ユーザーガイド

AWS Health

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Health: ユーザーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS Health 1
の概念 AWS Health 2
AWS Health イベント 2
アカウント固有のイベント 3
パブリックイベント 3
AWS Health ダッシュボード 3
AWS Health ダッシュボード – サービスの状態 4
イベントタイプのコード 4
イベントタイプのカテゴリ 4
イベントステータス 6
影響を受けるエンティティ 6
AWS Health Amazon EventBridge のイベント 6
AWS Health API 7
組織ビュー 7
AWS User Notifications 7
入門 8
設定 8
にサインアップする AWS アカウント 9
管理アクセスを持つユーザーを作成する 9
AWS Health Dashboard でアカウントイベントを表示する 11
未解決の問題と最近の問題 11
予定された変更 12
その他の通知 13
イベントログ 13
イベントの詳細 14
イベントタイプ 16
カレンダービュー 16
影響を受けるリソースビュー 17
タイムゾーン設定 19
組織のヘルス 19
AWS Health イベントのアラート 20
Amazon EventBridge を設定する 20
で通知を管理する AWS User Notifications 21
AWS Health イベントの AWS マネージド通知サブスクリプションを設定する 22

AWS マネージド通知に関するよくある質問 ... 23
AWS Health ダッシュボード ... 25
の計画されたライフサイクルイベント AWS Health ... 28
計画的ライフサイクルイベントとは？ ... 28
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? ... 29
レジリエンス維持のための責任分担モデル ... 32
計画されたライフサイクルイベントへのアクセス ... 32
AWS Health API を使用した他のシステムとの統合 ... 33
AWS Health API リクエストの署名 ... 33
AWS Health API リクエストのエンドポイントの選択 ... 34
デモ: 過去 7 日間のイベントデータをプログラムで取得する ... 36
デモ: Java を使用して過去 7 日間の AWS Health イベントデータを取得する ... 36
デモ: Python を使用して過去 7 日間の AWS Health イベントデータを取得する ... 39
チュートリアル: AWS Health API と Java の使用例 ... 42
ステップ 1: 認証情報を初期化する ... 42
ステップ 2: AWS Health API クライアントを初期化する ... 43
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 ... 43
セキュリティ ... 47
データ保護 ... 48
データ暗号化 ... 49
アイデンティティ/アクセス管理 ... 49
対象者 ... 50
アイデンティティを使用した認証 ... 50
ポリシーを使用したアクセスの管理 ... 53
が IAM と AWS Health 連携する方法 ... 56
アイデンティティベースのポリシーの例 ... 62
トラブルシューティング ... 75
サービスリンクロールの使用 ... 78
AWS の マネージドポリシー AWS Health ... 80
でのログ記録とモニタリング AWS Health ... 86
コンプライアンス検証 ... 86
耐障害性 ... 88
インフラストラクチャセキュリティ ... 88
設定と脆弱性の分析 ... 89
セキュリティに関するベストプラクティス ... 89
ユーザーに AWS Health 最小限のアクセス許可を付与する ... 89

を表示する AWS Health Dashboard ... 89
Amazon Chime または Slack AWS Health との統合 ... 89
AWS Health イベントのモニタリング ... 89
AWS Health イベントの集約 ... 91
前提条件 ... 91
組織ビューの有効化 ... 92
組織ビューを表示する ... 96
組織ビューの無効化 ... 101
組織の委任管理者ビューを管理する ... 102
委任管理者アカウントを登録する ... 102
委任管理者アカウントを削除する ... 103
EventBridge を使用した Health イベントのモニタリング ... 104
AWS リージョン カバレッジの EventBridge ルールの作成 ... 105
AWS Healthのアカウント固有イベントとパブリックイベントをモニタリングする ... 106
EventBridge での AWS Health イベントのページ分割リストの表示 ... 108
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 ... 108
AWS Health イベントモニタリングと通知を JIRA および ServiceNow と統合する ... 109
EventBridge ルールを設定してイベントに関する通知を送信する ... 109
複数のサービスおよびカテゴリに対するルールの作成 ... 113
イベントに関する通知を送信するようにチャットアプリケーションで Amazon Q Developer を設定する ... 115
前提条件 ... 115
イベントに応答して EC2 インスタンスでオペレーションを自動的に実行する ... 117
前提条件 ... 118
EventBridge のルールを作成する ... 122
リファレンス： AWS Health イベント Amazon EventBridge スキーマ ... 125
AWS Health イベントスキーマ ... 125
公開ヘルスイベント-Amazon EC2 の運用上の問題 ... 138
アカウント固有の AWS Health イベント - Elastic Load Balancing API の問題 ... 139
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 ... 140
モニタリング AWS Health ... 141
を使用した AWS Health API コールのログ記録 AWS CloudTrail ... 141
AWS Health CloudTrail の情報 ... 142
例: AWS Health ログファイルエントリ ... 143
ドキュメント履歴 ... 145

