントの通知を削除することはできません。がイベントを AWS サービス 解決すると、ダッシュボードビューから通知が削除されます。

Example : Amazon Elastic Compute Cloud (Amazon EC2) の運用上の問題イベント

次の図は、Amazon EC2インスタンスの起動失敗と接続の問題に関するイベントを示しています。



予定された変更

[予定された変更]タブを使用して、アカウントに影響する可能性のある今後のイベントについて知ることができます。これらのイベントには、サービスの定期メンテナンスアクティビティや、解決に必要な計画的なライフサイクルイベントなどが含まれます。こうしたアクティビティを計画しやすくするため、予定された変更を月次カレンダーにマッピングできるカレンダービューが用意されています。フィルターが利用可能です。計画されたライフサイクルイベントの詳細については、「の計画されたライフサイクルイベント AWS Health」を参照してください。

その他の通知

[通知] タブでは、アカウントに影響を及ぼす可能性のある、過去 7 日間のその他の通知や進行中のイベントをすべて確認できます。これには、証明書の口ーテーション、請求通知、セキュリティの脆弱性などのイベントが含まれる場合があります。

イベントログ

イベントログタブを使用して、すべての AWS Health イベントを表示します。ログテーブルには追加の列があり、[ステータス]と[開始時間]でフィルタリングできます。

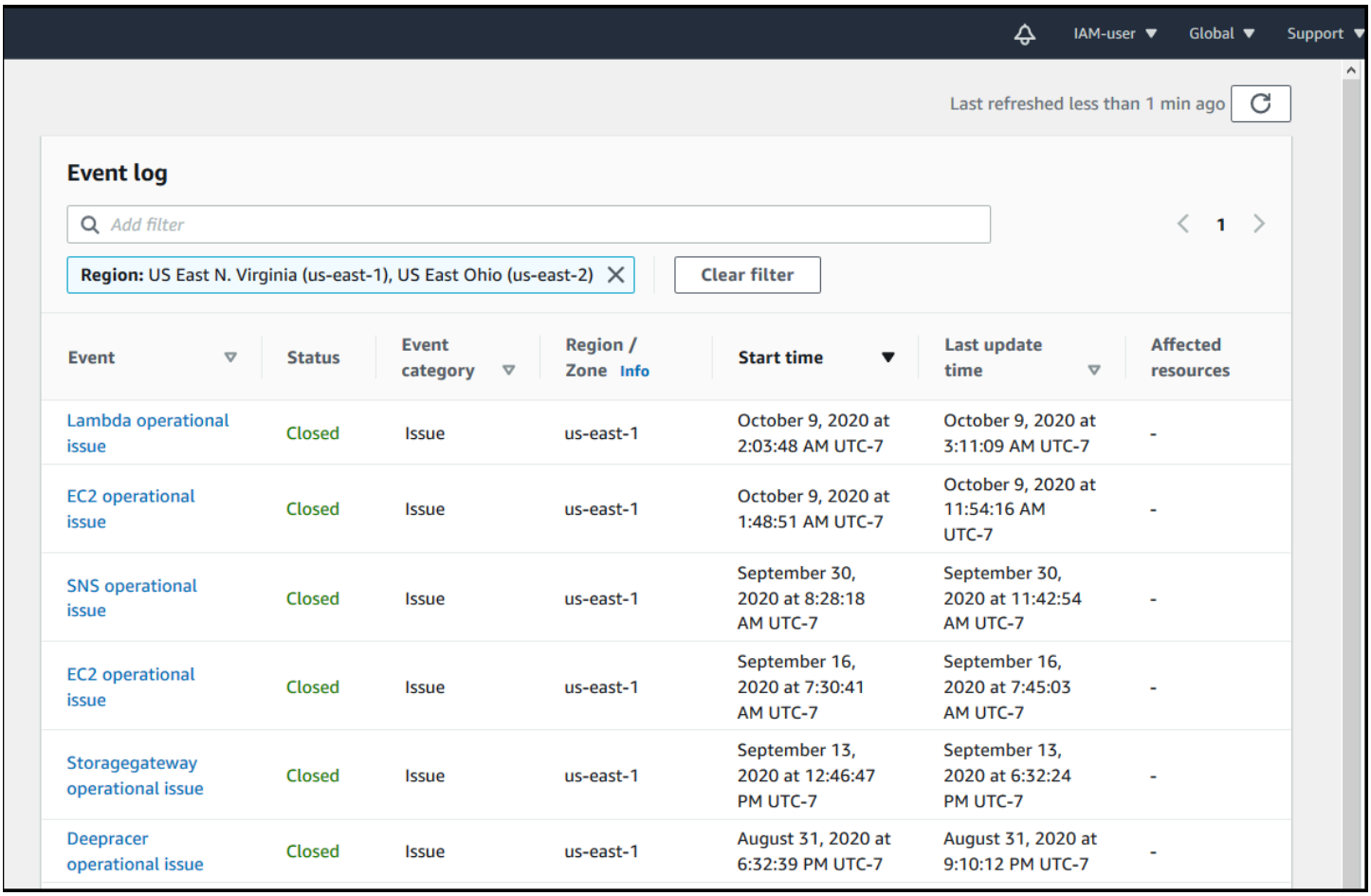
[イベントログ] テーブルでイベントを選択すると、[詳細] ペインにイベントと影響を受けるリソースのリストの情報が示されます。詳細については、「イベントの詳細」を参照してください。

検索結果を絞り込むには、次のフィルターオプションを使用できます。

- アベイラビリティーゾーン
- 終了時間
- イベント
- イベント ARN
- イベントカテゴリ
- 最終更新日時
- リージョン
- リソース ID / ARN
- サービス
- 開始時間
- ステータス

Example : イベントログ

次の画像は、米国東部 (バージニア北部) および米国東部 (オハイオ) リージョンの最近のイベントを示しています。



イベントの詳細

イベントを選択すると、そのイベントに関する 2 つのタブが表示されます。[詳細]タブは以下の情報を表示します。

- サービス
- ステータス
- リージョン/アベイラビリティーゾーン
- イベントがアカウント固有のものかどうか
- 開始時間と終了時間
- カテゴリ

- 影響を受けるリソースの数
- イベントに関する説明と最新情報のタイムライン

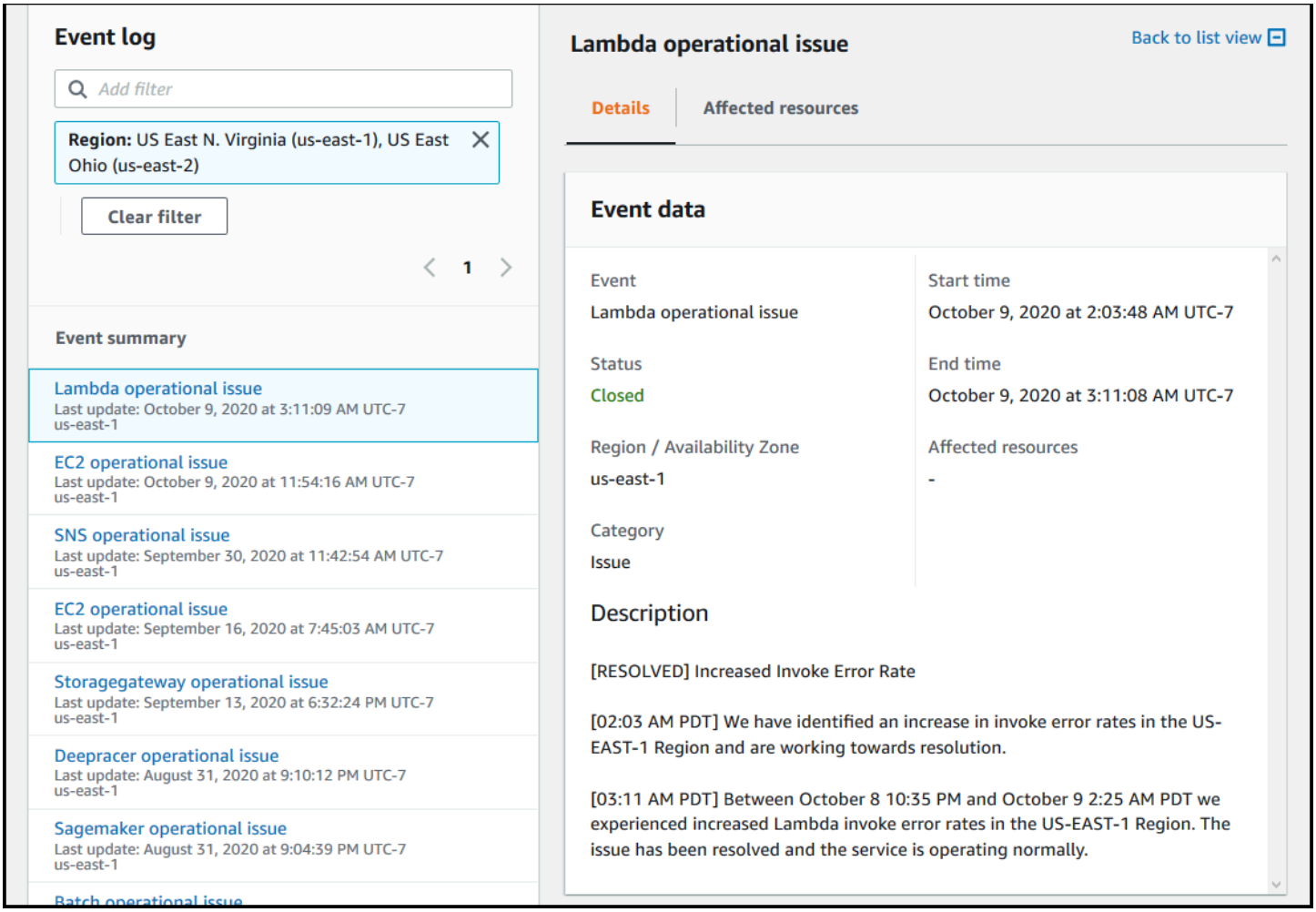
影響を受けるリソースタブには、イベントによって影響を受ける AWS リソースに関する次の情報が表示されます。

- リソース ID (などの Amazon EBSボリューム ID などvol-a1b2c34f) または Amazon リソースネーム (ARN) が使用可能または関連している場合。
- 計画されたライフサイクルイベントの場合、この影響を受けるリソースリストにはリソースの最新のステータス ([保留中]、[不明]、[解決済み]) も含まれています。このリストは、通常、24 時間ごとに更新されます。

リソースに表示される項目を絞り込むことができます。リソース ID または で結果を絞り込むことができますARN。

Example の : AWS Health event AWS Lambda

次のスクリーンショットは、Lambda に対するイベントの例を示しています。



イベントタイプ

AWS Health イベントには 2 つのタイプがあります。

- パブリックイベントは、アカウント固有ではないサービスイベントです。例えば、 EC2で Amazon に問題がある場合 AWS リージョン、 は、そのリージョンでサービスやリソースを使用していない場合でも、イベントに関する情報 AWS Health を提供します。
- アカウント固有のイベントは、アカウントまたは組織内のアカウントに固有です。例えば、使用するリージョンの Amazon EC2インスタンスに問題がある場合、 はイベントに関する情報と影響を受ける Amazon EC2インスタンスのリスト AWS Health を提供します。

次のオプションを使用して、イベントがパブリックかアカウント固有かを識別できます。

- AWS Health ダッシュボードで、イベントの影響を受けるリソースタブを選択します。リソースがあるイベントは、アカウントに固有です。リソースのないイベントはパブリックであり、アカウン

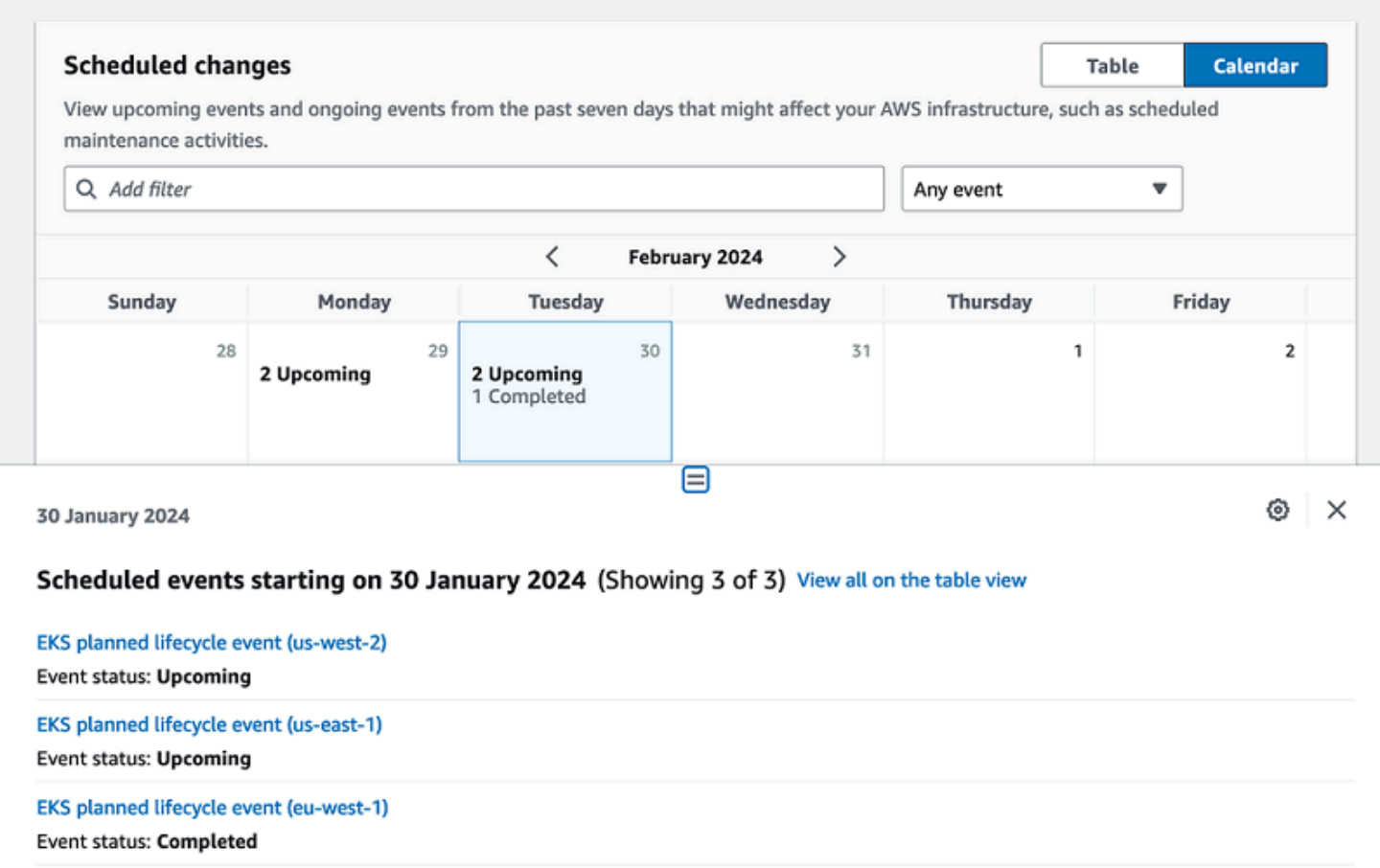
ト固有のものではありません。詳細については、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

- パラメータを AWS Health API返すには、 `eventScopeCode`を使用します。イベントには `PUBLIC`、`ACCOUNT_SPECIFIC`、または `NONE` の値を指定できます。詳細については、「 AWS Health APIリファレンス」の「 DescribeEventDetailsオペレーション」を参照してください。

カレンダービュー

カレンダービューは、スケジュールされた変更タブでイベントを毎月のカレンダー AWS Health に射影できます。このビューでは、過去 3 か月前までと今後 1 年の予定されている変更を確認できます。

AWS Health イベントは日付別に表示されます。日付を選択すると、 AWS Health イベントの詳細を含むサイドパネルが表示されます。[今後開催される] または [進行中] のイベントは黒く表示されます。[完了した] イベントは灰色で表示されます。1 つの日付に 3 つ以上のイベントがある場合は、黒とグレーのイベントの数だけが表示されます。日付を選択すると、サイドパネルに AWS Health イベントのリストが表示されます。サイドパネルでイベントを選択すると、そのイベントに関する情報を表示できます。サイドパネルには以前のビューに移動するためのパンくずリストがあります。



影響を受けるリソースビュー

AWS Health イベントは、影響を受ける正確なリソースを指定する場合があります。影響を受けるリソースは、 AWS Health イベントの「影響を受けるリソース」タブで表示できます。ステータスを表示するには、 AWS Health イベントを選択します。ステータスはサイドパネルの[影響を受けるリソース]タブに表示されます。計画されたライフサイクルイベントの場合、 AWS Health イベントは影響を受けるリソースのステータスを毎日更新します。

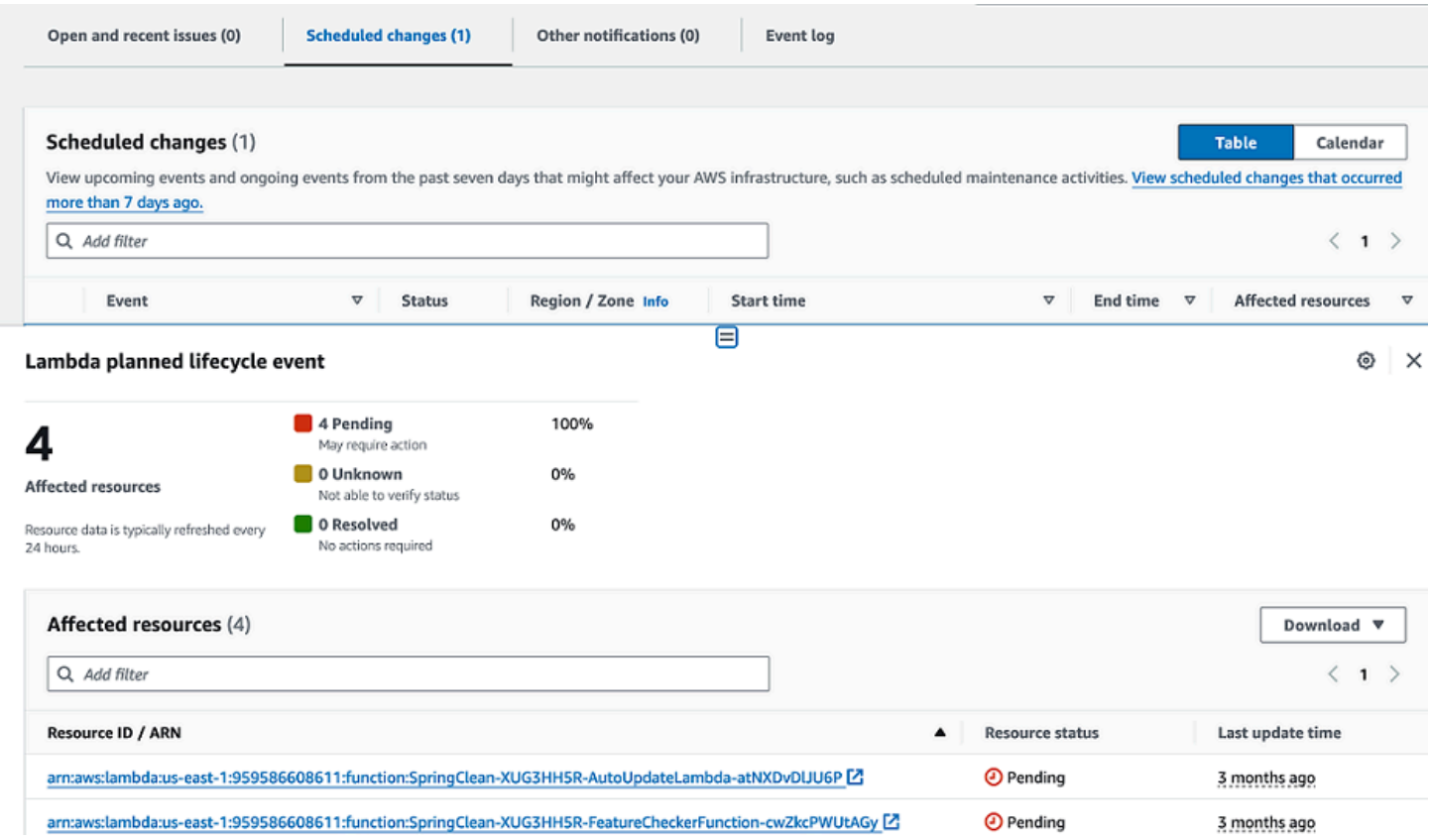
アカウントレベルの AWS Health イベントでは、影響を受けるリソースタブの上部に、影響を受けるリソースのステータスの概要が表示されます。影響を受けるリソースの一覧が、対応するステータスとともにテーブルに表示されます。計画ライフサイクルイベントは、[リソースステータス]フィールドを使用するイベントタイプの一例です。計画されたライフサイクルイベントの詳細については、の計画されたライフサイクルイベント AWS Healthを参照してください。

組織ビューにアクセスすると、 AWS Health イベントには、含まれているすべてのアカウントの影響を受けるすべてのリソースのステータスの概要が表示されます。概要の後には、影響を受けるアカウ

ントのリストと、そのアカウントの保留中のリソースの数が表示されます。アカウント番号または保留中のリソースの数を選択すると、アカウントビューの概要が表示されます。アカウントビューの概要には、影響を受けるアカウントの組織リストに戻るためのパンくずリストがあります。影響を受けるリソースステータスの概要は、分割パネルの上部に表示されます。

影響を受けるリソースのリストは、影響を受けるリソースタブの CSVまたは JSON形式でダウンロードできます。組織ビューでは、ダウンロードされたファイルには、リストされているアカウントのすべてのリソースが含まれます。組織ビューのアカウントレベルに移動して、ダウンロードしたファイルにそのアカウントのリソースのみを含めます。ダウンロードされたファイル内の影響を受ける各リソースには、 AWS アカウント ID、イベント ARN、エンティティ名、エンティティ ARN、ステータス、およびリソースの最終更新時刻が含まれます。フィルターがアクティブ化されている場合、ダウンロードされたファイルにはフィルタリングされた結果のみが含まれます。

一度にダウンロードできるファイルは 1 つだけです。ファイルは自動的にブラウザのデフォルトのダウンロードフォルダにダウンロードされ、、イベントタイトル AWS リージョン、イベント開始日、ダウンロード日に基づくプリセットファイル名が付けられます。



タイムゾーン設定

イベントは、ローカルタイムゾーンの AWS Health Dashboard または で表示できますUTC。 AWS Health ダッシュボードのタイムゾーンを変更すると、ダッシュボードのすべてのタイムスタンプとパブリックイベントは、指定したタイムゾーンに更新されます。

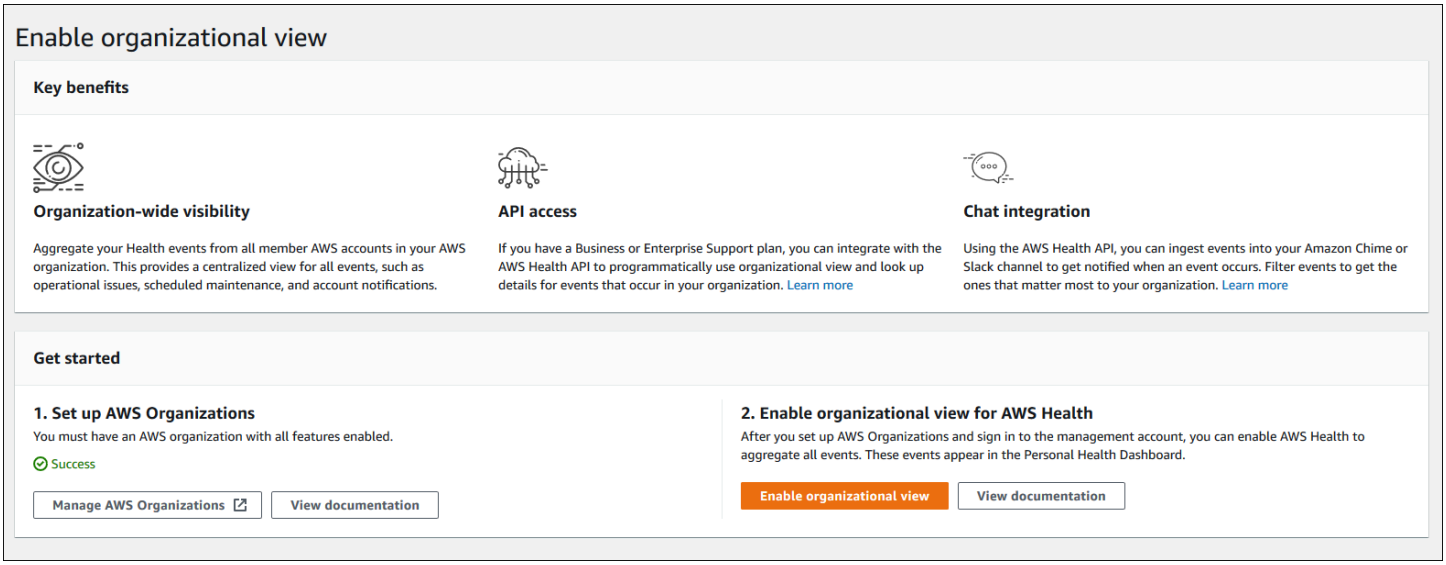
タイムゾーン設定を更新するには

1. ホーム で AWS Health https://health.aws.amazon.com/health/Dashboard を開きます。
2. ページの下部で、[クッキーの基本設定] を選択します。
3. 機能クッキーには [許可] を選択します。次に [基本設定の保存] を選択します。
4. AWS Health ダッシュボードのナビゲーションペインで、タイムゾーン設定 を選択します。
5. AWS Health ダッシュボードセッションのタイムゾーンを選択します。次に、変更の保存を選択します。

組織のヘルス

AWS Health は と統合 AWS Organizations されているため、組織の一部であるすべてのアカウントのイベントを表示できます。これにより、組織に表示されるイベントの一元化されたビューが提供されます。これらのイベントを使用して、リソース、サービス、およびアプリケーションの変更を監視できます。

詳細については、「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。



Amazon を設定する EventBridge

を使用して EventBridge 、 AWS Health イベントの変更を検出して対応します。アカウントで発生する特定の AWS Health イベントをモニタリングし、イベントが変更されたときに が AWS Health 通知するか、アクションを実行するようにルールを設定できます。

EventBridge で を使用する AWS Health

1. ホーム で AWS Health https://health.aws.amazon.com/health/Dashboard を開きます。
2. EventBridge コンソールに移動してルールを作成するには、次のいずれかを実行します。
   - ナビゲーションペインの Health Integrations で、Amazon EventBridgeを選択します。
   - の設定 で EventBridge、 に移動 EventBridgeを選択します。
3. この手順に従って、ルールを作成しイベントを監視します。「Amazon による AWS Health イベントのモニタリング EventBridge」を参照してください。

AWS Health 対応

Aware を使用して を開始 AWS Health APIできます。これは、Slack、 JIRA ServiceNow などにヘルスイベントを送信するために使用できる低コストのアプリケーションです。 AWS Health

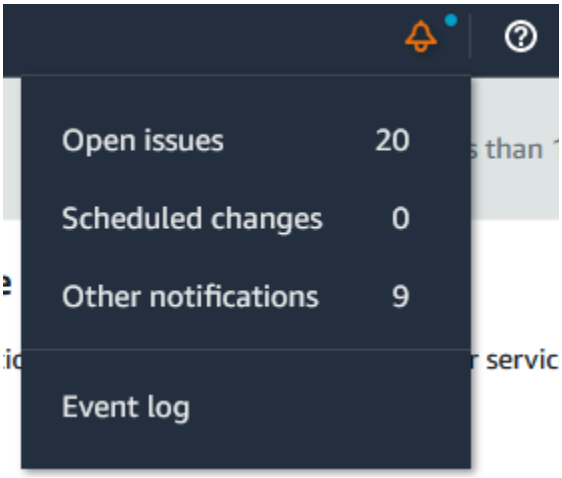
AWS Health イベントのアラート

AWS Health ダッシュボードのコンソールナビゲーションバーに、アラートメニュー付きのベルアイコンがあります。この機能は、各カテゴリのダッシュボードに表示される最近の AWS Health イベントの数を表示します。このベルアイコンは、Amazon 、Amazon Relational Database Service (Amazon RDS) EC2、 AWS Identity and Access Management （ IAM ）、 などの複数の AWS コンソールに表示されます AWS Trusted Advisor。

ベルアイコンを選択して、アカウントが最近のイベントから影響を受けているかを確認します。その後、イベントを選択して AWS Health ダッシュボードに移動し、詳細を確認できます。

Example : 未解決のイベント

以下の画像は、アカウントの未解決のイベントと通知イベントを示しています。


Open issues 20
Scheduled changes 0
Other notifications 9
Event log

AWS HealthへのAWSユーザーへの通知を設定する

AWS Healthは運用上の問題、計画メンテナンス、計画ソフトウェアライフサイクルイベントなど、サービス運用に関する情報を出力する機能があります。影響を受けるリソース ID、現在のステータス (オープンまたはクローズ)、リソースステータスなどのAWS Healthイベントの詳細を包括的に把握するには、AWS Health API、Amazon EventBridge の aws.health ソース、AWS Healthダッシュボードなどの AWS Healthエンドポイントを使用するのがベストプラクティスです。これらのエンドポイントにより、ワークロードに影響する可能性のある進行中のイベントや変更に関する最も詳細でリアルタイムの情報が取得できます。

AWSユーザー通知は、追加のUXチャネル (電子メール、チャット、またはAWSコンソールモバイルアプリケーションへのプッシュ通知) を通じて通知されます。 AWS Healthイベント通知には、上記のエンドポイントほど詳細なデータは含まれていませんが、問題や変更を利害関係者に通知する簡単で効果的な方法となります。作成したルールで指定した値とイベントが一致すると、ユーザー通知は作成したルールに基づいて通知を作成し、送信します。通知を送信する UX 配信チャネルを選択し、集計を設定することにより特定のイベントに対して生成される通知の数を減らすことができます。通知は、コンソール通知センターで表示することもできます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど、AWSアカウント内にアップデートが予定されているリソースがある場合、 チャット通知を受け取ることができます。

AWSユーザー通知の設定について詳しくは、「AWSユーザー通知入門」を参照してください。

AWS Health API へのアクセス

AWS Health は、トランスポートとして HTTPS を使用し、メッセージシリアライズフォーマットとして JSON を使用する RESTful なウェブサービスです。アプリケーションコードから直接、AWS Health API にリクエストを行うことができます。この REST API を直接使用するときは、リクエストの署名と認証のためのコードを書く必要があります。AWS Health が提供するオペレーションとパラメータの詳細については、AWS Health API リファレンスを参照してください。

> **Note**
>
> AWS Health API を使用するには、AWS Support のビジネス、エンタープライズ On-Ramp、またはエンタープライズのサポートプランが必要です。ビジネス、エンタープライズ On-Ramp、またはエンタープライズのサポートプランのない AWS アカウントから AWS Health APIを呼び出した場合は、`SubscriptionRequiredException` エラーが表示されます。

AWS SDK を使用して AWS Health REST API コールをラップすることで、アプリケーション開発を簡素化できます。開発者が AWS 認証情報を指定すれば、ライブラリによって認証とリクエスト署名の処理が自動的に行われます。

AWS Health では、AWS Management Consoleに AWS Health ダッシュボードが用意されており、イベントや影響を受けるエンティティを表示および検索できます。「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

エンドポイント

AWS Health API はマルチリージョンアプリケーションアーキテクチャに従い、アクティブ/パッシブ構成に 2 つのリージョンエンドポイントがあります。アクティブ/パッシブ DNS フェイルオーバーをサポートするために、AWS Health は単一のグローバルエンドポイントを提供します。グローバルエンドポイントで DNS ルックアップを実行して、アクティブなエンドポイントおよび対応する署名 AWS リージョンを判別できます。これにより、コードでどのエンドポイントを使用するかを把握できるため、AWS Health から最新の情報を取得できます。

グローバルエンドポイントにリクエストを行うときは、ターゲットとするリージョンエンドポイントに AWS アクセス認証情報を指定し、リージョンの署名を設定します。それ以外の場合は、認証が失敗することがあります。詳細については、「AWS Health API リクエストの署名」を参照してください。

次の表は、デフォルトの設定を示しています。

説明	署名リージョン	エンドポイント	プロトコル
[Active] (アクティブ)	us-east-1	health.us-east-1.amazonaws.com	HTTPS
パッシブ	us-east-2	health.us-east-2.amazonaws.com	HTTPS
グローバル	us-east-1 **Note** これは、現在のアクティブなエンドポイントの署名リージョンです。	global.health.amazonaws.com	HTTPS

エンドポイントがアクティブなエンドポイントであるかどうかを判断するには、グローバルエンドポイント CNAME で DNS ルックアップを実行し、解決された名前から AWS リージョンを抽出します。

Example : グローバルエンドポイントでの DNS ルックアップ

次のコマンドは、global.health.amazonaws.com エンドポイントでの DNS ルックアップを実行します。次に、このコマンドは us-east-1 リージョンエンドポイントを返します。この出力は、AWS Health にどのエンドポイントを使用する必要があるのかを示しています。

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

Tip

アクティブなエンドポイントとパッシブなエンドポイントの両方が AWS Health データを返します。ただし、最新の AWS Health データは、アクティブなエンドポイントからのみ提供

されます。パッシブなエンドポイントからのデータは、最終的にアクティブなエンドポイントと一致します。アクティブなエンドポイントが変更された場合は、ワークフローを再起動することをお勧めします。

高可用性エンドポイントのデモの使用

次のコード例では、AWS Health はグローバルエンドポイントに対して DNS ルックアップを使用し、アクティブなリージョンエンドポイントと署名リージョンを判断します。アクティブなエンドポイントが変更されると、コードはワークフローを再開します。

トピック

Java のデモの使用

前提条件

Gradle をインストールする必要があります。

Java の例を使用するには

1. GitHub からAWS Health 高可用性エンドポイントのデモをダウンロードします。
2. デモプロジェクトの high-availability-endpoint/java ディレクトリに移動します。
3. コマンドラインウィンドウで次のコマンドを入力します。

```
gradle build
```

4. 次のコマンドを入力して AWS 認証情報を指定します。

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. 次のコマンドを入力してデモを実行します。

```
gradle run
```

Example : AWS Health イベント出力

このコード例は、AWS アカウントの過去 7 日間の最新の AWS Health イベントを返します。次の例では、出力に AWS Config サービスの AWS Health イベントが含まれています。

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
```

```
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'
```

```
If you have any questions regarding this deprecation plan, please contact AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Java リソース

- 詳細については、AWS SDK for Java API リファレンスの Interface HealthClient およびソースコードを参照してください。
- DNS ルックアップのこのデモで使用しているライブラリの詳細については、GitHub で dnsjava を参照してください。

Python デモの使用

前提条件

Python 3 をインストールする必要があります。

Python の例を使用するには

1. GitHub からAWS Health 高可用性エンドポイントのデモをダウンロードします。
2. デモプロジェクトの high-availability-endpoint/python ディレクトリに移動します。
3. コマンドラインウィンドウで次のコマンドを入力します。

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Python 3.3 以降では、virtualenv をインストールする代わりに、組み込みの venv モジュールを使用して仮想環境を作成できます。詳細については、Pythonのウェブサイトで venv - Creation of virtual environments を参照してください。

```
python3 -m venv v-aws-health-env
```

4. 次のコマンドを入力して仮想環境をアクティブ化します。

```
source v-aws-health-env/bin/activate
```

5. 次のコマンドを入力して依存関係をインストールします。

```
pip install -r requirements.txt
```

6. 次のコマンドを入力して AWS 認証情報を指定します。

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. 次のコマンドを入力してデモを実行します。

```
python3 main.py
```

Example : AWS Health イベント出力

このコード例は、AWS アカウントの過去 7 日間の最新の AWS Health イベントを返します。次の出力は、AWS セキュリティ通知の AWS Health イベントを返します。

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
```

```
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. 完了したら、次のコマンドを入力して仮想マシンを無効にします。

```
deactivate
```

Python リソース

- `Health.Client` の詳細については、AWS SDK for Python (Boto3) API リファレンスを参照してください。
- DNS ルックアップのこのデモで使用しているライブラリの詳細については、GitHub で dnspython ツールキットとソースコードを参照してください。

AWS Health API リクエストの署名

AWS SDK または AWS Command Line Interface (AWS CLI) を使用して AWS へのリクエストを行う場合、これらのツールで、設定時に指定されたアクセスキーを使用して自動的にリクエストに署名されます。例えば、以前の高可用性エンドポイントデモの AWS SDK for Java を使用する場合、自分でリクエストに署名する必要はありません。

Java コードの例

AWS SDK for Java で AWS Health API を使用する方法の例については、このコード例を参照してください。

リクエストを行うときに、AWS Health への通常のアクセスには、AWS ルートアカウントの認証情報を使用しないことを強くお勧めします。IAM ユーザーの認証情報を代わりに使用できます。詳細については、IAM ユーザーガイドの AWS アカウントのルートユーザーアクセスキーをロックするを参照してください。

AWS SDK も AWS CLI も使用しない場合は、リクエストを自分で署名する必要があります。AWS 署名バージョン 4 を使用することをお勧めします。詳細については、『AWS』の「AWS 全般のリファレンス API リクエストの署名」を参照してください。

AWS Health でサポートされているオペレーション

AWS Health では、AWS アカウントに影響するイベントの情報を入手するためのオペレーションとして以下がサポートされています。

- AWS Health でサポートされているイベントタイプ。
- 指定したフィルタ条件に一致する 1 つ以上のイベントの情報。
- 1 つ以上のイベントから影響を受けるエンティティの情報。
- 指定したフィルタ条件に一致するイベントやエンティティの分類別の数。

すべてのオペレーションは変化を伴いません。つまり、データは取得されますが、変更されることはありません。以下のセクションでは、AWS Health オペレーションの概要を示します。

イベントタイプ

DescribeEventTypes オペレーションでは、オプションで指定したフィルタに一致するイベントタイプを取得します。イベントタイプは、イベントに関する AWS のサービス、イベントタイプコード、およびカテゴリのテンプレート定義です。イベントタイプとイベントは、オブジェクト指向プログラミングのクラスとオブジェクトに似ています。AWS Health でサポートされるイベントタイプの数は、時間とともに増えます。

のイベント

DescribeEvents オペレーションでは、AWS アカウントに関連するイベントについての概要情報を取得します。イベントは、AWS のオペレーションの問題、AWS インフラストラクチャの予定された変更、またはセキュリティと請求の通知に関連している場合があります。DescribeEventDetails オペレーションでは、1 つ以上のイベントの詳細情報を取得します。たとえば、AWS のサービス、リージョン、アベイラビリティーゾーン、イベントの開始時刻と終了時刻、テキストの説明などが該当します。

影響を受けるエンティティ

DescribeAffectedEntities オペレーションでは、1 つ以上のイベントから影響を受けるエンティティの情報を取得します。表示された結果は、追加の条件 (AWS のリソースに割り当てられているステータスなど) を指定してフィルタできます。

集約

DescribeEventAggregates オペレーションでは、イベントタイプのカテゴリ別のイベント数を取得します。カテゴリは、必要に応じてその他の条件でフィルタすることもできます。DescribeEntityAggregates オペレーションは、1 つ以上の指定したイベントから影響を受けるエンティティ (リソース) の数を取得します。

AWS Organizations および組織ビュー

DescribeEventsForOrganization

DescribeEventsForOrganization は、指定されたフィルタ条件を満たす AWS Organizations 全体のイベントに関する概要情報を返します。

DescribeAffectedAccountsForOrganization

DescribeAffectedAccountsForOrganization は、指定されたイベントの影響を受けている AWS Organizations の AWS アカウントのリストを返します。

DescribeEventDetailsForOrganization

DescribeEventDetailsForOrganization は、AWS Organizations の 1 つ以上のアカウントの 1 つ以上の指定されたイベントに関する詳細情報を返します。

DescribeAffectedEntitiesForOrganization

DescribeAffectedEntitiesForOrganization は、フィルタ条件に基づいて、組織の 1 つ以上のアカウントの 1 つ以上のイベントの影響を受けているエンティティのリストを返します。

EnableHealthServiceAccessForOrganization

EnableHealthServiceAccessForOrganization オペレーションは、お客様に代わって AWS Organizations とやり取りするためのアクセス許可を AWS Health サービスに付与し、サービスにリンクされたロールを組織の管理アカウントに適用します。

DisableHealthServiceAccessForOrganization

DisableHealthServiceAccessForOrganization オペレーションは、AWS Health サービスがお客様に代わって AWS Organizations とやり取りするためのアクセス許可を取り消します。

DescribeHealthServiceStatusForOrganization

DescribeHealthServiceStatusForOrganization オペレーションは、AWS Health による組織の操作の有効化または無効化に関するステータス情報を表示します。

これらのオペレーションの詳細については、AWS Health API リファレンスを参照してください。

AWS Health API 用の Java コード例

以下の Java コード例では、AWS Health クライアントを初期化して、イベントやエンティティの情報を取得する方法を示します。

ステップ 1: 認証情報を初期化する

AWS Health API との通信には、有効な認証情報が必要です。AWS アカウントに関連付けられている IAM ユーザーのキーペアを使用できます。

AWSCredentials インスタンスを作成して初期化します。

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

ステップ 2: AWS Health API クライアントを初期化する

前のステップで初期化した認証情報オブジェクトを使用して、AWS Health クライアントを作成します。

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

ステップ 3: AWS Health API オペレーションを使用してイベント情報を取得する

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
```

```
List<Event> resultEvents = response.getEvents();

Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
```

```
import com.amazonaws.services.health.model.EventDetails;


DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);
```

```
for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

のセキュリティ AWS Health

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

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

- クラウドのセキュリティ — クラウドで AWS サービスを実行するインフラストラクチャを保護する責任 AWS は にあります AWS 。 AWS また、 では、安全に使用できるサービスも提供しています。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS Health、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

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

トピック

- でのデータ保護 AWS Health
- AWS Healthのためのアイデンティティおよびアクセス管理
- での口グ記録とモニタリング AWS Health
- のコンプライアンス検証 AWS Health
- の耐障害性 AWS Health
- AWS Health内のインフラストラクチャセキュリティ
- での設定と脆弱性の分析 AWS Health
- AWS Healthのセキュリティに関するベストプラクティス

でのデータ保護 AWS Health

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Health。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS 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FAQ」を参照してください。欧州におけるデータ保護の詳細については、AWS 「 セキュリティブログ」のAWS 「責任共有モデル」とGDPRブログ記事を参照してください。

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

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して APIおよびユーザーアクティビティの ログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS サービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、、 AWS Health または を使用して または他の AWS サービス を操作する場合API AWS CLIも同様です AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

データ暗号化

がデータを AWS Health 暗号化する方法については、以下の情報を参照してください。

データ暗号化とは、転送中 (サービスから AWS アカウントに移動するとき) および保管中 (AWS サービスに保存されているとき) のデータを保護することです。Transport Layer Security (TLS) を使用して転送中のデータを保護するか、クライアント側の暗号化を使用して保管中のデータを保護できます。