以前の更新 154
..... clv

とは AWS Health

AWS Health は、リソースのパフォーマンスと、 AWS のサービス および アカウントの可用性を継続的に可視化します。イベントを使用して AWS Health 、サービスやリソースの変更が 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学習できます AWS。 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 AWS Health 提供します。 AWS Health また、 は、計画されたアクティビティを認識し、準備するのに役立ちます。このサービスは、 AWS リソースの正常性の変化によってトリガーされるアラートと通知を配信するため、ほぼ瞬時にイベントを可視化し、トラブルシューティングを迅速化するためのガイダンスを得ることができます。

すべてのお客様は、 AWS Health API を搭載した AWS Health Dashboard を使用できます。ダッシュボードはセットアップを必要とせず、認証された AWS ユーザーに使用できる状態です。その他のサービスハイライトについては、AWS Health 「ダッシュボードの詳細ページ」を参照してください。

AWS Health は、すべてのお客様に AWS Health Dashboard と呼ばれるコンソールを提供します。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。

サービスの使用中に発生する AWS Health と用語の基本については、 AWS Health 「」を参照してくださいの概念 AWS Health。

> **メモ**
>
> - AWS Health ダッシュボードは、すべての AWS お客様が追加料金なしで利用できます。
> - すべての 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。
> - Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合は、AWS Health API を使用して社内およびサードパーティーのシステムと統合できます。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。
> - 利用可能な AWS サポート プランの詳細については、「」を参照してくださいAWS サポート。

の概念 AWS Health

の AWS Health 概念について説明し、 サービスを使用して 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 ダッシュボード
- イベントタイプのコード
- イベントタイプのカテゴリ
- イベントステータス
- 影響を受けるエンティティ
- AWS Health Amazon EventBridge のイベント
- AWS Health API
- 組織ビュー
- AWS User Notifications

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、 AWS Identity and Access Management (IAM) が管理ポリシーを廃止する予定の場合、またはマネージドルールを廃止 AWS Config する予定の場合、 はイベントを送信 AWS Health できます。 は、 でサービスの可用性の問題が発生した場合 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
- パブリックイベント

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 AWS 組織内のアカウントのいずれかにローカルです。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、または Amazon EventBridge やAWS ユーザー通知を使用して通知を受け取ることができます。

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、 AWS Health は、そのサービスを使用していなくても、またそのリージョンに S3 バケットがあっても、イベントに関する情報を提供します。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 Dashboard – 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」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」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の問題など、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 ダッシュボードを使用して、アカウントの廃止されたリソースなど、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 して、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」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」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のがベストプラクティスです。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。DescribeEventTypes 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確認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 WorkSpaces にサービスに関する問題があります。

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、サポート終了通知や異なるバージョンの自動アップグレードなど、計画的な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 AI には、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、お客様の対応が必要な、あるバージョンのサポート終了イベントなど、計画的なライフサイクルイベントをスケジュールしています。

> **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 EventBridge のイベント

アカウントに Amazon EventBridge ルールを設定して、アカウントが適切な AWS Health イベントを受信した後の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 EventBridge AWS Health を使用した でのイベントのモニタリング」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 サポートを使用するには、 からビジネス、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。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 Health Dashboard の 1 つのビュー AWS Organizations 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、「アカウント間の AWS Health イベントの集約」を参照してください。

AWS User Notifications

AWS Health は と統合AWS User Notificationsされているため、 および のサービスに影響するイベントに関する通知を簡単に受信 AWS アカウント および制御できます。 は、デフォルトで AWS Health イベントのマネージド通知 User Notifications を提供します。これらのサブスクリプションを設定して、時間ベースの集約によるメッセージの受信頻度、通知を受け取る AWS Health イベントの種類、通知の配信先を制御できます。開始するには、 User Notifications で を開きますAWS Management Console。詳細については、「で AWS Health 通知を管理する AWS User Notifications」を参照してください

AWS Health ダッシュボードの開始方法

AWS Health ダッシュボードを使用して 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 のサービス 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 ダッシュボードに以下の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**
>
> がない場合は AWS アカウント、 を使用して一般的なサービスの可用性AWS Health ダッシュボードを確認できます。
> アカウントをお持ちの場合は、 AWS Health Dashboard にサインインして、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。

トピック

- AWS アカウントのセットアップ
- AWS Health Dashboard でアカウントイベントを表示する
- Amazon EventBridge を設定する
- で AWS Health 通知を管理する AWS User Notifications

AWS アカウントのセットアップ

を有効にする前に AWS Health、 が必要です AWS アカウント。 AWS アカウントがない場合は、次の手順を実行してアカウントを作成します。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