AWS Health は、E メールアドレスや顧客名などの個人識別情報 (PII) をイベントに記録しません。

保管中の暗号化

によって保存されるすべてのデータは AWS Health 、保管時に暗号化されます。

転送中の暗号化

との間で送受信されるすべてのデータは AWS Health 、転送中に暗号化されます。

キー管理

AWS Health は、 AWS クラウドで暗号化されたデータのカスタマーマネージド暗号化キーをサポートしていません。

AWS Healthのためのアイデンティティおよびアクセス管理

AWS Identity and Access Management （ IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS サービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Health リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS サービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- と の AWS Health 連携方法 IAM
- AWS Health アイデンティティベースのポリシーの例
- AWS Health ID とアクセスのトラブルシューティング
- AWS Healthのサービスにリンクされたロールの使用
- AWS の マネージドポリシー AWS Health

対象者

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

サービスユーザー – AWS Health サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS Health 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 AWS Health機能にアクセスできない場合は、「AWS Health ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS Health リソースを担当している場合は、通常、 へのフルアクセスがあります AWS Health。サービスユーザーがどの AWS Health 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、 の基本概念を理解してくださいIAM。会社で を使用する方法の詳細については、IAM AWS Health「」を参照してくださいと の AWS Health 連携方法 IAM。

IAM 管理者 – IAM管理者の場合は、 へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります AWS Health。で使用できる AWS Health アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してくださいAWS Health アイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAMユーザーとしてAWS アカウントのルートユーザー、または IAMロールを引き受けることによって認証 （ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 にサインインする方法 AWS アカウントAWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は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、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、「 IAMユーザーガイド」のAWS API「リクエストの署名」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「 ユーザーガイド」の「 での多要素認証 (MFA) AWS IAM の使用」を参照してください。

AWS アカウントのルートユーザー

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

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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、「 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でアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクション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、 という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールの代わりに) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーと似ていますが、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS サービス、(ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS サービス を使用します AWS サービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び

出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。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 – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS サービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。 AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」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、「 ユーザーガイド」の「 (ユーザーではなく) IAMロールを作成する場合IAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは AWS 、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下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。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できますAPI。

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のポリシーは、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アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーとインラインポリシーのどちらかを選択する方法については、IAM ユーザーガイドの「管理ポリシーとインラインポリシーの選択」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、リソースにアタッチする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の例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。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コントロールできます。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 サービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーIAMでは、 の AWS 管理ポリシーを使用できません。

AWS Health はリソースベースの条件をサポートします。ユーザーが表示できる AWS Health イベントを指定できます。例えば、 内の特定の Amazon EC2イベントへのIAMユーザーアクセスのみを許可するポリシーを作成できます AWS Health Dashboard。

詳細については、「リソース」を参照してください。

アクセスコントロールリスト

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、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。

AWS Health は をサポートしていませんACLs。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal`

フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理する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 (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCP を制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」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、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、 ユーザーガイドの「ポリシー評価ロジックIAM」を参照してください。

と の AWS Health 連携方法 IAM

IAM を使用して へのアクセスを管理する前に AWS Health、 で使用できるIAM機能を理解しておく必要があります AWS Health。 AWS Health およびその他の AWS のサービスが と連携する方法の概要を把握するにはIAM、「 IAMユーザーガイド」のAWS 「 と連携IAMする のサービス」を参照してください。

トピック

- AWS Health アイデンティティベースのポリシー
- AWS Health リソースベースのポリシー
- AWS Health タグに基づく認可

- AWS Health IAM ロール

AWS Health アイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否された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。 は、特定のアクション、リソース、および条件キー AWS Health をサポートします。JSON ポリシーで使用するすべての要素については、ユーザーガイドのIAMJSON「ポリシー要素のリファレンスIAM」を参照してください。

アクション

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下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`要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

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

のポリシーアクションは、アクションの前にプレフィックス AWS Health を使用しますhealth:。例えば、 DescribeEventDetailsAPIオペレーションで指定されたイベントに関する詳細情報を表示するアクセス許可をユーザーに付与するには、ポリシーに `heath:DescribeEventDetails`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。 は、このサービスで実行できるタスクを記述する独自のアクションのセット AWS Health を定義します。

単一のステートメントに複数の アクションを指定するには、次のようにコンマで区切ります。

```
"Action": [
      "health:action1",
      "health:action2"
```

ワイルドカード *を使用して複数のアクションを指定することができます。例えば、`Describe` 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": "health:Describe*"
```

AWS Health アクションのリストを確認するには、「 ユーザーガイド」の「 で定義されるアクション AWS HealthIAM」を参照してください。

リソース

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

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

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

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

AWS Health イベントには、次の Amazon リソースネーム (ARN) 形式があります。

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

例えば、 ステートメントで EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456イベントを指定するには、次の を使用しますARN。

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

特定のアカウントEC2に属する Amazon のすべての AWS Health イベントを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

の形式の詳細についてはARNs、「Amazon リソースネーム (ARNs) 」および AWS 「サービス名前空間」を参照してください。

一部の AWS Health アクションは、特定のリソースで実行できません。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": "*"
```

AWS Health API オペレーションには複数のリソースが含まれる場合があります。例えば、DescribeEventsオペレーションは、指定されたフィルター条件を満たすイベントに関する情報を返します。つまり、 IAM ユーザーはこのイベントを表示するためのアクセス許可を持っている必要があります。

1 つのステートメントで複数のリソースを指定するには、 をカンマARNsで区切ります。

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health は、ヘルスイベントと DescribeAffectedEntitiesおよび DescribeEventDetailsAPIオペレーションのリソースレベルのアクセス許可のみをサポートします。詳細については、「リソースおよびアクションに基づく条件」を参照してください。

AWS Health リソースタイプとその のリストを確認するにはARNs、「 IAMユーザーガイド」の「 で定義されるリソース AWS Health」を参照してください。各リソースARNの を指定できるアクションについては、「 で定義されるアクション AWS Health」を参照してください。

条件キー

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下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 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、IAMユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」を参照してください。

AWS Health は独自の条件キーのセットを定義し、一部のグローバル条件キーの使用もサポートします。すべての AWS グローバル条件キーを確認するには、「 IAMユーザーガイドAWS 」の「グローバル条件コンテキストキー」を参照してください。

DescribeAffectedEntities および DescribeEventDetailsAPIオペレーションは、`health:eventTypeCode`および `health:service`条件キーをサポートします。

AWS Health 条件キーのリストを確認するには、「 IAMユーザーガイド」の「 の条件キー AWS Health」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、「 で定義されるアクション AWS Health」を参照してください。

例

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

AWS Health 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、指定されたプリンシパルが AWS Health リソースに対して実行できるアクションと条件を指定するJSONポリシードキュメントです。 は、ヘルスイベントのリソースベースのアクセス許可ポリシー AWS Health をサポートします。リソースベースのポリシーでは、リソースごとに他の アカウントに使用許可を付与することができます。リソースベースのポリシーを使用して、 AWS サービスが AWS Health イベントにアクセスすることを許可することもできます。

クロスアカウントアクセスを有効にするには、リソースベースのポリシー で、アカウント全体または別のアカウントのIAMエンティティをプリンシパルとして指定できます。 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_principal.html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 AWS アカウントにある場合は、プリンシパルエンティティにリソースへのアクセス許可も付与する必要があります。アクセス許可は、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、ID ベースのポリシーをさらに付与する必要はありません。詳細については、「 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の違い」を参照してください。 IAM

AWS Health は、 DescribeAffectedEntitiesおよび DescribeEventDetailsAPIオペレーションのリソースベースのポリシーのみをサポートします。これらのアクションをポリシーで指定して、 AWS Health イベントに対してアクションを実行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、フェデレーティッドユーザー) を定義できます。

例

AWS Health リソースベースのポリシーの例を表示するには、「」を参照してくださいリソースおよびアクションに基づく条件。

AWS Health タグに基づく認可

AWS Health では、リソースのタグ付けやタグに基づいたアクセスの制御はサポートされていません。

AWS Health IAM ロール

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

での一時的な認証情報の使用 AWS Health

一時的な認証情報を使用して、フェデレーションでサインインしたり、 IAMロールを引き受けたり、クロスアカウントロールを引き受けたりすることができます。一時的なセキュリティ認証情報を取得するには、 AssumeRoleや などのオペレーションを呼び出し AWS STS APIますGetFederationToken。

AWS Health では、一時的な認証情報の使用がサポートされています。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスにリンクされたロールはIAMアカウントに表示され、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

AWS Health は、 と統合する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。サービスにリンクされたロール

は、AWSServiceRoleForHealth_Organizations と呼ばれます。ロールにアタッチされるのは Health_OrganizationsServiceRolePolicy AWS managed ポリシーです。管理ポリシーでは AWS Health 、 AWS が組織内の他の AWS アカウントからヘルスイベントにアクセスできるようにします。

EnableHealthServiceAccessForOrganization オペレーションを使用して、 アカウントにサービスにリンクされたロールを作成できます。ただし、この機能を無効にする場合は、まず DisableHealthServiceAccessForOrganizationオペレーションを呼び出す必要があります。その後、IAMコンソール、、APIまたは AWS Command Line Interface () IAM を使用してロールを削除できますAWS CLI。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの使用IAM」を参照してください。

詳細については、「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。

サービスロール

この機能により、ユーザーに代わってサービスがサービスロールを引き受けることが許可されます。このロールにより、サービスがお客様に代わって他のサービスのリソースにアクセスし、アクションを完了することが許可されます。サービスロールはIAMアカウントに表示され、アカウントによって所有されます。つまり、IAM管理者はこのロールのアクセス許可を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

AWS Health はサービスロールをサポートしていません。

AWS Health アイデンティティベースのポリシーの例

デフォルトでは、IAMユーザーとロールには AWS Health リソースを作成または変更するアクセス許可はありません。また、、 AWS Management Console AWS CLI、または を使用してタスクを実行することはできません AWS API。IAM 管理者は、必要な特定のリソースに対して特定のAPIオペレーションを実行するアクセス許可をユーザーとロールに付与するIAMポリシーを作成する必要があります。その後、管理者は、これらのアクセス許可を必要とするIAMユーザーまたはグループにこれらのポリシーをアタッチする必要があります。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、 ユーザーガイドのJSON「 タブでのポリシーの作成IAM」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWS Health コンソールを使用する

- 自分の権限の表示をユーザーに許可する
- AWS Health Dashboard および へのアクセス AWS Health API
- リソースおよびアクションに基づく条件

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS Health リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーAWS 」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの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、アクションと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 を使用して送信する必要があることを指定できますSSL。条件を使用して、 などの特定の を通じてサービスアクションが使用される場合に AWS サービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化MFAするために をオンにします。API オペレー

ションが呼び出されるMFAタイミングを要求するには、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「 で保護されたAPIアクセスの設定」を参照してください。

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「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

AWS Health コンソールを使用する

AWS Health コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 AWS アカウント内の AWS Health リソースの詳細を一覧表示および表示できます。最小限必要なアクセス許可よりも制限された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 (IAM 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。

これらのエンティティが引き続き AWS Health コンソールを使用できるようにするには、次の AWS マネージドポリシー をアタッチしますAWSHealthFullAccess。

AWSHealthFullAccess ポリシーでは、エンティティは次のものへのフルアクセスが付与されます。

- AWS Health 組織内のすべてのアカウントの AWS 組織ビュー機能を有効または無効にする
- AWS Health コンソール AWS Health Dashboard の
- AWS Health API オペレーションと通知
- AWS 組織の一部であるアカウントに関する情報を表示する
- 管理アカウントの組織単位 (OU) の表示

Example : AWSHealthFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
        }
    ]
}
```

> **Note**
>
> Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを使用して、AWS Health が組織内の他のアカウントのイベントを表示できるようにすることもできます。詳細については、「AWS Healthのサービスにリンクされたロールの使用」を参照してください。

AWS CLI または のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。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を許可します。

詳細については、「 IAMユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています AWS API。

```
{
    "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": "*"
        }
    ]
}
```

AWS Health Dashboard および へのアクセス AWS Health API

AWS Health Dashboard はすべての AWS アカウントで使用できます。 AWS Health API は、Business、Enterprise On-Ramp、または Enterprise Support プランのアカウントでのみ使用できます。詳細については、「AWS Support」を参照してください。

IAM を使用してエンティティ (ユーザー、グループ、またはロール) を作成し、それらのエンティティに AWS Health Dashboard および へのアクセス許可を付与できます AWS Health API。

デフォルトでは、IAMユーザーは AWS Health Dashboard または にアクセスできません AWS Health API。単一のユーザー、ユーザーのグループ、またはロールにIAMポリシーをアタッチすることで、ユーザーにアカウントの AWS Health 情報へのアクセスを許可します。詳細については、「アイデンティティ (ユーザー、グループ、ロール) 」および「ポリシーの概要」を参照してください。 IAM

IAM ユーザーを作成したら、それらのユーザーに個別のパスワードを付与できます。その後、アカウント固有のサインインページを使用して、アカウントにサインインし、 AWS Health 情報を表示できます。詳細については、「ユーザーがアカウントにサインインする方法」を参照してください。

> **Note**
>
> 表示する権限を持つIAMユーザーは AWS Health Dashboard 、アカウント上のすべての AWS サービスでヘルス情報に読み取り専用でアクセスできます。これには、Amazon EC2インスタンス、EC2インスタンス IP アドレスIDs、一般的なセキュリティ通知IDsなどの AWS リソースが含まれますが、これらに限定されません。
> 例えば、 IAMポリシーが AWS Health Dashboard および AWS Health にのみアクセスを許可する場合API、ポリシーが適用されるユーザーまたはロールは、他のIAMポリシーがそのアクセスを許可していない場合でも、 AWS のサービスおよび関連リソースに関して投稿されたすべての情報にアクセスできます。

APIs には の 2 つのグループを使用できます AWS Health。

- 個々のアカウント – DescribeEventsや などのオペレーションを使用してDescribeEventDetails、アカウントの AWS Health イベントに関する情報を取得できます。
- 組織アカウント – DescribeEventsForOrganizationや などのオペレーションを使用してDescribeEventDetailsForOrganization、組織の一部であるアカウントの AWS Health イベントに関する情報を取得できます。

使用可能なAPIオペレーションの詳細については、「AWS Health APIリファレンス」を参照してください。

個々のアクション

IAM ポリシーの Action要素を に設定できますhealth:Describe*。これにより、 AWS Health Dashboard および へのアクセスが許可されます AWS Health。 AWS Health は、eventTypeCodeおよび サービスに基づくイベントへのアクセスコントロールをサポートします。

アクセスの説明

このポリシーステートメントは、 AWS Health Dashboard および Describe* AWS Health APIオペレーションへのアクセスを許可します。例えば、このポリシーを持つIAMユーザーは、 AWS Health Dashboard の にアクセスして AWS Management Console DescribeEventsAPIオペレーションを AWS Health 呼び出すことができます。

Example : アクセスの説明

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

アクセスを拒否する

このポリシーステートメントは、 AWS Health Dashboard および へのアクセスを拒否します AWS Health API。このポリシーを持つIAMユーザーは、 AWS Health Dashboard で を表示 AWS Management Console できず、 オペレーションを AWS Health API呼び出すこともできません。

Example : アクセスを拒否する

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

```
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

組織ビュー

の組織ビューを有効にする場合は AWS Health、 AWS Health および AWS Organizations アクションへのアクセスを許可する必要があります。

IAM ポリシーの `Action`要素には、次のアクセス許可を含める必要があります。

- `iam:CreateServiceLinkedRole`
- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

各 に必要な正確なアクセス許可についてはAPIs、 IAMユーザーガイドの「 で AWS Health APIs定義されるアクション」および「通知」を参照してください。

> **Note**
>
> の にアクセスするには AWS Health APIs、組織の管理アカウントの認証情報を使用する必要があります AWS Organizations。詳細については、「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。

AWS Health 組織ビューへのアクセス許可

このポリシーステートメントは、組織ビュー機能に必要なすべての AWS Health および AWS Organizations アクションへのアクセスを許可します。

Example : AWS Health 組織ビューへのアクセスを許可する

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

AWS Health 組織ビューへのアクセス拒否

このポリシーステートメントは、 AWS Organizations アクションへのアクセスを拒否しますが、個々のアカウントの AWS Health アクションへのアクセスを許可します。

Example : AWS Health 組織ビューへのアクセスを拒否する

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

> **Note**
>
> アクセス許可を付与するユーザーまたはグループに既に IAMポリシーがある場合は、そのポリシーに AWS Health固有のポリシーステートメントを追加できます。

リソースおよびアクションに基づく条件

AWS Health は、 DescribeAffectedEntitiesおよび DescribeEventDetailsAPIオペレーションIAMの条件をサポートします。リソースおよびアクションベースの条件を使用して、 が AWS Health APIユーザー、グループ、またはロールに送信するイベントを制限できます。

そのためには、IAMポリシーの `Condition`ブロックを更新するか、 `Resource`要素を設定します。文字列条件を使用して、特定の AWS Health イベントフィールドに基づいてアクセスを制限できます。

ポリシーで AWS Health イベントを指定するときは、次のフィールドを使用できます。

- `eventTypeCode`
- `service`

> **メモ**
>
> - DescribeAffectedEntities および DescribeEventDetailsAPIオペレーションは、リソースレベルのアクセス許可をサポートします。例えば、特定の AWS Health イベントを許可または拒否するポリシーを作成できます。
> - DescribeAffectedEntitiesForOrganization および DescribeEventDetailsForOrganizationAPIオペレーションは、リソースレベルのアクセス許可をサポートしていません。
> - 詳細については、「サービス認証リファレンス」の「 および の通知の AWS Health APIs 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。

Example : アクションベースの条件

このポリシーステートメントは、 AWS Health Dashboard および AWS Health `Describe*`APIオペレーションへのアクセスを許可しますが、Amazon に関連する AWS Health イベントへのアクセスを拒否しますEC2。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example : リソースベースの条件

次のポリシーでも結果は同じですが、Resource 要素を代わりに使用しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
```

```
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example : eventTypeCode 条件

このポリシーステートメントは、 AWS Health Dashboard および AWS Health `Describe*`APIオペレーションへのアクセスを許可しますが、 `eventTypeCode`に一致する を持つ AWS Health イベントへのアクセスを拒否します`AWS_EC2_*`。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

> **Important**
>
> DescribeAffectedEntities および DescribeEventDetailsオペレーションを呼び出し、 AWS Health イベントにアクセスするアクセス許可がない場合、`AccessDeniedException`エラーが表示されます。詳細については、「AWS Health ID とアクセスのトラブルシューティング」を参照してください。

AWS Health ID とアクセスのトラブルシューティング

次の情報を使用して、 および の使用時に発生する可能性がある一般的な問題を診断 AWS Health して修正しますIAM。

トピック

- でアクションを実行する権限がない AWS Health
- iam を実行する権限がありません。PassRole
- アクセスキーを表示したい
- 管理者として、他のユーザーにアクセスを許可したい AWS Health
- 自分の AWS アカウント以外のユーザーに自分の AWS Health リソースへのアクセスを許可したい

でアクションを実行する権限がない AWS Health

からアクションを実行する権限がないと AWS Management Console 通知された場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

このAccessDeniedExceptionエラーは、ユーザーに AWS Health Dashboard または AWS Health API オペレーションを使用するアクセス許可がない場合に表示されます。

この場合、ユーザーの管理者はポリシーを更新して、ユーザーアクセスを許可する必要があります。

には、 AWS Health APIのビジネス、エンタープライズオンランプ、またはエンタープライズサポートプランが必要ですAWS Support。Business、Enterprise On-Ramp、または Enterprise Support プランがないアカウント AWS Health APIから を呼び出すと、エラーコード が返されますSubscriptionRequiredException。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS Healthにロールを渡すことができるようにする必要があります。

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

次の例のエラーは、 というIAMユーザーがコンソールを使用して marymajor でアクションを実行しようする場合に発生します AWS Health。ただし、このアクションをサービスが実行するには、

サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

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

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

アクセスキーを表示したい

IAM ユーザーアクセスキーを作成したら、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーを再表示することはできません。シークレットアクセスキーを紛失した場合は、新しいアクセスキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: AKIAIOSFODNN7EXAMPLE) とシークレットアクセスキー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) の 2 つで構成されています。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーは安全に管理してください。

> **Important**
>
> 正規のユーザー ID を確認するためであっても、アクセスキーを第三者に提供しないでください。これにより、自分の への永続的なアクセスを誰かに許可することができます AWS アカウント。

アクセスキーペアを作成する場合、アクセスキー ID とシークレットアクセスキーを安全な場所に保存するように求めるプロンプトが表示されます。このシークレットアクセスキーは、作成時にのみ使用できます。シークレットアクセスキーを紛失した場合は、新しいアクセスキーをIAMユーザーに追加する必要があります。アクセスキーは最大 2 つまで持つことができます。既に 2 つある場合は、新規キーペアを作成する前に、いずれかを削除する必要があります。手順を確認するには、「 ユーザーガイド」の「アクセスキーの管理IAM」を参照してください。

管理者として、他のユーザーにアクセスを許可したい AWS Health

他のユーザーが にアクセスできるようにするには AWS Health、アクセスを必要とするユーザーまたはアプリケーションにアクセス許可を付与する必要があります。を使用して AWS IAM Identity Center ユーザーとアプリケーションを管理する場合は、アクセスレベルを定義するアクセス許可セットをユーザーまたはグループに割り当てます。アクセス許可セットは、ユーザーまたはアプリケーションに関連付けられたIAMロールにIAMポリシーを自動的に作成して割り当てます。詳細については、「 ユーザーガイド」の「アクセス許可セットAWS IAM Identity Center 」を参照してください。

IAM Identity Center を使用していない場合は、アクセスが必要なユーザーまたはアプリケーションのIAMエンティティ (ユーザーまたはロール) を作成する必要があります。次に、 AWS Healthの適切なアクセス許可を付与するポリシーを、そのエンティティにアタッチする必要があります。アクセス許可が付与されたら、ユーザーまたはアプリケーション開発者に認証情報を提供します。これらの認証情報を使用して にアクセスします AWS。IAM ユーザー、グループ、ポリシー、アクセス許可の作成の詳細については、 IAMユーザーガイドのIAM「 でのアイデンティティとポリシー、アクセス許可IAM」を参照してください。

自分の AWS アカウント以外のユーザーに自分の AWS Health リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- がこれらの機能 AWS Health をサポートしているかどうかを確認するには、「」を参照してくださいと の AWS Health 連携方法 IAM。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 ユーザーガイド」の「所有 AWS アカウント している別の のIAMユーザーへのアクセスを提供するIAM」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、 IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、 IAMユーザーガイドの「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション) 」を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、ユーザーガイドの「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

AWS Healthのサービスにリンクされたロールの使用

AWS Health は AWS Identity and Access Management （ IAM ） サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプのIAMロールです AWS Health。サービスリンクロールは、 AWS Health によって事前に定義されたロールであり、お客様から他の AWS サービス を呼び出すために必要なすべてのアクセス許可を備えています。

サービスにリンクされたロールを使用して、必要なアクセス許可を手動で追加 AWS Health しないように を設定できます。 は、サービスにリンクされたロールのアクセス許可 AWS Health を定義します。特に定義されている場合を除き、 のみがそのロールを引き受け AWS Health ることができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

AWS Healthのサービスリンクロールのアクセス許可

AWS Health には 2 つのサービスにリンクされたロールがあります。

- AWSServiceRoleForHealth_Organizations – このロールは AWS Health （ `health.amazonaws.com`) を信頼して、アクセスするロールを引き受け AWS サービス ます。このロールにアタッチされるのは `Health_OrganizationsServiceRolePolicy` AWS マネージドポリシーです。
- AWSServiceRoleForHealth_EventProcessor – このロールは、 AWS Health サービスプリンシパル (`event-processor.health.amazonaws.com`) を信頼してロールを引き受けます。このロールにアタッチされるのは `AWSHealth_EventProcessorServiceRolePolicy` AWS マネージドポリシーです。サービスプリンシパルは、 ロールを使用して、 AWS インシデントの検出と対応用の Amazon EventBridge マネージドルールを作成します。このルールは、 アカウントから AWS アカウント にアラーム状態変更情報を配信するために必要なインフラストラクチャです AWS Health。

AWS 管理ポリシーの詳細については、「」を参照してくださいAWS の マネージドポリシー AWS Health。

AWS Healthのサービスリンクロールの作成

AWSServiceRoleForHealth_Organizations 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。EnableHealthServiceAccessForOrganization オペレーションを呼び出すと、 AWS Health はアカウントでこのサービスにリンクされたロールを作成します。

AWSServiceRoleForHealth_EventProcessor サービスリンクロールはアカウントに手動で作成される必要があります。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの作成IAM」を参照してください。

AWS Healthのサービスにリンクされたロールの編集

AWS Health では、サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、 を使用してロールの説明を編集することはできますIAM。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編集」を参照してください。

AWS Healthのサービスリンクロールの削除

AWSServiceRoleForHealth_Organizations ロールを削除するには、まず DisableHealthServiceAccessForOrganizationオペレーションを呼び出す必要があります。その後、IAMコンソール、、APIまたは AWS Command Line Interface () IAM を使用してロールを削除できますAWS CLI。

AWSServiceRoleForHealth_EventProcessor ロールを削除するには、 に連絡して、 AWS インシデントの検出 AWS Support と対応からワークロードをオフボードするように依頼します。このプロセスが完了したら、IAMコンソール、、APIまたは IAM を使用していずれかのロールを削除できます AWS CLI。

関連情報

詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの使用IAM」を参照してください。

AWS の マネージドポリシー AWS Health

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースに対するアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

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

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

詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

AWS Health には、次の 管理ポリシーがあります。

目次

AWS マネージドポリシー: AWSHealth_EventProcessorServiceRolePolicy

AWS Health は AWSHealth_EventProcessorServiceRolePolicy AWS マネージドポリシーを使用します。このマネージドポリシーは、`AWSServiceRoleForHealth_EventProcessor` サービスリンクロールにアタッチされます。このポリシーは、サービスリンクロールがユーザーに代わってアクションを完了することを許可します。このポリシーをIAMエンティティにアタッチすることはできません。詳細については、「AWS Healthのサービスにリンクされたロールの使用」を参照してください。

マネージドポリシーには、 が AWS インシデント検出と対応用の Amazon EventBridge ルールにアクセス AWS Health できるようにする以下のアクセス許可があります。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `events` – EventBridge ルールを記述および削除し、それらのルールのターゲットを記述および更新します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

ポリシーへの変更のリストについては、「AWS HealthAWS 管理ポリシーの更新」を参照してください。

AWS マネージドポリシー: Health_OrganizationsServiceRolePolicy

AWS Health は Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを使用します。このマネージドポリシーは、`AWSServiceRoleForHealth_Organizations` サービスリンクロール

にアタッチされます。このポリシーは、サービスリンクロールがユーザーに代わってアクションを完了することを許可します。このポリシーをIAMエンティティにアタッチすることはできません。詳細については、「AWS Healthのサービスにリンクされたロールの使用」を参照してください。

このポリシーは、 AWS Health が Health Organizational ビューの必要な AWS Organizations 詳細にアクセスできるアクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `organizations` – Organizations AWS サービス で使用できる AWS Organizations および のアカウントについて説明します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

ポリシーへの変更のリストについては、「AWS HealthAWS 管理ポリシーの更新」を参照してください。

AWS マネージドポリシー: AWSHealthFullAccess

AWS Health は AWSHealthFullAccess AWS マネージドポリシーを使用します。このポリシーは、エンティティ (IAM ユーザーまたはロール) に AWS Health コンソールへのアクセスを許可します。詳細については、「AWS Health コンソールを使用する」を参照してください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `organizations` – AWS Health 組織内のすべてのアカウントの AWS 組織ビュー機能を有効または無効にし、管理アカウントの組織単位 (OU) を表示します。
- `health` – オペレーションと通知へのアクセス AWS Health API
- `iam` – AWS Health サービスにリンクされた IAMロールを作成します。

```
{
    "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
                "Sid": "ServiceLinkAccess",
```

```
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

ポリシーへの変更のリストについては、「AWS HealthAWS 管理ポリシーの更新」を参照してください。

AWS HealthAWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AWS Health 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、のドキュメント履歴 AWS Healthページの RSS フィードをサブスクライブします。

次の表は、2022 年 1 月 13 日以後の AWS Health マネージドポリシーの重要な更新を示しています。

AWS Health

変更	説明	日付
AWS マネージドポリシー: AWSHealthFullAccess – 既存ポリシーへの更新	AWS Health は AWSHealth FullAccess 、ポリシーを AWS GovCloud (US) Regions および中国リージョンに拡張しました。	2023 年 10 月 16 日
AWS マネージドポリシー: Health_OrganizationsService	AWS Health は、サービスにリンクされたロールが で使用できるアカウントと AWS	2023 年 7 月 19 日

変更	説明	日付
RolePolicy – 既存ポリシーへの更新	サービスを記述できるようにする新しい AWS Organizations アクションを追加しました AWS Organizations。	
変更ログが発行されました	AWS Health 管理ポリシーの変更ログ。	2023 年 1 月 13 日

でのログ記録とモニタリング AWS Health

モニタリングは、 AWS Health およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 をモニタリングし AWS Health、問題が発生した場合に報告し、必要に応じてアクションを実行するために、以下のモニタリングツール AWS を提供します。

- Amazon CloudWatch は、 AWS リソースと、 で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのCPU使用状況やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。
- Amazon EventBridge は、 AWS resources. EventBridge enables 自動イベント駆動型コンピューティングの変更を記述するシステムイベントの near-real-time ストリームを提供します。特定のイベントを監視し、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを作成できます。詳細については、「Amazon による AWS Health イベントのモニタリング EventBridge」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

詳細については、「モニタリング AWS Health」を参照してください。

のコンプライアンス検証 AWS Health

AWS 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 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 サービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – 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**
>
> すべての AWS サービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」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 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) など) 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 サービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS 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DSS、 PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- AWS Audit Manager – これにより AWS サービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Health

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

AWS Health イベントは複数のアベイラビリティーゾーンにまたがって保存およびレプリケートされます。このアプローチにより、 AWS Health Dashboard または AWS Health API オペレーションからアクセスできるようになります。 AWS Health イベントは、発生してから最大 90 日間表示できます。

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

AWS Health内のインフラストラクチャセキュリティ

マネージドサービスである AWS Health は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

が AWS 公開したAPI呼び出しを使用して、ネットワーク AWS Health 経由で にアクセスします。クライアントは Transport Layer Security (TLS) 1.0 以降をサポートしている必要があります。1.2 TLS 以降をお勧めします。クライアントは、エフェメラル Diffie-Hellman (PFS) や楕円曲線エフェメラル Diffie-Hellman () などの完全前方秘匿性 (DHE) を持つ暗号スイートもサポートする必要がありますECDHE。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。

さらに、リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID と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。

での設定と脆弱性の分析 AWS Health

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

AWS Healthのセキュリティに関するベストプラクティス

の使用に関する以下のベストプラクティスを参照してください AWS Health。

AWS Health ユーザーに最小限のアクセス許可を付与する

最小権限の原則に従って、 のユーザーおよびグループのアクセスポリシーのアクセス許可には最小限のものを使用します。例えば、 AWS Identity and Access Management （ IAM) ユーザーに へのアクセスを許可するとします AWS Health Dashboard。ただし、同じユーザーに AWS Organizationsへのアクセスを有効または無効にすることを許可しない場合があります。

詳細については、「AWS Health 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。

を表示する AWS Health Dashboard

を AWS Health Dashboard 頻繁にチェックして、アカウントまたはアプリケーションに影響を与える可能性のあるイベントを特定します。例えば、更新が必要な Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど、 リソースに関するイベント通知を受け取る場合があります。

詳細については、「AWS Health ダッシュボードの開始方法 – アカウントのヘルス」を参照してください。

Amazon Chime または Slack AWS Health との統合

をチャットツール AWS Health と統合できます。この統合により、ユーザーとチームが AWS Health イベントについてリアルタイムで通知を受け取ることができます。詳細については、「 のAWS Health ツール」を参照してください GitHub。

AWS Health イベントのモニタリング

Amazon CloudWatch Events AWS Health と統合して、特定のイベントのルールを作成できます。CloudWatch イベントがルールに一致するイベントを検出すると、通知が届き、アクションを実行できます。 CloudWatch イベントイベントはリージョン固有であるため、アプリケーションまたはインフラストラクチャが存在するリージョンでこのサービスを設定する必要があります。

場合によっては、 AWS Health イベントのリージョンを特定できないことがあります。このような場合、デフォルトで米国東部 (バージニア北部)リージョンにイベントが表示されます。このリージョンで CloudWatch イベントを設定して、これらのイベントを確実にモニタリングできます。

詳細については、「Amazon による AWS Health イベントのモニタリング EventBridge」を参照してください。

組織ビューでのアカウント全体の AWS Health イベントの集計

デフォルトでは、AWS Health を使用して 1 つの AWS アカウントの AWS Health イベントを表示できます。AWS Organizations では、組織全体で AWS Health を一元的に表示することもできます。この機能により、1 つのアカウントオペレーションと同じ情報にアクセスできます。フィルターを使用して、AWS の特定のリージョン、アカウント、およびサービスのイベントを表示できます。

イベントを集計し、運用イベントの影響を受けている組織内のアカウントや、セキュリティの脆弱性の通知を受けている組織内のアカウントを特定できます。また、この情報を使用して、組織全体のリソースメンテナンスイベントを事前に管理および自動化することもできます。この機能を使用して、更新またはコードの変更が必要な可能性のある AWS サービスに対する今後の変更について常に最新情報を把握できます。

委任管理者機能を使用して、AWS Health組織ビューへのアクセスをメンバーアカウントに委任するのがベストプラクティスです。これにより、運用チームは組織内のAWS Healthイベントに簡単にアクセスできるようになります。委任管理者機能を使うと、管理アカウントを制限したまま、AWS Healthイベントへの対応に必要な情報をチームが得ることができます。

> **Important**
>
> - AWS Health では、組織ビューを有効にする前に組織内で発生したイベントは記録されません。例えば、この機能を有効にする前に組織内のメンバーアカウント (111122223333) が Amazon Elastic Compute Cloud (Amazon EC2) のイベントを受信した場合、このイベントは組織ビューに表示されません。
> - 組織内のアカウントに送信された AWS Health イベントは、これらのアカウントの 1 つ以上が組織を離れた場合でも、そのイベントが使用可能である限り、組織ビューに最大90日間表示されます。
> - 組織のイベントは、削除されるまで 90 日前使用可能です。このクォータを増やすことはできません。

前提条件

組織ビューを使用する前に、次のことを行う必要があります。

- すべての機能が有効な組織に参加する。
- AWS Identity and Access Management (IAM) ユーザーとして管理アカウントにサインインするか、IAM ロールを引き受ける。

  組織の管理アカウントでルートユーザーとしてサインインすることもできます (推奨されません) 。詳細については、IAM ユーザーガイドの AWS アカウントのルートユーザーアクセスキーをロックするを参照してください。
- IAM ユーザーとしてサインインする場合は、AWSHealthFullAccess ポリシーなど、AWS Health および Organizations アクションへのアクセスを付与する IAM ポリシーを使用します。詳細については、「AWS Health 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。

トピック

組織ビュー (コンソール)

AWS Health コンソールを使用して、AWS 組織内のヘルスイベントを一元的に表示します。

組織ビューは、すべての AWS Support プランで追加コストなしに AWS Health コンソールで使用できます。

> **Note**
>
> 管理アカウントでこの機能へのアクセスをユーザーに許可するには、AWSHealthFullAccess ポリシーなどのアクセス許可が必要です。詳細については、「AWS Health 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。

目次

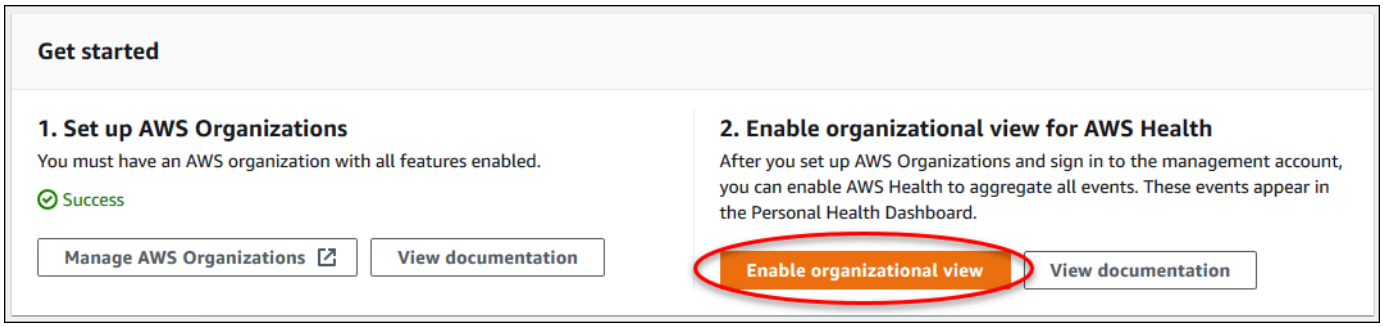
- 予定された変更
- その他の通知
- イベントログ
- 影響を受けるアカウントとリソースの表示 (コンソール)
- 組織ビューの無効化 (コンソール)

組織ビューの有効化 (コンソール)

組織ビューは、AWS Health コンソールから有効にできます。AWS 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。

組織の AWS Health ダッシュボードを表示するには

1. https://health.aws.amazon.com/health/home でAWS Healthダッシュボードを開きます。
2. ナビゲーションペインの [組織の状態] で [構成] を選択します。
3. [Enable organizational view] (組織ビューの有効化) ページで、[Enable organizational view] (組織ビューの有効化) を選択します。



4. (オプション) 組織単位 (OU) の作成など、AWS 組織に変更を加える場合は、[Manage AWS Organizations] (Amazon Organizations の管理) を選択します。

   詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations の使用開始」を参照してください。

> **メモ**
>
> - この機能の有効化は非同期プロセスであり、完了するまでに時間がかかります。組織内のアカウント数によっては、アカウントの読み込みに数分かかる場合があります。そのままにして、後で AWS Health コンソールを確認することができます。

- ビジネスサポートプラン、エンタープライズ On-Ramp サポートプラン、またはエンタープライズサポートプランを使用する場合は、DescribeHealthServiceStatusForOrganization API オペレーションを呼び出して、プロセスのステータスを確認できます。
- この機能を有効にすると、Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを持つ AWSServiceRoleForHealth_Organizations サービスにリンクされたロールが組織内の管理アカウントに適用されます。詳細については、「AWS Health のサービスにリンクされたロールの使用」を参照してください。

組織ビューイベントの表示 (コンソール)

組織ビューを有効にすると、AWS Health は組織内のすべてのアカウントのヘルスイベントを表示します。

アカウントが組織に参加すると、AWS Health は、自動的にそのアカウントを組織ビューに追加します。アカウントが組織から離れると、そのアカウントからの新しいイベントが組織ビューに記録されなくなります。ただし、既存のイベントは残り、90 日間の制限までそのクエリを実行できます。

AWS は、管理者アカウントの閉鎖の発効日から 90 日間にわたり、そのアカウントのポリシーデータを保持します。90 日の期間の終了時、AWS は、アカウントのすべてのポリシーデータを完全に削除します。

- 結果を 90 日を超えて保持するには、ポリシーをアーカイブします。EventBridge ルールを用いてカスタムアクションを使用して、結果を S3 バケットに保存することもできます。
- AWS がポリシーデータを保持している限り、閉鎖されたアカウントを再度開くと、AWS は、アカウントをサービス管理者として再割り当てし、そのアカウントのサービスポリシーデータを回復します。
- 詳細については、「アカウントの解約」を参照してください。

Important

AWS GovCloud (US) リージョンの顧客の場合

- アカウントを閉鎖する前に、アカウントリソースをバックアップしてから、削除します。アカウントを閉鎖した後は、当該アカウントへのアクセス権を失います。

> **Note**
>
> この機能を有効にすると、AWS Health コンソールは過去7日間の AWS Healthダッシュボード – サービスの状態 のパブリックイベントを表示できます。これらのパブリックイベントは、組織内のアカウントに固有のものではありません。AWS Health ダッシュボード – サービスヘルスからのイベントにより、リージョンでのAWSサービスの可用性に関する公開情報が得られます。

次のページで組織ビューイベントを表示できます:.

トピック

- 未解決の問題と最近の問題
- 予定された変更
- その他の通知
- イベントログ

未解決の問題と最近の問題

[未解決の問題と最近の問題]タブを使用して、組織に影響する AWS サービスリソースへの変更など、AWS インフラストラクチャに影響する可能性のあるイベントを表示できます。

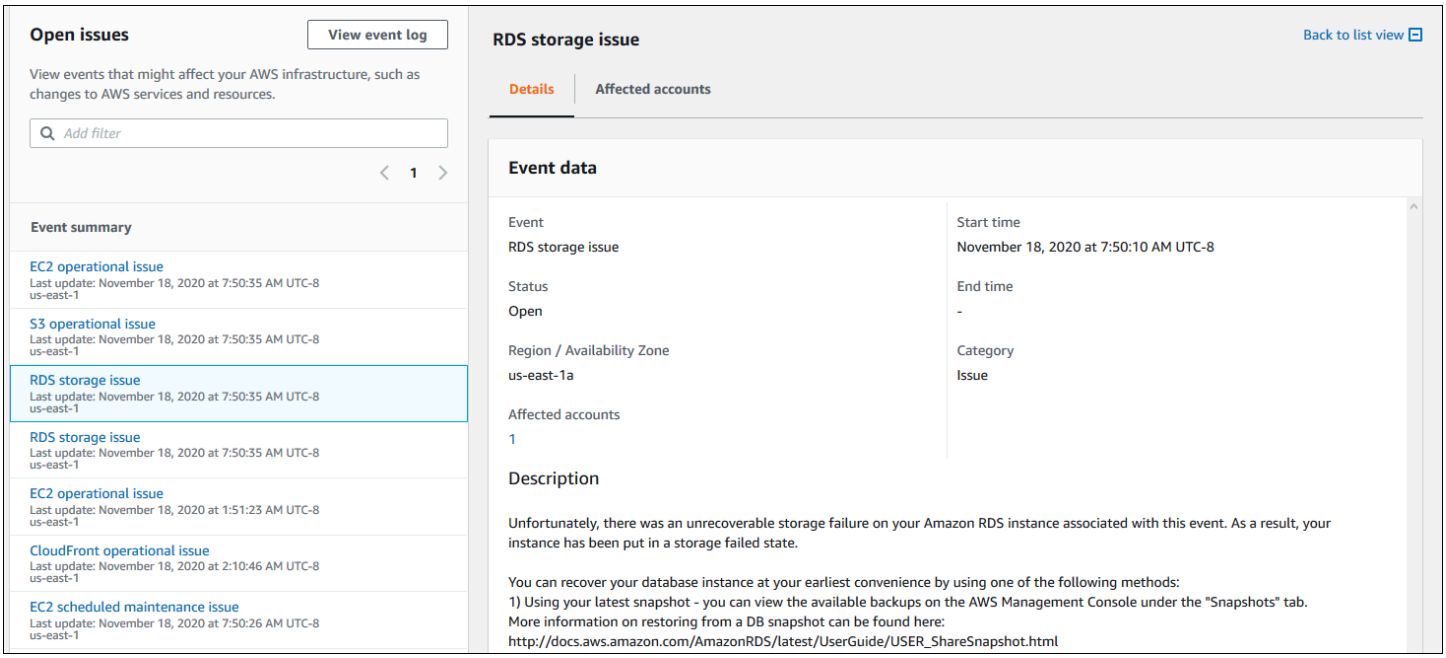
組織ビューイベントの表示するには

1. https://health.aws.amazon.com/health/home でAWS Healthダッシュボードを開きます。
2. ナビゲーションペインの [組織のヘルス] で [未解決の問題と最近の問題] を選択すると、最近報告されたイベントが表示されます。
3. イベントを選択します。[詳細] タブで、イベントに関する次の情報を確認できます。
   - イベント名
   - ステータス
   - リージョン/アベイラビリティーゾーン
   - 影響を受けるアカウント
   - 開始時間
   - 終了時間

- カテゴリ
- 説明

Example ：組織ビューでの未解決問題

次の Amazon Relational Database Service (Amazon RDS) イベントが組織ビューの[未解決の問題と最近の問題]タブに表示され、組織内の1つのアカウントが影響を受けています。



予定された変更

[スケジュールされた変更]タブでは、組織に影響を与える可能性のある今後のイベントを確認できます。これらのイベントには、サービスの定期メンテナンスアクティビティが含まれる場合があります。

その他の通知

[通知]タブでは、過去7日間のその他すべての通知や組織に影響を与える可能性のある進行中のイベントを確認できます。これには、証明書のローテーション、請求通知、セキュリティの脆弱性などのイベントが含まれる場合があります。

イベントログ

また、[イベントログ]ページを使用して、組織ビューの AWS Health イベントを表示できます。列のレイアウトと動作は[未解決の問題と最近の問題]タブと似ています。ただし、[イベントログ]タブに

は、イベントのカテゴリ、ステータス、開始時間などの追加の列とフィルターオプションがあります。

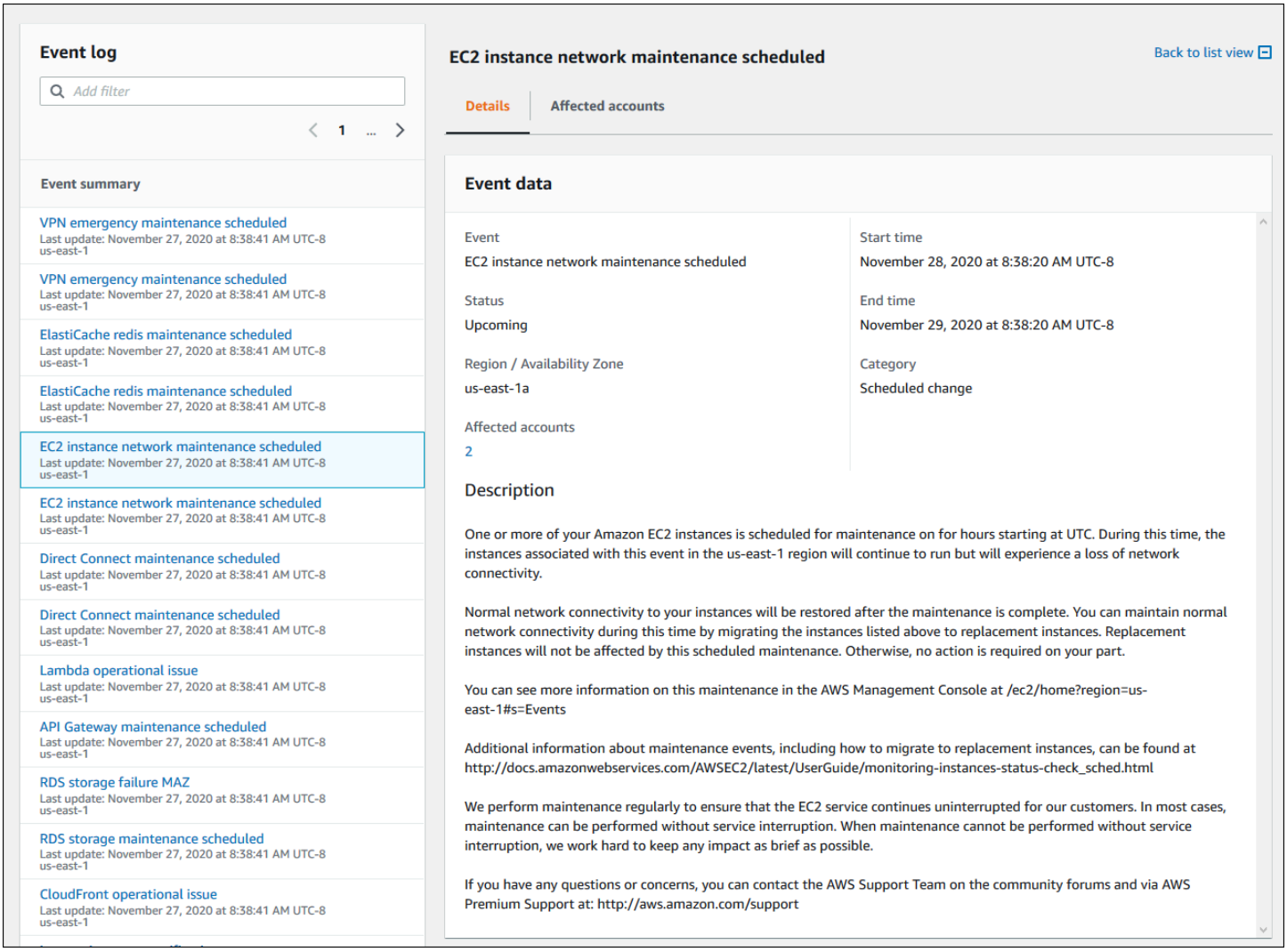
[イベントログ]タブで組織ビューイベントを表示するには

1. https://health.aws.amazon.com/health/home でAWS Healthダッシュボードを開きます。
2. ナビゲーションペインの [Your organization health] (組織の状態) で、[Event log] (イベントログ) を選択します。
3. [イベントログ] で、イベント名を選択します。イベントに関する以下の情報を確認できます。

   - イベント名
   - ステータス
   - リージョン/アベイラビリティーゾーン
   - 影響を受けるアカウント
   - 開始時間
   - 終了時間
   - カテゴリ
   - 説明

Example : 組織ビューの[イベントログ]タブ

次の Amazon DynamoDB (DynamoDB) イベントの例が[イベントログ]タブに表示され、組織内の 2 つのアカウントが影響を受けています。



影響を受けるアカウントとリソースの表示 (コンソール)

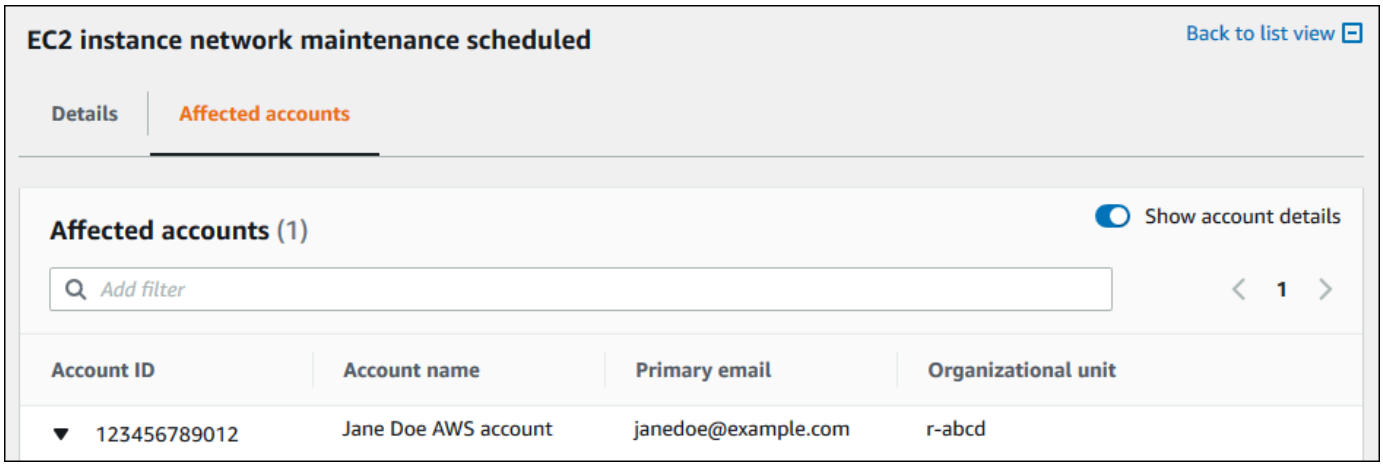
[組織の状態]で、イベントの影響を受けている組織内のアカウントおよび関連するリソースを表示できます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのメンテナンスという今後のイベントがある場合、Amazon EC2 インスタンスを持つ組織内のアカウントを [詳細] タブに表示できます。具体的なリソースを特定し、アカウント所有者に連絡することができます。

影響を受けるアカウントとリソースを表示するには

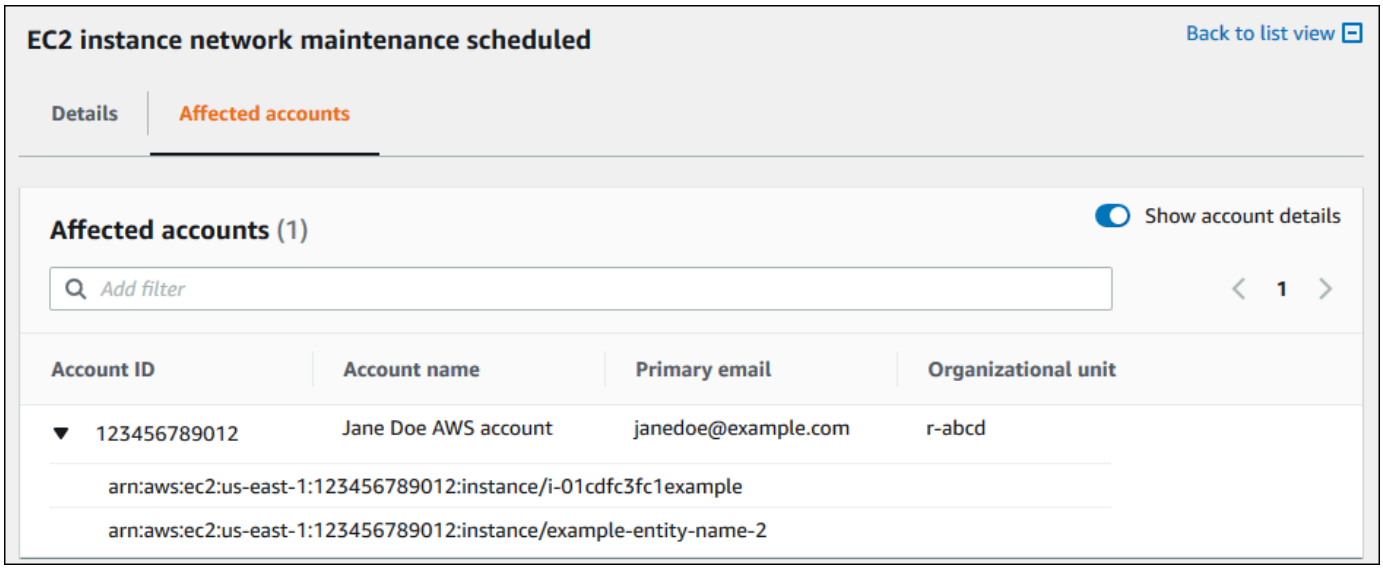
1. https://health.aws.amazon.com/health/home でAWS Healthダッシュボードを開きます。
2. ナビゲーションペインの [組織の状態] のタブの1つを選択します。
3. [影響を受けるアカウント]に値があるイベントを選択してください。
4. [Affected accounts] (影響を受けるアカウント) タブを選択します。

5. [Show account details] (アカウント詳細の表示) を選択し、アカウントに関する次の情報を表示します。

   - アカウント ID
   - アカウント名
   - プライマリ E メール
   - 組織単位 (OU)



6. アカウントを展開して、影響を受けるリソースを表示します。



7. リソースが 10 を超える場合は、[View all resources] (すべてのリソースを表示) を選択して表示します。

8. この特定のイベントをアカウント ID でフィルタリングするには、次の手順を実行します。

a. [Affected accounts] (影響を受けるアカウント) タブで、[Add filter] (フィルタの追加) を選択し、[Account ID] (アカウント ID) を入力します。一度に入力できるアカウント ID は 1 つだけです。

b. [Apply] (適用) を選択します。入力したアカウントが一覧に表示されます。

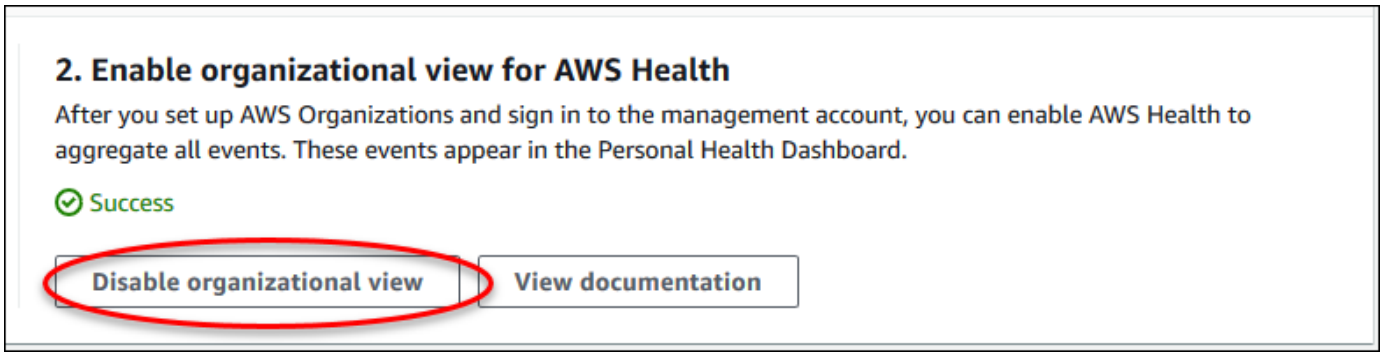
組織ビューの無効化 (コンソール)

組織のイベントを集計したくない場合は、管理アカウントからこの機能をオフにすることができます。

AWS Health は組織内の他のすべてのアカウントのイベントの集計を停止します。組織の以前のイベントは、削除されるまで引き続き表示できます。

組織ビューを無効にするには

1. https://health.aws.amazon.com/health/home でAWS Healthダッシュボードを開きます。
2. ナビゲーションペインの [組織の状態] で [構成] を選択します。
3. [Enable organizational view] (組織ビューの有効化) ページで、[Disable organizational view] (組織ビューの無効化) を選択します。



この機能をオフにすると、AWS Health は組織のイベントを集計しなくなります。ただし、サービスにリンクされたロールは、AWS Identity and Access Management (IAM) コンソール、IAM API、または AWS Command Line Interface (AWS CLI) で削除するまで管理アカウントに残ります。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。

組織ビュー (CLI)

AWS Health コンソールの代わりに、AWS Command Line Interface (AWS CLI) から組織ビュー機能を有効にすることもできます。コンソールを使用するには、「組織ビューの有効化 (コンソール)」を参照してください。

> **Note**
>
> 組織ビュー機能用の管理アカウントへのアクセスをユーザーに許可するには、AWSHealthFullAccess ポリシーなどのアクセス許可が必要です。詳細については、「AWS Health 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。

目次

組織ビューの有効化 (CLI)

組織ビューは、EnableHealthServiceAccessForOrganization API オペレーションを使用してのみ有効にできます。

AWS Command Line Interface (AWS CLI) または独自のコードを使用して、このオペレーションを呼び出すことができます。

> **Note**
>
> - AWS Health API を呼び出すには、ビジネスサポートプラン、エンタープライズ On-Ramp サポートプラン、またはエンタープライズサポートプランが必要です。
> - 米国東部 (バージニア北部) リージョンのエンドポイントを使用する必要があります。

Example

次の AWS CLI コマンドは、AWS アカウントからこの機能を有効にします。このコマンドは、管理アカウントから、または必要なアクセス許可を持つロールを引き受けることができるアカウントから使用できます。

```
aws health enable-health-service-access-for-organization --region us-east-1
```

次のコード例では、EnableHealthServiceAccessForOrganization API オペレーションを呼び出します。

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

次の例では、バージョン Java 2.0 用の AWS SDK を使用できます。

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;
```

```
public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
        }
    }
}
```

詳細については、 AWS SDK for Java 2.0 開発者ガイドを参照してください。

この機能を有効にすると、Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを持つ AWSServiceRoleForHealth_Organizations サービスにリンクされたロールが組織内の管理アカウントに適用されます。

> **Note**
>
> この機能の有効化は非同期プロセスであり、完了するまでに時間がかかります。DescribeHealthServiceStatusForOrganization オペレーションを呼び出して、このプロセスのステータスを確認できます。

組織ビューイベントの表示 (CLI)

この機能を有効にした後、AWS Health は、組織内のアカウントに影響を与えるイベントの記録を開始します。アカウントが組織に参加すると、AWS Health は、自動的にそのアカウントを組織ビューに追加します。

> **Note**
>
> AWS Health では、組織ビューを有効にする前に組織内で発生したイベントは記録されません。

アカウントが組織から離れると、そのアカウントからの新しいイベントが組織ビューに記録されなくなります。ただし、既存のイベントは残り、90 日間の制限までそのクエリを実行できます。

AWS は、管理者アカウントの閉鎖の発効日から 90 日間にわたり、そのアカウントのポリシーデータを保持します。90 日の期間の終了時、AWS は、アカウントのすべてのポリシーデータを完全に削除します。

- 結果を 90 日を超えて保持するには、ポリシーをアーカイブします。EventBridge ルールを用いてカスタムアクションを使用して、結果を S3 バケットに保存することもできます。
- AWS がポリシーデータを保持している限り、閉鎖されたアカウントを再度開くと、AWS は、アカウントをサービス管理者として再割り当てし、そのアカウントのサービスポリシーデータを回復します。
- 詳細については、「アカウントの解約」を参照してください。

> **Important**
>
> AWS GovCloud (US) リージョンの顧客の場合
>
> - アカウントを閉鎖する前に、アカウントリソースをバックアップしてから、削除します。アカウントを閉鎖した後は、当該アカウントへのアクセス権を失います。

AWS Health API オペレーションを使用して、組織ビューからイベントを返すことができます。

Example : 組織ビューイベントの説明

次の AWS CLI コマンドは、組織内の AWS アカウントのヘルスイベントを返します。

```
aws health describe-events-for-organization --region us-east-1
```

その他の AWS Health API オペレーションについては、次のセクションを参照してください。

組織ビューの無効化 (CLI)

組織ビューは、DisableHealthServiceAccessForOrganization API オペレーションを使用して無効にすることができます。

Example

次の AWS CLI コマンドは、アカウントからこの機能を無効にします。

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> また、Organizations の DisableAWSServiceAccess API オペレーションを使用して、組織機能を無効にすることもできます。このオペレーションを呼び出し後、AWS Health は、組織内の他のすべてのアカウントのイベントの集計を停止します。組織ビューの AWS Health API オペレーションを呼び出すと、AWS Health はエラーを返します。AWS Health は AWS アカウントのヘルスイベントを引き続き集計します。

この機能を無効にすると、AWS Health は組織からのイベントを集約しなくなります。ただし、サービスにリンクされたロールは、AWS Identity and Access Management (IAM) コンソール、IAM API、

または AWS CLI から削除するまで管理アカウントに残ります。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。

AWS Health 組織ビュー API オペレーション

組織ビューには、次の AWS Health API オペレーションを使用できます。

- DescribeEventsForOrganization – 組織全体のイベントに関する概要情報を返します。
- DescribeAffectedAccountsForOrganization – 指定されたイベントの影響を受けている組織内の AWS アカウントのリストを返します。
- DescribeEventDetailsForOrganization – 組織内の 1 つ以上のアカウントの指定されたイベントに関する詳細情報を返します。
- DescribeAffectedEntitiesForOrganization – 組織内の 1 つ以上のアカウントの 1 つ以上のイベントの影響を受けているエンティティのリストを返します。

次のオペレーションを使用すると、AWS Health による Organizations の操作を有効化または無効化できます。

- EnableHealthServiceAccessForOrganization — AWS Health に Organizations と対話するためのアクセス許可を付与し、SLR を組織内の管理アカウントに適用します。
- DisableHealthServiceAccessForOrganization — AWS Health が Organizations と対話するためのアクセス許可を取り消します。
- DescribeHealthServiceStatusForOrganization 組織で AWS Health が有効になっているかどうかに関するステータス情報を返します。

これらの API オペレーションを呼び出すには、ビジネスサポートプラン、エンタープライズ On-Ramp サポートプラン、またはエンタープライズサポートプランが必要です。少なくともビジネスサポートプランがあるアカウントから `DescribeEventForOrganization` および `DescribeAffectedAccountsForOrganization` オペレーションを呼び出すと、個々のアカウントのサポートレベルに関係なく、組織内の任意のアカウントに関する情報を返すことができます。次の 例を参照してください。

Example 例: ビジネスサポートプランと開発者サポートプランがあるアカウントを持つ組織

- 組織に 3 つのアカウントがあります。管理アカウントにビジネスサポートプランがあり、残りの 2 つのアカウントに開発者サポートプランがあります。

- 管理アカウントまたは必要なアクセス許可を持つロールを引き受けることができるアカウントから、DescribeEventForOrganization API オペレーションを呼び出します。
- AWS Health は、3 つのアカウントすべてに関する情報を返します。

少なくともビジネスサポートプランがあるアカウントから DescribeEventDetailsForOrganization および DescribeAffectedEntitiesForOrganization API オペレーションを呼び出すと、ビジネス、エンタープライズ On-Ramp、またはエンタープライズのサポートプランがある組織内のアカウントに関する情報のみを返すことができます。

Example 例: エンタープライズ、ビジネス、および開発者のサポートプランがあるアカウントを持つ組織

- 組織に 5 つのアカウントがあります。管理アカウントにエンタープライズサポートプランがあり、2 つのアカウントにビジネスサポートプランがあり、2 つのアカウントに開発者サポートプランがあります。
- 管理アカウントから DescribeEventDetailsForOrganization API オペレーションを呼び出します。
- AWS Health は、エンタープライズサポートプランまたはビジネスサポートプランがあるアカウントの情報のみを返します。開発者サポートプランがあるアカウントは、応答の failedSet に表示されます。

委任管理者の組織ビュー

AWS Healthでは、管理アカウント以外のアカウントが、集計されたAWS HealthイベントをAWS Healthダッシュボードに表示したり、AWS HealthAPIを介してプログラム的に表示したりできる、AWS Organizationsからの委任管理者機能を利用できます。委任管理者機能を使用すると、さまざまなチームが組織全体のヘルスイベントを柔軟に表示および管理できます。AWSのセキュリティ上のベストプラクティスは、可能な場合には管理アカウント外に責任を委任することです。

目次

組織ビューに委任管理者を登録する

組織の組織ビューを有効にすると、組織内の最大5つのメンバーアカウントを委任管理者として登録できます。これを行うには、RegisterDelegatedAdministrator APIオペレーションを呼び出します。メンバーアカウントを登録すると、メンバーは委任された管理者アカウントになり、AWS Healthダッシュボードから AWS Health 組織ビューにアクセスできるようになります。アカウントにビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートプランがある場合、委任された管理者はAWS HealthAPIを使用してAWS Health組織ビューにアクセスできます。

委任管理者を設定するには、組織の管理アカウントから次の AWS Command Line Interface (AWS CLI) コマンドを呼び出します。このコマンドは、管理アカウントから、または必要なAWS Identity and Access Managementアクセス許可を持つロールを引き受けることができるアカウントから使用できます。以下のコマンド例では、ACCOUNT_ID を、AWS Healthサービスプリンシパル「health.amazonaws.com」とともに登録したいメンバーアカウント ID に置き換えます。

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-principal  health.amazonaws.com
```

委任管理者を登録すると、組織全体のアカウントに影響を与えるすべてのAWS Healthイベントを確認できるようになります。過去90日間、または組織ビュー機能が最初に有効になってからのいずれか新しい日付の履歴イベントを表示できます。委任管理者機能の有効化は非同期処理であり、完了するまでに最大1分かかる点に注意してください。

組織ビューから委任管理者を削除する

委任された管理者のアクセスを削除するには、DeregisterDelegatedAdministrator API オペレーションを呼び出します。

組織の管理アカウントから次のAWS CLIコマンドを呼び出して、委任管理者としてのメンバーアカウントを削除します。次のコマンド例では、ACCOUNT_ID を削除するメンバーアカウント ID に置き換えます。

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-principal  health.amazonaws.com
```

Amazon による AWS Health イベントのモニタリング EventBridge

Amazon を使用して EventBridge 、 AWS Health イベントを検出して対応できます。次に、作成したルールに基づいて、イベントがルールで指定した値と一致すると、 は 1 つ以上のターゲットアクションを EventBridge 呼び出します。イベントのタイプに応じて、イベント情報の取得、追加イベントの開始、通知の送信、是正措置の実施、またはその他のアクションを実行することができます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど、更新が予定されている AWS リソース AWS アカウント が にある場合、 AWS Health を使用して E メール通知を受信できます。

> メモ
>
> - AWS Health は、ベストエフォートベースでイベントを提供します。イベントが に配信されるとは限りません EventBridge。
> - 作成した EventBridge ルールは、 の通知のみを受信できます AWS アカウント。内の他のアカウントの組織イベントを受信するには AWS Organizations、「組織ビューと委任された管理者アクセスを使用した AWS Health イベントの集約」を参照してください。

AWS Health ワークフロー EventBridge の一部として、以下を含む複数のターゲットタイプから選択できます。

- AWS Lambda 関数
- Amazon Kinesis Data Streams
- Amazon Simple Queue Service Amazon SQSキュー
- 組み込みターゲット (CloudWatch アラームアクションなど)
- Amazon Simple Notification Service (Amazon SNS)のトピック

例えば、 AWS Health イベントの発生時に、Lambda 関数を使用して通知を Slack チャネルに渡すことができます。または、Lambda と を使用して、 AWS Health イベントが発生したときに Amazon SNS でカスタムテキストまたは SMS 通知 EventBridge を送信することもできます。

AWS Health イベントに応じて作成できる自動化とカスタマイズされたアラートのサンプルについては、「 のAWS Health ツール」を参照してください GitHub。

トピック

AWS リージョン の について AWS Health

AWS Health イベントを受信するリージョンごとに EventBridge ルールを作成する必要があります。ルールを作成しなければ、イベントは受信されません。例えば、米国西部 (オレゴン) リージョンからイベントを受信するには、このリージョンのルールを作成する必要があります。

バックアップリージョンに追加のルールを設定すると、プライマリルールが進行中のイベントの影響を受けた場合に備えて、ワークフローの耐性がさらに高まります。のパブリックイベント AWS Health は、影響を受けるリージョンとバックアップリージョンの両方に同時に送信されます。詳細については、「AWS Health の公開イベントについて」を参照してください。標準 AWS パーティションのすべてのリージョンについて、バックアップとして米国西部 (オレゴン) にルールを設定して、プライマリリージョンが進行中の問題の影響を受けている場合でもイベントの受信を継続できます。米国西部 (オレゴン) のバックアップリージョンは米国東部 (バージニア北部) です。

例えば、欧州 (フランクフルト) リージョンでイベントをモニタリングしていて、そのリージョンが一時的に使用できない場合、 はそのイベントを米国西部 (オレゴン) リージョンにも配信 AWS Health します。次に、バックアップ EventBridge ルールは指定したターゲットにイベントを送信します。バックアップルールを作成するには、の EventBridge ルールの作成 AWS Healthに対する以下の手順に従い、米国西部 (オレゴン) リージョンを使用します。

一部の AWS Health イベントはリージョン固有ではありません。リージョンに固有ではないイベントはグローバルイベントと呼ばれます。これには、 AWS Identity and Access Management (IAM) について送信されるイベントが含まれます。グローバルイベントを受信するには、米国東部 (バージニア

北部) リージョンをプライマリーリージョンとし、米国西部 (オレゴン) をバックアップリージョンにするルールを作成する必要があります。

でグローバルイベントを受信するには AWS GovCloud (US)、 AWS GovCloud （ 米国西部) リージョンにルールを作成する必要があります。

のパブリックイベントについて AWS Health

からのイベントをモニタリングする EventBridgeルールを作成すると AWS Health、そのルールはアカウント固有のイベントとパブリックイベントの両方を配信します。

- アカウント固有イベントは、Amazon EC2 インスタンスの必須更新、またはその他の予定された変更イベントを通知するイベントなどにより、アカウントとリソースに影響を及ぼします。
- 公開イベントはAWS Health ダッシュボード — サービスヘルスに表示されます。公開イベントは AWS アカウント に固有ではなく、地域でサービスが利用できるかの公開情報を表示します。

> **Important**
>
> 両方のイベントタイプを受信するには、ルールで`"source": [ "aws.health"]`値を使用する必要があります。`"source": [ "aws.health*"]`などのワイルドカードは、どのイベントも監視するパターンとも一致しません。

からパブリックイベントをモニタリングする場合は AWS リージョン、バックアップルールを作成することをお勧めします。のパブリックイベント AWS Health は、影響を受けるリージョンとバックアップリージョンの両方に同時に送信されます。eventARN と communicationId を使用して AWS Health イベントの重複を解除することをお勧めします。これらのイベントは、バックアップリージョンに送信される AWS Health メッセージに対して一貫性が保たれるためです。

eventScopeCode パラメータ EventBridgeを使用して、イベントが でパブリックかアカウント固有かを特定できます。イベントには、 `PUBLIC`または を含めることができます`ACCOUNT_SPECIFIC`。このパラメーターでルールをフィルタリングすることもできます。

Amazon Elastic Compute Cloud の公開イベントの例

次のイベントは米国東部 (バージニア北部) リージョンでの Amazon EC2 の運用上の問題を示しています。

```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [
            {
                "latestDescription": "We are investigating increased API Error rates
 and Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
                "language": "en_US"
            }
        ],
        "page": "1",
        "totalPages": "1",
        "affectedAccount":"123456789012",

    }
}
```

のイベントプロセッサ AWS Health

アカウントに AWS インシデント検出と対応を使用する場合は、AWSServiceRoleForHealth_EventProcessorサービスにリンクされたロールをアカウントにインストールする必要があります。

このロールは event-processor.health.amazonaws.com サービスプリンシパルを信頼してそのロールを引き受けます。このロールにアタッチされるのは

AWSHealth_EventProcessorServiceRolePolicy AWS マネージドポリシーです。このポリシーには、他の を呼び出すなど、ロールが実行できるアクセス許可が一覧表示 AWS サービス されます。

次に、このロールはアカウントに Amazon EventBridge マネージドルールを作成します。ルールの名前は AWSHealthEventProcessor-DO-NOT-DELETE です。このルールは、 が アカウントから にアラーム状態変更情報を EventBridge 配信できるようにするための、 アカウントに必要なインフラストラクチャです AWS Health。

関連情報

詳細については、以下のトピックを参照してください。

- AWS Healthのサービスにリンクされたロールの使用
- AWS マネージドポリシー: AWSHealth_EventProcessorServiceRolePolicy

の EventBridge ルールの作成 AWS Health

アカウント内の AWS Health イベントの通知を受け取る EventBridge ルールを作成できます。のイベントルールを作成する前に AWS Health、次の操作を行います。

- のイベント、ルール、ターゲットについて理解します EventBridge。詳細については、「Amazon ユーザーガイド」の「Amazon EventBridgeとは」および「新規 EventBridge – AWS リソースへの変更の追跡と対応」を参照してください。 EventBridge
- イベントのルールで使用するターゲットを作成する。

の EventBridge ルールを作成するには AWS Health

1. https://console.aws.amazon.com/events/ で Amazon EventBridge コンソールを開きます。
2. を変更するには AWS リージョン、ページの右上隅にあるリージョンセレクターを使用します。AWS Health イベントを追跡するリージョンを選択します。
3. ナビゲーションペインで Rules] (ルール) を選択します。
4. [Create rule] (ルールを作成) を選択します。
5. [Define rule detail] (ルールの詳細を定義) ページで、ルールの名前と説明を入力します。
6. [Event bus] (イベントバス) と [Rule type] (ルールタイプ) のデフォルト値を維持して、[Next] (次へ) を選択します。

7. ビルドイベントパターンページのイベントソース で、AWS イベントと EventBridge パートナーイベント を選択します。
8. イベントソース で、イベントパターン に対してAWS サービスを選択します。
9. イベントパターン の [AWS サービス] で、[Health] を選択します。
10. [Event Type] (イベントタイプ) で、以下のいずれかのオプションを選択します。
    - [Specific Health Abuse Events] (特定の不正行為に関する Health イベント) – イベントタイプ名に `Abuse` という単語が含まれている AWS Health イベント用のルールを作成します。
    - 特定のヘルスイベント – Amazon EC2 など AWS サービス、特定の のイベントのルールを作成します。
11. [Any service] (任意のサービス) または [Specific service(s)] (特定のサービス) を選択できます。特定のサービスを選択する場合は、以下のオプションの 1 つを選択します。
    - すべてのイベントタイプのカテゴリに適用されるルールを作成するには、[Any event type category] (任意のイベントタイプのカテゴリ) を選択します。
    - [Specific event type category(s)] (特定のイベントタイプのカテゴリ) を選択してから、[issue]、[accountNotification]、または [scheduledChange] などの値をリストから選択します。

> **Tip**
>
> - 特定のサービスのすべての AWS Health イベントをモニタリングするには、任意のイベントタイプカテゴリ と任意のリソース を選択することをお勧めします。これにより、指定したサービスに対して、新しいイベントタイプのコードを含む、すべての AWS Health イベントがルールで確実にモニタリングされます。ルールの例については、すべての Amazon EC2 イベントを参照してください。
> - 複数のサービスまたはイベントタイプのカテゴリをモニタリングするルールを作成できます。そのためには、ルールのイベントパターンを手動で更新する必要があります。詳細については、「複数のサービスおよびカテゴリに対するルールの作成」を参照してください。

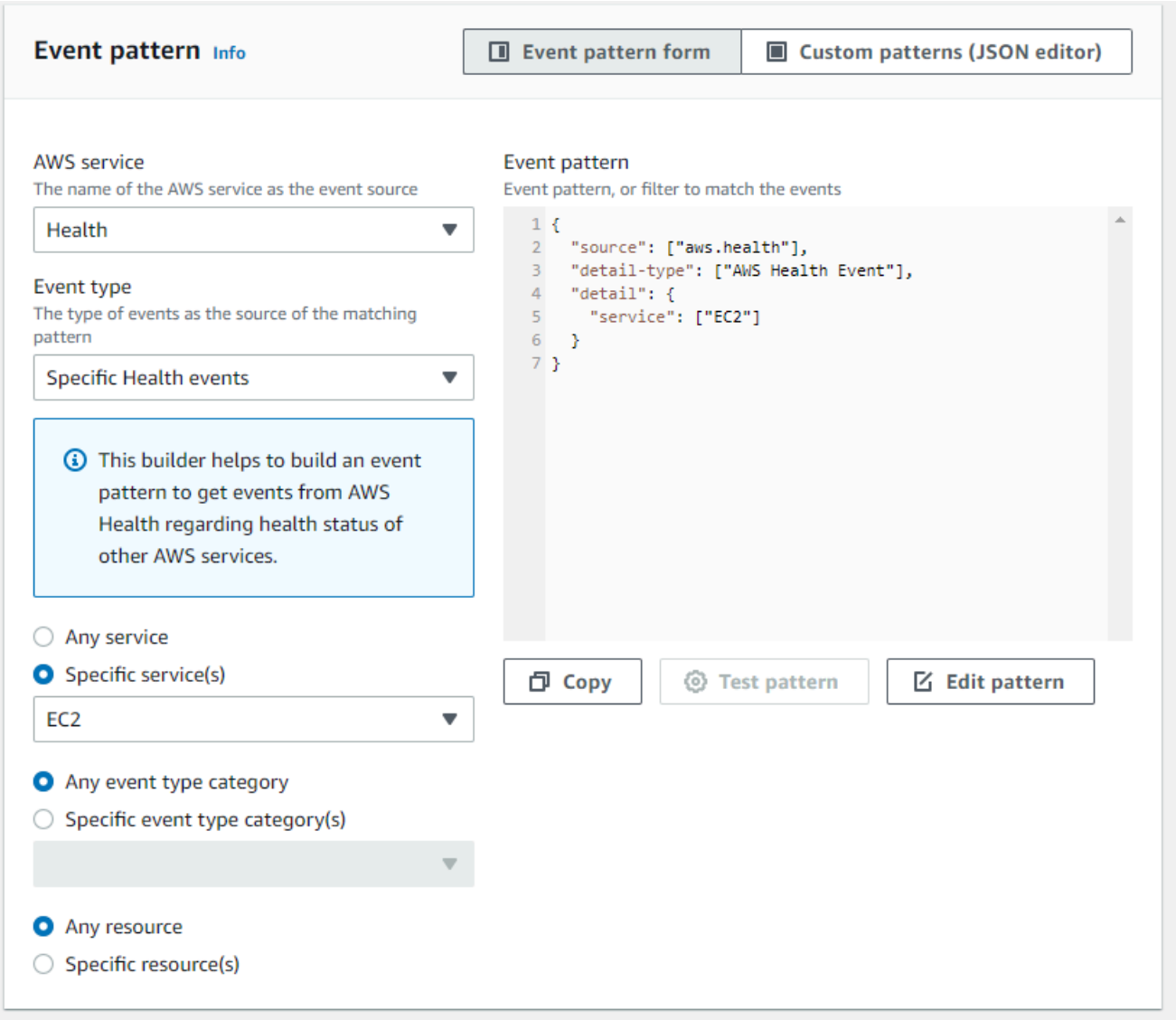
12. 特定のサービスおよびイベントタイプのカテゴリを選択した場合は、イベントタイプのコードに対して以下のいずれかのオプションを選択します。
    - すべてのイベントタイプのコードに適用されるルールを作成するには、[Any event type code] (任意のイベントタイプのコード) を選択します。

- [Specific event type code(s)] (特定のイベントタイプのコード) を選択し、リストから 1 つ以上の値を選択します。これにより、特定のイベントタイプのコードにのみ適用されるルールが作成されます。例えば、**AWS_EC2_INSTANCE_STOP_SCHEDULED** と **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED** を選択すると、これらのイベントがアカウントで発生した場合に、それらのイベントのみにルールが適用されます。

13. 影響を受けるリソースに対して、以下のいずれかのオプションを選択します。
    - すべてのリソースに適用されるルールを作成するには、[Any resource] (任意のリソース) を選択します。
    - [Specific resource(s)] (特定のリソース) を選択し、1 つ以上のリソースの ID を入力します。例えば、*i-EXAMPLEa1b2c3de4* などの Amazon EC2 インスタンス ID を指定して、このリソースのみに影響を及ぼすイベントを監視できます。
14. ルールのセットアップを見直して、イベントモニタリング要件を満たしていることを確認します。
15. [次へ] をクリックします。
16. [Select target(s)] (ターゲットを選択) ページで、このルール用に作成したターゲットタイプを選択してから、そのタイプに必要な追加のオプションを設定します。例えば、イベントを Amazon SQS キューまたは Amazon SNS トピックに送信できます。
17. 次へ をクリックします。
18. (オプション) [Configure tags] (タグの設定) ページで、いずれかのタグを追加し、[Next] (次へ) を選択します。
    - 注: タグは現在、 の aws.health ソースからは送信されません EventBridge。
19. [Review and create] (確認および作成) ページで、ルールの設定を確認し、イベントモニタリング要件を満たしていることを確認してください。
20. [ルールの作成] を選択します。

Example : すべての Amazon EC2 イベントに対するルール

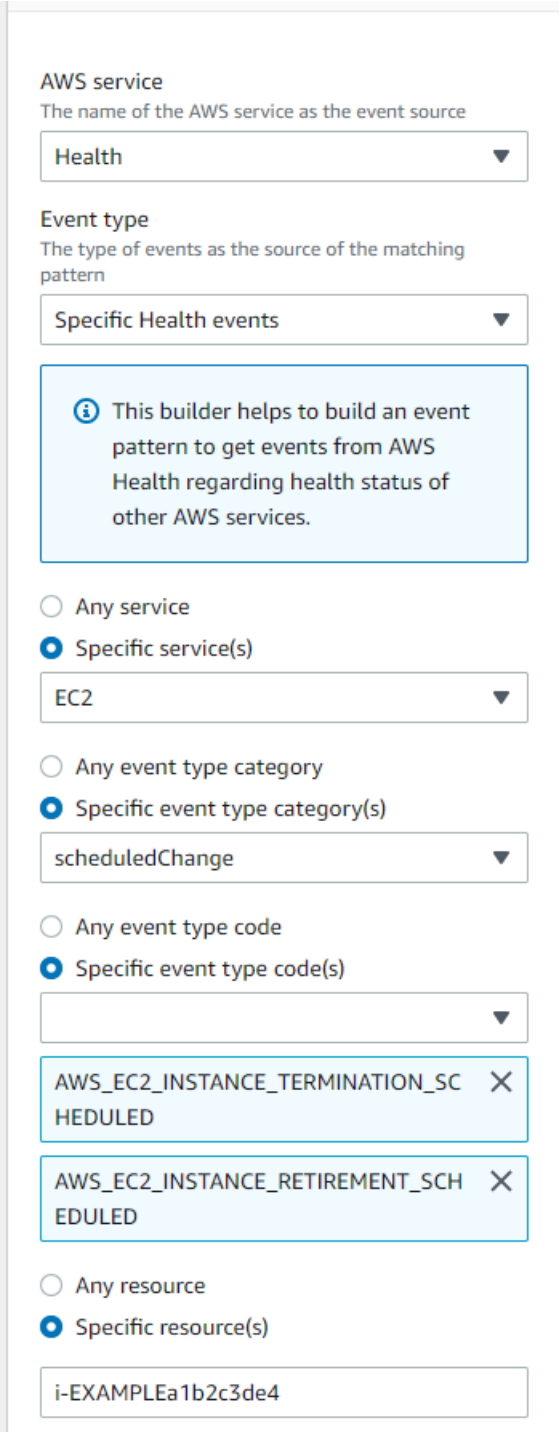
次の例では、イベントタイプのカテゴリ、イベントコード、リソースなど、すべての Amazon EC2 イベントを が EventBridge モニタリングするルールを作成します。



Example : 特定の Amazon EC2 イベントに対するルール

次の例では、 が以下を EventBridge モニタリングするルールを作成します。

- Amazon EC2 サービス
- scheduledChange イベントタイプのカテゴリ
- `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` および `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED` のイベントタイプのコード
- `i-EXAMPLEa1b2c3de4` という ID を持つインスタンス



複数のサービスおよびカテゴリに対するルールの作成

前の手順の例は、単一のサービスおよびイベントタイプのカテゴリに対してルールを作成する方法を示しています。複数のサービスやイベントタイプのカテゴリに対してルールを作成することもできます。つまり、モニタリングするサービスやカテゴリごとに個別のルールを作成する必要はありません。そのためには、イベントパターンを編集し、変更を手動で入力する必要があります。

次のオプションの 1 つを使用できます。

既存のルールにサービスとカテゴリを追加するには

1. EventBridge コンソールのルールページで、ルール名を選択します。
2. 右上隅の[編集] を選択します。
3. [Next] (次へ) を選択します。
4. [Event pattern] (イベントパターン) で [Edit pattern] (パターンを編集) をクリックしてから、変更内容をテキストフィールドに入力します。
5. [Review and update] (確認と更新) ページが表示されるまで [Next] (次へ) を選択します。
6. [Update rule] (ルールを更新) を選択して変更を保存します。

新しいルールにサービスとカテゴリを追加するには

1. 「の EventBridge ルールの作成 AWS Health」の手順をステップ 9 まで実行します。
2. リストから単一のサービスまたはカテゴリを選択する代わりに、[Event pattern] (イベントパターン) で [Edit pattern] (パターンを編集) を選択します。
3. テキストフィールドに変更を入力します。独自のイベントパターンを作成するためのモデルとして、以下のサンプルパターンを参照してください。
4. イベントパターンを確認してから、「の EventBridge ルールの作成 AWS Health」の残りの手順を実行してルールを作成します。

API または AWS Command Line Interface （ AWS CLI) を使用する

新規または既存のルールの場合は、 PutRule API オペレーションまたは `aws events put-rule` コマンドを使用してイベントパターンを更新します。コマンドの例については、 AWS CLI 「 コマンドリファレンス」の「put-rule」を参照してください。 AWS CLI

Example 例: 複数のサービスとイベントタイプのカテゴリ

次のイベントパターンは、Amazon EC2`issue`、Amazon EC2 Amazon EC2 Auto Scaling`accountNotification`、Amazon VPC の 3 つの AWS サービスの 、、および `scheduledChange`イベントタイプのカテゴリのイベントをモニタリングするルールを作成します。Amazon EC2 Auto Scaling

```
{
  "detail": {
```

```
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

AWS Health イベント Amazon EventBridge スキーマ

AWS Health イベントのスキーマを次に示します。以前のバージョンのスキーマに対する変更または追加は「新規」として強調表示されます。スキーマの後にサンプルペイロードが付けられます。

AWS Health イベントスキーマ

AWS Health イベントスキーマ

パラメータ	説明	必須
バージョン	EventBridge バージョン、現在「0」	はい
id	イベントの uniqueEve ntBridge 識別子	はい
詳細タイプ	ディテールタイプを記述し	はい

パラメータ	説明	必須
	ます。 AWS Health イベントの場合、これは &AWS Health Eventまたはになります。 AWS Health Abuse Event	
source	イベントバスソース。 AWS Health イベントの場合、これは aws.health	はい

パラメータ	説明	必須
account	AWS Health イベントが送信された accountId。 Note 組織側ビューでは、管理アカウントまたは委任管理者アカウントで受信された場合は AffectedAccount とは異なります。	はい

パラメータ	説明	必須
time	通知が に送信された時刻 EventBridge。形式: `yyyy-mm-ddThh:mm:ssZ` 。	はい

パラメータ	説明	必須
region	通知 AWS リージョンが配信されたを識別します。 Note このフィールドには、このAWS Healthイベントの影響を受けるリージョンは表示されません。これは「Detail.EventRegion」に	はい

パラメータ	説明	必須
	よって示されます。	

パラメータ	説明	必須
resources	影響を受けるリソースがある場合、アカウント内の影響を受けるリソースのリストを記述します。 Note 参照されているリソースがない場合は、このフィールドは空にすることもできます。	いいえ

パラメータ	説明	必須
詳細	このセクションには、以下に示す AWS Health イベントの詳細がすべて含まれています。	はい

パラメータ		説明	必須
	eventArn	特定のリージョンの AWS Health イベントの一意の識別子には、リージョンとイベント ID が含まれます。 **Note** eventArn は特定の顧客アカウントや地域に固有のものではありません。	はい

パラメータ		説明	必須
	service	AWS Health イベントの AWS サービス 影響を受ける 。たとえば、Amazon EC2、Amazon Simple Storage Service、Amazon Redshift、Amazon Relational Database Service。	はい

パラメータ		説明	必須
	eventTypeCode	イベントタイプの一意の識別子。例: AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED および AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED 。MAINTENANCE_SCHEDULED を含むイベントは、通常、startTime の約2週間前に延期されます。 Note 新たに予定されているライフサイクルイベン	はい

パラメータ		説明	必須
		トにはすべてイベントタイプAWS_{SICE}_PLANNED_LIFECYCLE_EVENT があります。	
	イベントTypeCategory	イベントのカテゴリコード指定できる値は、issue、accification 、investigation 、schedChange です。	はい

パラメータ		説明	必須
	イベントScopeCode	AWS Health イベントがアカウント固有かパブリックかを示します。想定される値は、ACCOUNT_SPECIFIC または PUBLIC です。	はい

パラメータ		説明	必須
	communicationId (新規)	AWS Health イベントのこの通信の一意の識別子。 同じ communicationId を持つメッセージは、1 つの AWS Health イベントのバックアップメッセージまたはページである可能性があります。この識別子を accountId と組み合わせて使用すると、メッセージの重複排除に役立ちます。 Note ページネーション機能のリリー	はい

パラメータ	説明	必須
	スでは、communicationId をページ間で一意に保つためのページ番号が communicationId に含まれるようになりました (例:1234578910-1)。詳細については、「[での AWS Health イ](#)	

パラメータ	説明	必須
	ベントのページ分割 EventBridge」を参照してください。	

パラメータ		説明	必須
	startTime	AWS Health イベントの開始時刻は、の形式ですDoW, DD, MMM, YYYY, HH:MM:SS TZ。 Note 予定されているイベントの開始時間は、未来であってもかまいません。	はい

パラメータ		説明	必須
	endTime	形式の AWS Health イベントの終了時刻: `DoW, DD MMM YYYY HH:MM:SS TZ`。 **Note** endTime は、今後設定されるイベントには提供されない場合があります。	いいえ

パラメータ		説明	必須
	最後のUpdatedTime	形式の AWS Health イベントの最終更新時刻: `DoW, DD MMM YYYY HH:MM:SS TZ`。	はい

パラメータ		説明	必須
	statusCode	AWS Health イベントのステータス。タイプカテゴリには異なるステータスがあります。 Issue イベントカテゴリに使用できる値は、open、、cたは ですupcoming。 scheduledChanges イベントカテゴリのステータスはUpcoming、 などさまざまです。 AccountNotifications イベントカテゴリにはステータスはなく、"-"に設定されます。	はい

leted

パラメータ			説明	必須
	eventRegion		この AWS Health イベントで説明される影響を受けるリージョン。	はい
	eventDescription		AWS Health イベントを説明するセクション。これには、イベントを説明する言語やテキストのフィールドが含まれます。	はい
		language	AWS Health イベントで使用される言語。これは通常、イベントが公開されている地域によって決まります。us-east-1 リージョンでは、これは通常 "en_US" です。	はい

パラメータ			説明	必須
		latestDescription	AWS Health API からレンダリングされる AWS Health イベントを記述し、通常は AWS Health ダッシュボードに表示されます。 Note 公開イベントの場合、これには最新の更新のみが含まれ、イベントの履歴全体は含まれ	はい

パラメータ		説明	必須
		ません。	
	eventMetadata	AWS Health イベントに供給できる追加のイベントメタデータ。	いいえ

パラメータ			説明	必須
		<metadata key 1>	メタデータキー、値文字列"keystring1": "keyvalue1" Note イベントメタデータのキーと値のペアは、AWS Healthイベントを送信したサービスによって決まります。	いいえ

パラメータ			説明	必須
	affectedEntities		この AWS Health イベント内の影響を受けるリソースのリソース値とステータスを記述する配列。	いいえ
		entityValue	リソース/エンティティ ID	いいえ
		lastUpdatedtime (新規)	このリソース/エンティティのステータスが最後に更新された時刻は次の形式で表示されます。`DoW, DD MMM YYYY HH:MM:SS TZ`	いいえ
		status (新規)	影響されたリソース/エンティティのステータス。値は、`IMPAIRED D` 、`PENDING`、どです。	いいえ `KNOWN`

パラメータ		説明	必須
	page (新規)	このメッセージが表すページ。詳細については、「[での AWS Health イベントのページ分割 EventBridge]」を参照してください。 Note ページ分割はリソース上でのみ行われます。256 KB のサイズ制限違反のその他の原因として、通	はい

パラメータ		説明	必須
		信が失敗する原因があります。	

パラメータ		説明	必須
	totalPages (新規)	このヘルスイベントのページの総数。詳細については、「での AWS Health イベントのページ分割 EventBridge」を参照してください。 Note これを使用して、あるアカウントについて複数ページにわたる通信の全ページを受信した	はい

パラメータ	説明	必須
	かどうかを判断できます。	

パラメータ		説明	必須
	affectedAccount (新規)	これは影響を受けるアカウントの accountId です。 Note これは、このヘルスイベントがの一部であるアカウントに送信 AWS Organizations され、管理アカウントまたは委任された管	はい

パラメータ		説明	必須
		理者アカウントで受信された場合、「アカウント」フィールドとは異なることがあります。	

公開ヘルスイベント-Amazon EC2 の運用上の問題

```
{
  "version": "0",
  "id": "7bf73129-1428-4cd3-a780-95db273d1602",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2023-01-27T09:01:22Z",
  "region": "af-south-1",
  "resources": [],
  "detail": {
```

```
            "eventArn": "arn:aws:health:af-south-1::event/EC2/
AWS_EC2_OPERATIONAL_ISSUE/AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-
d0179ed6d68f",
            "service": "EC2",
            "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
            "eventTypeCategory": "issue",
            "eventScopeCode": "PUBLIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
            "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
            "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
            "statusCode": "open",
            "eventRegion": "af-south-1",
            "eventDescription":
            [{
              "language": "en_US",
              "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
            }],
            "affectedEntities":[],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
        }
```

アカウント固有の AWS Health イベント - Elastic Load Balancing API の問題

```
        {
          "version": "0",
          "id": "121345678-1234-1234-1234-123456789012",
          "detail-type": "AWS Health Event",
          "source": "aws.health",
          "account": "123456789012",
          "time": "2022-06-10T06:27:57Z",
          "region": "ap-southeast-2",
          "resources": [],
```

```
          "detail": {
            "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
            "service": "ELASTICLOADBALANCING",
            "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
            "eventTypeCategory": "issue",
            "eventScopeCode": "ACCOUNT_SPECIFIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
            "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
            "statusCode": "open",
            "eventRegion": "ap-southeast-2",
            "eventDescription": [{
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
        }
```

アカウントに固有の AWS Health イベント - Amazon EC2 インスタンスストアドライブのパフォーマンス低下

```
        {
          "version": "0",
          "id": "121345678-1234-1234-1234-123456789012",
          "detail-type": "AWS Health Event",
          "source": "aws.health",
          "account": "123456789012",
          "time": "2022-06-03T06:27:57Z",
          "region": "us-west-2",
          "resources": [
            "i-abcd1111"
          ],
          "detail": {
            "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
            "service": "EC2",
```

```
            "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
            "eventTypeCategory": "issue",
            "eventScopeCode": "ACCOUNT_SPECIFIC",
            "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
            "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
            "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
            "statusCode": "open",
            "eventRegion": "us-west-2",
            "eventDescription": [{
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }],
            "affectedEntities": [{
              "entityValue": "i-abcd1111",
            }],
            "page": "1",
            "totalPages": "1",
            "affectedAccount": "123456789012",
          }
        }
```

での AWS Health イベントのページ分割 EventBridge

AWS Health は、「リソース」またはaffectedEntities」のリストによってメッセージのサイズが の 256 EventBridgeKB メッセージサイズ制限を超えた場合に、 AWS Health イベントのページ分割をサポートします。 256KB 以前は、この制限を超えた場合、 はリソースの完全なリストをイベントと通信していません AWS Health でした。

AWS Health では、メッセージにすべての「リソース」と「detail.affectedEntities」が含まれるようになりました。この「resources」と「detail.affectedEntities」のリストが 256KBを超える場合、 はヘルスイベントを複数のページに AWS Health 分割し、これらのページを個々のメッセージとして に発行します EventBridge。すべてのページを受信した後に「resources」または「Detail.AffectedEntities」のリストを再結合できるように、各ページには同じ eventARN と communicationId が保持されます。

これらの追加メッセージは、 EventBridge ルールが E メールやチャットなどの人間が読めるインターフェイスに向けられている場合など、不必要なメッセージを引き起こす可能性があります。人間が読める形式の通知を使用しているお客様は、「detail.page」フィールドに最初のページのみを処理するフィルターを追加して、後続のページから作成される不要なメッセージを除外できます。

ページネーションの起動をサポートするために、いくつかのスキーマ変更が含まれています。各 communicationId には、ページが1ページしかない場合でも、communicationId の後ろにハイフンでつながれたページ番号が含まれるようになりました。また、現在のページ番号と AWS Health イベントの合計ページ数を記述する detail.page と detail.totalPages という 2 つの新しいフィールドもあります。ページ分割された各メッセージに含まれる情報は、「Detail.affectedEntities」または「resources」のリストを除いて同じです。これらのリストは、すべてのページを受信した後で再構築できます。影響を受けるリソースやエンティティのページは、順序に依存しません。

組織ビューと委任された管理者アクセスを使用した AWS Health イベントの集約

AWS Health は、Amazon で公開された AWS Health イベントの組織ビューと委任された管理者アクセスをサポートします EventBridge。で組織ビューが有効になっている場合 AWS Health、管理アカウントまたは委任された管理者アカウントは、 の組織内のすべてのアカウントから AWS Health イベントの 1 つのフィードを受け取ります AWS Organizations。

この機能は、組織全体の AWS Health イベントを管理するのに役立つ一元的なビューを提供するように設計されています。管理アカウントで組織ビューと EventBridge ルールを設定しても、組織内の他のアカウントの EventBridge ルールは非アクティブ化されません。

で組織ビューと委任された管理者アクセスを有効にする方法の詳細については AWS Health、「イベントの集約」を参照してください AWS Health。

でのイベントの受信 AWS HealthAWS Chatbot

Slack や Amazon Chime などのチャットクライアントで AWS Health イベントを直接受信できます。このイベントを使用して、アプリケーションやインフラストラクチャに影響を与える可能性のある最近の AWS サービスの問題を特定できます AWS 。その後、AWS Health Dashboard にサインインして、更新に関する詳細情報を確認できます。例えば、 AWS アカウントのAWS_EC2_INSTANCE_STOP_SCHEDULEDイベントタイプをモニタリングしている場合、 AWS Health イベントは Slack チャネルに直接表示されることがあります。

前提条件

開始する前に、以下のものが必要です。

- で設定されたチャットクライアント AWS Chatbot。Amazon Chime と Slack を設定できます。詳細については、AWS Chatbot 管理者ガイドのAWS Chatbotの開始方法を参照してください。

- 作成した、およびサブスクライブした Amazon SNS トピック。SNS トピックが既にある場合、既存のトピックを使用できます。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。

で AWS Health イベントを受信するには AWS Chatbot

1. 「の EventBridge ルールの作成 AWS Health」の手順をステップ 13 まで実行します。

   a. ステップ 13 でイベントパターンの設定が完了したら、パターンの最後の行にカンマを追加し、次の行を追加してページ分割された AWS Health イベントから不要なチャットメッセージを削除します。での AWS Health イベントのページ分割 EventBridge を参照してください。

      ```
      "detail.page": ["1"]
      ```

   b. ステップ 14 でターゲットを選択するときに、SNS トピックを選択します。 AWS Chatbot コンソールで同じ SNS トピックを使用します。

   c. 残りの手順を完了して、ルールを作成します。

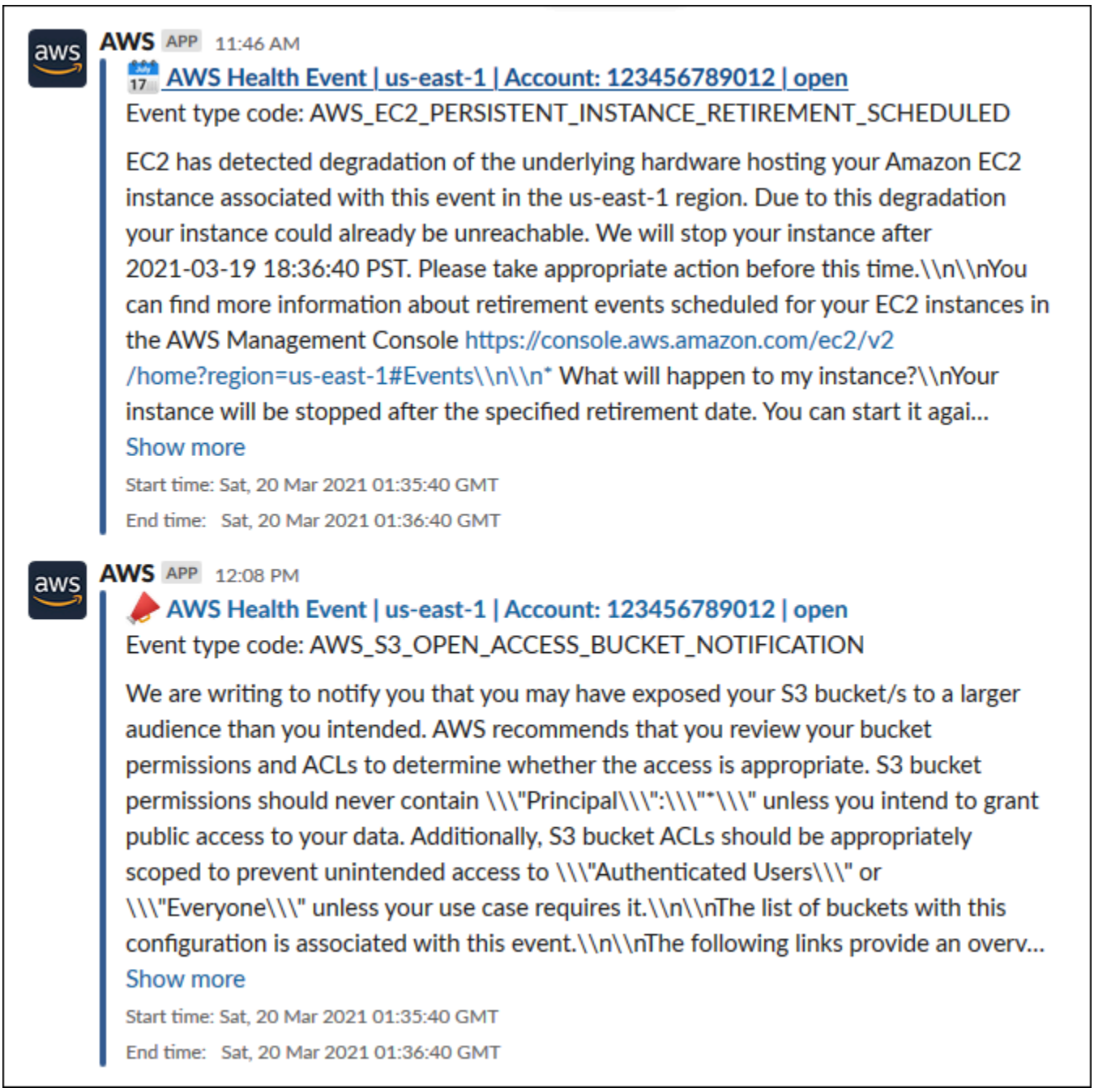
2. AWS Chatbot コンソールに移動します。
3. Slack チャネル名など、チャットクライアントを選択し、[Edit] (編集) を選択します。
4. [Notifications - optional] (通知 – オプション) セクションの [Topics] (トピック) で、ステップ 1 で指定したものと同じ SNS トピックを選択します。
5. [保存] を選択します。

   がルール EventBridge に一致するイベントを AWS Health に送信すると、 AWS Health イベントがチャットクライアントに表示されます。

6. イベント名を選択すると、 AWS Health ダッシュボードに詳細情報が表示されます。

Example :Slack に送信された AWS Health イベント

以下は、Slack チャネルに表示される米国東部 (バージニア北部) リージョンの Amazon EC2 と Amazon Simple Storage Service (Amazon S3) の 2 つの AWS Health イベントの例です。



Amazon EC2 インスタンスのアクションの自動化

Amazon EC2 インスタンスに対してスケジュールされたイベントに対応するアクションを自動化することができます。がアカウントにイベント AWS Health を送信すると AWS 、 EventBridge ルールは AWS Systems Manager オートメーションドキュメントなどのターゲットを呼び出して、ユーザーに代わってアクションを自動化できます。

例えば、Amazon EC2 インスタンスのリタイアイベントが Amazon Elastic Block Store (Amazon EBS)-backed EC2 インスタンスにスケジュールされている場合、 AWS Health は`AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED`イベントタイプを AWS Health Dashboard に送信します。ルールでこのイベントタイプが検出されると、インスタンスの停止と開始を自動化できます。この方法では、これらのアクションを手動で実行する必要はありません。

> **Note**
>
> Amazon EC2 インスタンスに対するアクションを自動化するには、そのインスタンスが Systems Manager によって管理されている必要があります。

詳細については、Amazon EC2 ユーザーガイド」の「 による EventBridge Amazon EC2 の自動化」を参照してください。

前提条件

ルールを作成する前に、 AWS Identity and Access Management (IAM) ポリシーを作成し、IAM ロールを作成し、ロールの信頼ポリシーを更新する必要があります。

IAM ポリシーを作成する

ロール用のカスタマー管理ポリシーを作成するには、次の手順に従います。このポリシーは、ユーザーに代わってアクションを実行するためのロールアクセス許可を付与します。この手順では、IAM コンソールの JSON ポリシーエディタを使用します。

IAM ポリシーを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で 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. ポリシーの作成を選択します。
4. [JSON] タブを選択します。
5. 次の JSON をコピーし、エディタでデフォルトの JSON を置き換えます。

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
  ]
}
```

a. Resource パラメータで、Amazon リソースネーム (ARN) に AWS アカウント ID を入力します。

b. ロール名を置き換えることも、デフォルトを使用することもできます。この例は *AutomationEVRole* を使用します。

6. [次へ: タグ] を選択します。
7. (オプション) キーバリューペアとしてのタグを使用して、メタデータをポリシーに追加することができます。
8. [次へ: レビュー] を選択します。
9. ポリシーの確認ページで、*AutomationEVRolePolicy* などの名前 とオプションの 説明 を入力します。
10. [Summary] (概要) ページで、ポリシーが許容する許可を確認します。ポリシーが適切であれば、[Create policy] (ポリシーの作成) を選択します。

このポリシーによって、このロールが実行できるアクションが定義されます。詳細については、IAM ユーザーガイドのIAM ポリシーの作成 (コンソール) を参照してください。

IAM ロールを作成する

このポリシーを作成したら、IAM ロールを作成し、そのロールにポリシーをアタッチする必要があります。

AWS サービスのロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで [Roles] (ロール) を選択してから、[Create role] (ロールを作成する) を選択します。
3. 信頼できるエンティティの種類の選択 で、AWS サービス を選択します。
4. このロールを引き受けることを許可するサービスに [EC2] を選択します。
5. [次へ: アクセス許可] を選択します。
6. *AutomationEVRolePolicy* など、作成したポリシー名を入力し、ポリシーの横にあるチェックボックスをオンにします。
7. 次へ: タグ を選択します。
8. (オプション) キーと値のペアとしてタグを使用し、メタデータをロールに追加できます。
9. 次へ: レビュー を選択します。
10. [Role name] (ロール名) には *AutomationEVRole* を入力します。この名前は、作成した IAM ポリシーの ARN に表示される名前と同じものにする必要があります。
11. (オプション) [Role description] (ロールの説明) に、ロールの説明を入力します。
12. ロール情報を確認し、ロールの作成 を選択します。

詳細については、「IAM ユーザーガイド」の「 AWS サービスのロールの作成」を参照してください。

信頼ポリシーの更新

最後に、作成したロールの信頼ポリシーを更新できます。 EventBridge コンソールでこのロールを選択できるようにするには、この手順を完了する必要があります。

ロールの信頼ポリシーを更新するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで、[ロール] を選択します。
3. AWS アカウントのロールのリストで、*AutomationEVRole*など、作成したロールの名前を選択します。
4. [Trust relationships] タブを選択し、続いて [Edit trust relationship] を選択します。
5. [Policy Document] (ポリシードキュメント) には、以下の JSON をコピーし、デフォルトポリシーを削除して、その代わりにコピーした JSON を貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. 信頼ポリシーの更新 を選択します。

詳細については、IAM ユーザーガイドのロールの信頼ポリシーの変更 (コンソール) を参照してください。

のルールを作成する EventBridge

以下の手順で EventBridge コンソールでルールを作成し、リタイアが予定されている EC2 インスタンスの停止と起動を自動化できるようにします。

Systems Manager 自動アクション EventBridge の のルールを作成するには

1. https://console.aws.amazon.com/events/ で Amazon EventBridge コンソールを開きます。
2. ナビゲーションペインの イベント で、ルール を選択します。
3. [Create rule] (ルールの作成) ページで、ルールの [Name] (名前) と [Description] (説明) を入力します。
4. [Define pattern] (パターンの定義) で、[Event pattern] (イベントパターン) を選択してから、[Pre-defined pattern by service] (サービスごとに事前定義されたパターン) を選択します。
5. [Service provider (サービスプロバイダー)] で、「AWS」を選択します。
6. [Service name] (サービス名) には [Health] を選択します。
7. [Event type] (イベントタイプ) には [Specific Health events] (特定の Health イベント) を選択します。
8. [Specific service(s)] (特定のサービス) を選択し、[EC2] を選択します。
9. [Specific event type category(s)] (特定のイベントタイプのカテゴリ) を選択し、[scheduledChange] を選択します。
10. [Specific event types code(s)] (特定のイベントタイプのコード) を選択し、イベントタイプのコードを選択します。

    例えば、Amazon EC2 EBS-backed インスタンスの場合、**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED** を選択します。Amazon EC2 インスタンスの store-backed インスタンスの場合、**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED** を選択します。
11. [任意のリソース] を選択します。

    [Event pattern] (イベントパターン) は以下の例のようになります。

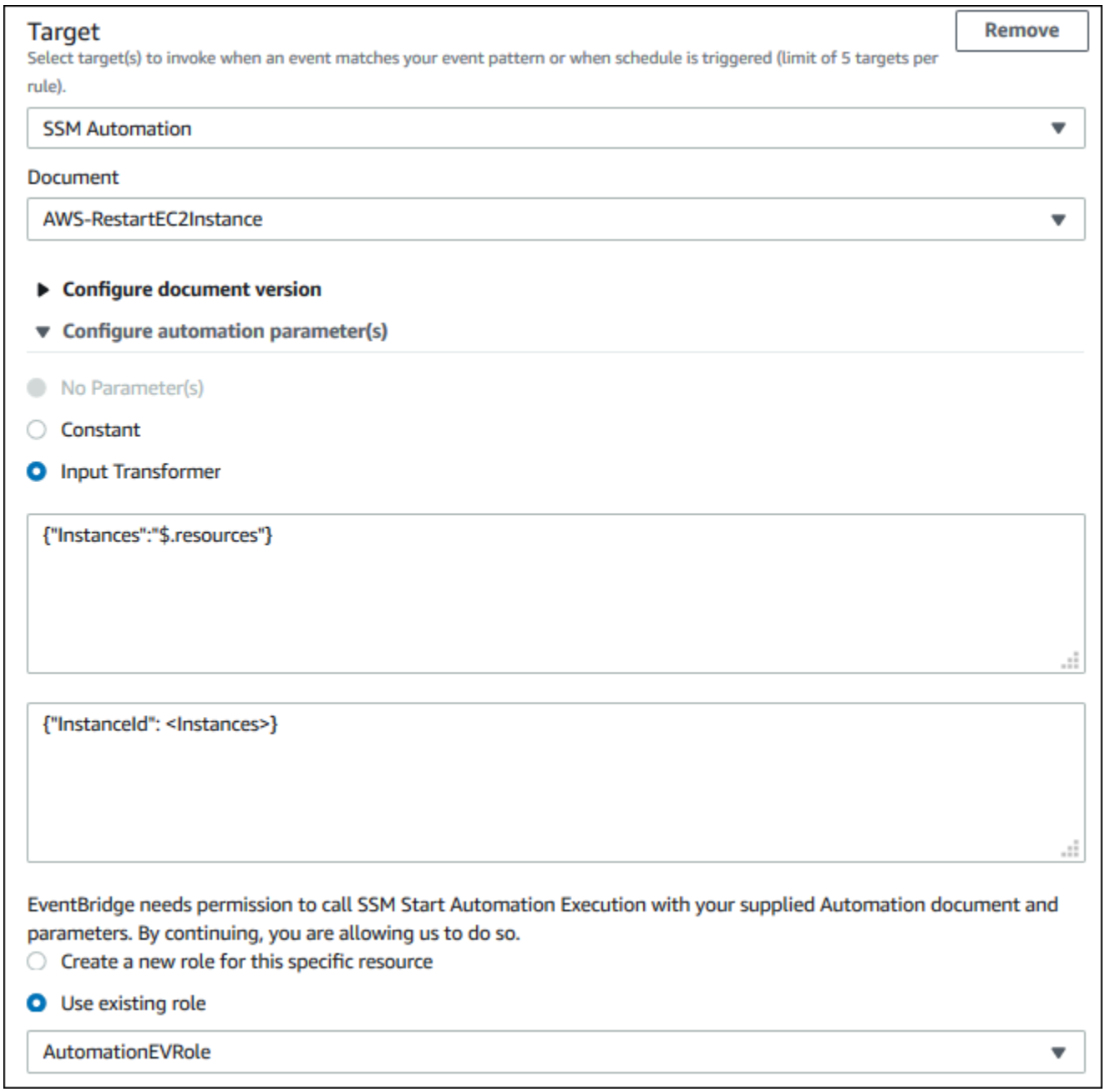
    Example

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

```
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Systems Manager オートメーションドキュメントターゲットを追加します。[Select targets] (ターゲットを選択) の [Target] (ターゲット) で [SSM Automation] (SSM オートメーション) を選択します。
13. [ドキュメント] で、[AWS-RestartEC2Instance] を選択します。
14. [Configure automation parameters(s)] (オートメーションパラメータの構成) を展開し、[Input Transformer] (入力トランスフォーマー) を選択します。
15. [Input Path] (入力パス) フィールドに、**{"Instances":"$.resources"}** を入力します。
16. 2 番目のフィールドに、**{"InstanceId": <Instances>}** を入力します。
17. [Use existing role] (既存のロールを使用) を選択してから、作成した IAM ロール (*AutomationEVRole* など) を選択します。

    ターゲットは以下の例のようになります。



> **Note**
>
> 必要な EC2 と Systems Manager のアクセス許可と、信頼されたリレーションシップを持つ既存の IAM ロールがない場合、ロールはリストに表示されません。詳細については、「前提条件」を参照してください。

18. [Create] (作成) を選択します。

ルールに一致するイベントがアカウントで発生した場合、 EventBridge は指定されたターゲットにイベントを送信します。

の SMC コネクタを設定する AWS Health

AWS Health イベントを JIRA および と統合 ServiceNow して、運用およびアカウント情報を受信し、スケジュールされた変更の準備を行い、Service Management Connector (SMC) を使用して Health イベントを管理できます。との SMC 統合では AWS Health 、 を介して送信されたヘルスイベントを使用して、JIRA チケット ServiceNowとインシデント EventBridge を自動的に作成、マッピング、更新できます。

組織ビューと委任された管理者アクセスを使用して、JIRA と 内の組織全体の Health イベントを簡単に管理し ServiceNow、情報をチームのワークフローに直接組み AWS Health 込むことができます。

SMC を使用した ServiceNow 統合の詳細については、「 での統合」を参照してください AWS Health ServiceNow。

SMC を使用した JIRA Management Cloud の統合の詳細については、AWS Health 「JIRA 」の「」を参照してください。

モニタリング AWS Health

モニタリングは、 AWS Health およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 をモニタリングし AWS Health、問題が発生した場合に報告し、必要に応じてアクションを実行するために、以下のモニタリングツール AWS を提供します。

- Amazon は、 AWS リソースと で AWS 実行しているアプリケーションをリアルタイムで CloudWatch モニタリングします。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

  Amazon を使用すると EventBridge 、サービスやリソースに影響を与える可能性のある AWS Health イベントについて通知を受け取ることができます。例えば、 が Amazon EC2インスタンスに関するイベント AWS Health を発行する場合、これらの通知を使用してアクションを実行し、必要に応じてリソースを更新または置き換えることができます。詳細については、「Amazon による AWS Health イベントのモニタリング EventBridge」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

- を使用した通話のログ記録 AWS Health API AWS CloudTrail

を使用した通話のログ記録 AWS Health API AWS CloudTrail

AWS Health は、 と統合されています AWS Health。これは AWS CloudTrail、. CloudTrail captures のユーザー、ロール、または サービスによって実行されたアクションを記録する AWS サービスです。 は を AWS Health イベントとしてAPI呼び出します。キャプチャされた呼び出しには、AWS Health コンソールからの呼び出しと、 オペレーションへのコード呼び出しが含まれます AWS Health API。証跡を作成する場合は、 の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます AWS Health。証跡を設定しない場合でも、

CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 に対するリクエスト AWS Health、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の設定と有効化の方法など CloudTrail、 の詳細については、AWS CloudTrail 「 ユーザーガイド」を参照してください。

AWS Health の情報 CloudTrail

CloudTrail AWS アカウントを作成すると、 がアカウントで有効になります。でサポートされているイベントアクティビティが発生すると AWS Health、そのアクティビティは CloudTrail イベント履歴の他の AWS サービスイベントとともにイベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「イベント履歴を使用した CloudTrail イベントの表示」を参照してください。

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

- 証跡の作成のための概要
- CloudTrail サポートされているサービスと統合
- の Amazon SNS Notifications の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての AWS Health APIオペレーションは によってログに記録 CloudTrail され、AWS Health APIリファレンス に記載されています。例えば、`DescribeEvents`、、および `DescribeAffectedEntities`オペレーションを呼び出すと`DescribeEventDetails`、CloudTrail ログファイルにエントリが生成されます。

AWS Health では、次のアクションをイベントとして CloudTrail ログファイルに記録できます。

- リクエストがルートまたはIAM認証情報を使用して行われたかどうか

- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが別の AWS サービスによって行われたかどうか

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

Amazon S3 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。デフォルトでは、ログファイルは Amazon S3 サーバー側の暗号化 () で暗号化されますSSE。

ログファイルの配信時に通知を受けるには、新しいログファイルの配信時に Amazon SNS通知を発行 CloudTrail するように を設定できます。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。

複数の AWS リージョンと複数の AWS アカウントの AWS Health ログファイルを 1 つの Amazon S3 バケットに集約することもできます。

詳細については、「複数のリージョンからの CloudTrail ログファイルの受信」および「複数のアカウントからの CloudTrail ログファイルの受信」を参照してください。

例: AWS Health ログファイルエントリ

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 DescribeEntityAggregatesオペレーションを示す CloudTrail ログエントリを示しています。

```
{
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
```

```
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

のドキュメント履歴 AWS Health

次の表に、 の今回のリリースのドキュメントを示します AWS Health。

- API バージョン： 2016-08-04

次の表は AWS Health 、2020 年 8 月 28 日以降のドキュメントの重要な更新点を示しています。RSS フィードをサブスクライブして、更新に関する通知を受け取ることができます。

変更	説明	日付
影響を受けるリソースのダウンロードに関する情報を更新しました	詳細については、「影響を受けるリソースビュー」を参照してください。	2024 年 7 月 27 日
セキュリティセクションの AWS Health ドキュメントから Internetwork トラフィックのプライバシーを削除しました	詳細については、「 のセキュリティ AWS Health」を参照してください。	2024 年 3 月 27 日
AWS Health ドキュメントの AWS Health Dashboard – Service Health and Planned Lifecycle Events を更新しました。	詳細については、AWS Health「Dashboard – Service Health」と「 の計画されたライフサイクルイベント AWS Health」を参照してください。	2024 年 2 月 15 日
の EventBridge ルールの作成で重複する箇条書きを削除しました AWS Health	「 の EventBridge ルールの作成」の「重複する箇条書き AWS Health」を削除しました。	2023 年 12 月 4 日
計画されたライフサイクルイベントに関するドキュメントを追加しました	詳細については、AWS Health の計画されたライフサイクルイベントを参照してください。	2023 年 10 月 31 日

AWSHealthFullAccess のドキュメントの更新	これで、 AWS GovCloud (US) Regionsで AWSHealthFullAccess のマネージドポリシーを使用できるようになりました。の AWS マネージドポリシーを参照してください AWS Health。	2023 年 10 月 16 日
で AWS ユーザー通知を設定するためのドキュメントを追加しました AWS Health。	で AWS ユーザー通知を設定できるようになりました AWS Health。詳細については、「 のAWS ユーザー通知を設定する AWS Health」を参照してください。	2023 年 8 月 30 日
委任管理者機能のドキュメントを AWS Health イベントの集約 セクションに追加しました。	詳細については、「委任された管理者の組織図」を参照してください。	2023 年 7 月 27 日
SLR ポリシーの更新	AWS マネージドポリシーの更新: Health_OrganizationsServiceRolePolicy。詳細については、「AWS HealthのAWS マネージドポリシー」を参照してください。	2023 年 7 月 19 日
AWS Health スキーマがイベントメタデータをサポートするようになりました	イベントから AWS Health イベントメタデータを受信できるようになりました。詳細については、「Amazon によるイベントのモニタリング AWS Health EventBridge」を参照してください。	2023 年 6 月 20 日

Amazon のドキュメントを更新しました EventBridge	Amazon EventBridge ルールを使用して、アカウント固有のイベントとパブリックイベントの両方をモニタリングできるようになりました。詳細については、「Amazon によるイベントのモニタリング AWS Health EventBridge」を参照してください。	2023 年 5 月 2 日
AWS 管理ポリシーのドキュメントを追加	「AWS HealthのAWS マネージドポリシー」と「AWS Healthのサービスリンクロールの使用」に関するドキュメントを追加しました。	2023 年 1 月 18 日
タイムゾーン設定に関するドキュメントを追加しました	新しいタイムゾーン機能を使用して、ローカルタイムゾーンまたは で AWS Health Dashboard を表示しますUTC。詳細については、AWS Health 「ダッシュボードの開始方法 – アカウントのヘルス」およびAWS Health 「ダッシュボード – サービスのヘルス」を参照してください。	2022 年 9 月 21 日
更新版	対応 AWS Health に関するドキュメントを追加しました。詳細については、「AWS Health Aware」を参照してください。	2022 年 5 月 25 日

更新版	Service Health Dashboard と AWS Personal Health Dashboardは、 AWS Health Dashboard にブランド変更されました。 詳細については、AWS Health「ダッシュボードの開始方法 – アカウントのヘルス」およびAWS Health「ダッシュボード – サービスのヘルス」を参照してください。	2022 年 2 月 28 日
Amazon のドキュメントを更新しました EventBridge	Amazon を使用して Health イベント EventBridge をモニタリング AWS Health するための の新しいトピック。詳細については、「Amazon によるイベントのモニタリング AWS Health EventBridge」を参照してください。	2022 年 2 月 3 日
更新版	Enterprise On-Ramp Support プランをお持ちの場合は、を使用できます AWS Health API。	2021 年 11 月 24 日
ドキュメントの追加	AWS Health 概念の新しいトピック。詳細については、AWS Healthの概念を参照してください。	2021 年 7 月 29 日

Events のドキュメントを更新しました CloudWatch	複数のサービスとイベントタイプのカテゴリに対してルールを作成する方法に関するセクションを追加しました。詳細については、複数のサービスおよびカテゴリに対するルールの作成を参照してください。	2021 年 5 月 7 日
Events のドキュメントを更新しました CloudWatch	Amazon CloudWatch Events ルールの AWS Systems Manager アクションを自動化するように セクションを更新しました。詳細については、「Amazon EC2インスタンスのアクションの自動化」を参照してください。	2021 年 4 月 28 日
Events のドキュメントを更新しました CloudWatch	チャットクライアントで AWS Health イベントを受信するためのセクションを追加しました。詳細については、「 で AWS Health イベントを受信する AWS Chatbot」を参照してください。	2021 年 3 月 16 日

更新版	以下のトピックが更新されました。 • AWS Health イベントの集計に関するトピックを更新しました • Amazon CloudWatch Events による AWS Health イベントのモニタリングトピックを再編成して更新しました • リソースおよびアクションに基づく条件セクションを更新しました	2021 年 1 月 29 日
AWS Health コンソールに組織ビューの AWS Health ダッシュボードを追加	AWS Health コンソールを使用して、組織ビュー機能を有効にできます。その後、 AWS 組織内のメンバーアカウントのヘルスイベントを表示できます。	2020 年 12 月 14 日
高可用性エンドポイントのデモ	サンプルコードを使用して、のアクティブなリージョンエンドポイントと署名 AWS リージョンを判断できます AWS Health。	2020 年 10 月 22 日
AWS Health ユーザーガイドの更新	組織が を更新し、 RSSフィードを追加しました。これにより、 AWS Health ドキュメントの最新の更新をサブスクライブできます。	2020 年 8 月 28 日

以前の更新

変更	説明	日付
組織ビューのトピックを更新し、例を含めました。	「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。	2020 年 6 月 3 日
セキュリティと AWS Health	AWS Healthを使用する際のセキュリティ上の考慮事項に関する情報を追加しました。「のセキュリティ AWS Health」を参照してください。	2020 年 5 月 4 日
AWS Organizationsのすべてのアカウントにわたって集計されたイベントに対して、組織ビューを使用する方法を説明する新しいセクションを追加しました。	「組織ビューでのアカウント全体の AWS Health イベントの集計」を参照してください。	2019 年 12 月 18 日
によって提供されるイベントの制限を説明する新しいセクション「リソースベースおよびアクションベースの条件」を追加しました AWS Health API。	「AWS Healthのためのアイデンティティおよびアクセス管理」を参照してください。	2018 年 8 月 2 日
AWS Health 情報の可視性に関するメモを追加しました。	「AWS Healthのためのアイデンティティおよびアクセス管理」を参照してください。	2017 年 8 月 16 日
サービスのリリース。	AWS Health がリリースされました。	2016 年 12 月 1 日

AWS 用語集

AWS の最新の用語については、「AWS の用語集リファレンス」の「AWS 用語集」を参照してください。

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