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

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

管理アクセスを持つユーザーを作成する

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

を保護する AWS アカウントのルートユーザー

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

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

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

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

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

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

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

管理アクセス権を持つユーザーとしてサインインする

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

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

追加のユーザーにアクセス権を割り当てる

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

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

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

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

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. AWS Health ダッシュボードを https://health.aws.amazon.com/health/home で開きます。
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。

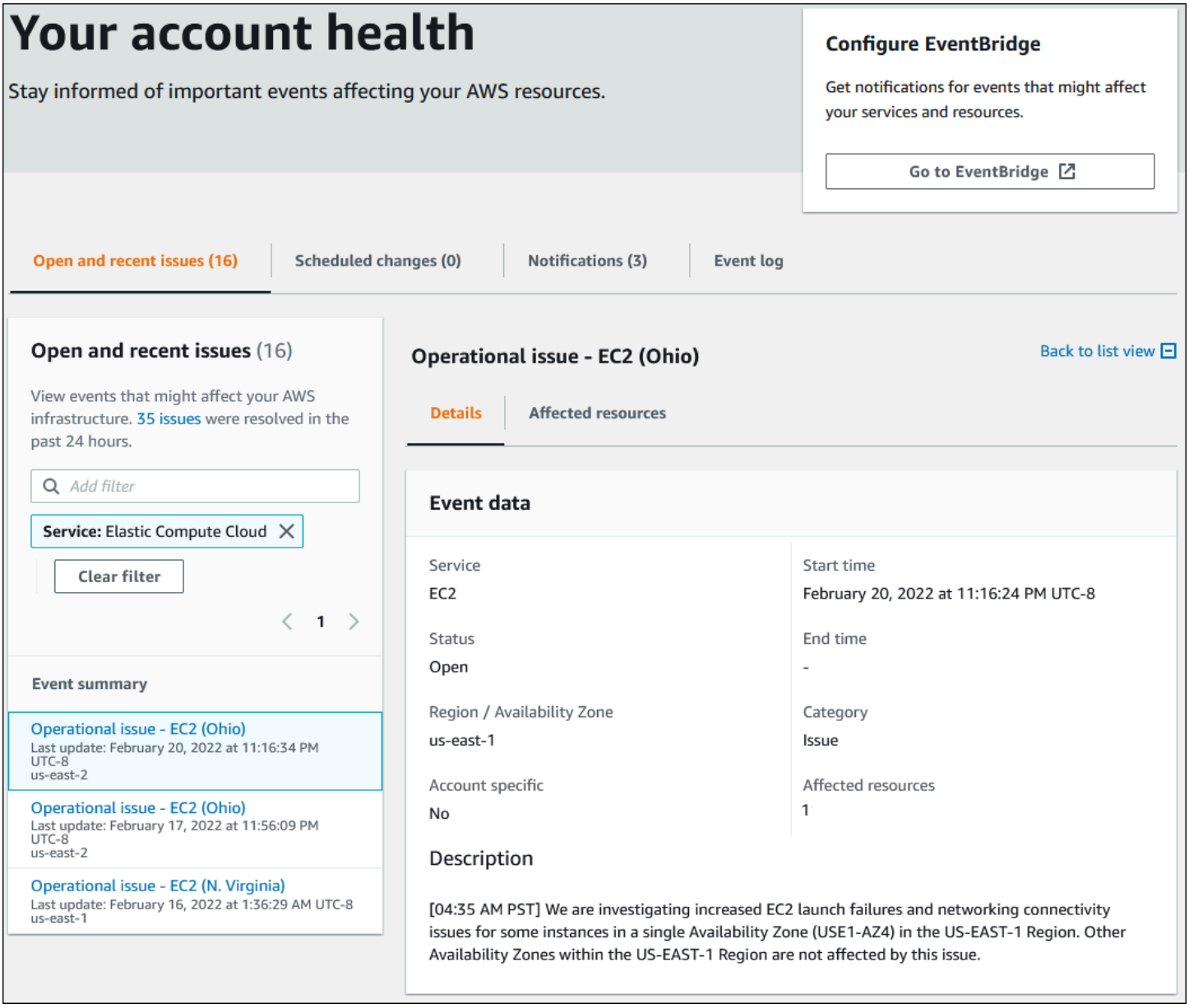
表示されたイベントは、タブを問わず、フィルタリストからオプションを選択してフィルタリングできます。たとえば、アベイラビリティーゾーン、リージョン、イベント終了時刻、最終更新時刻 AWS のサービスなどで結果を絞り込むことができます。

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 のサービス 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) の運用問題イベント

以下の画像は、Amazon EC2 インスタンスの起動エラーと接続問題の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、「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。

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

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。

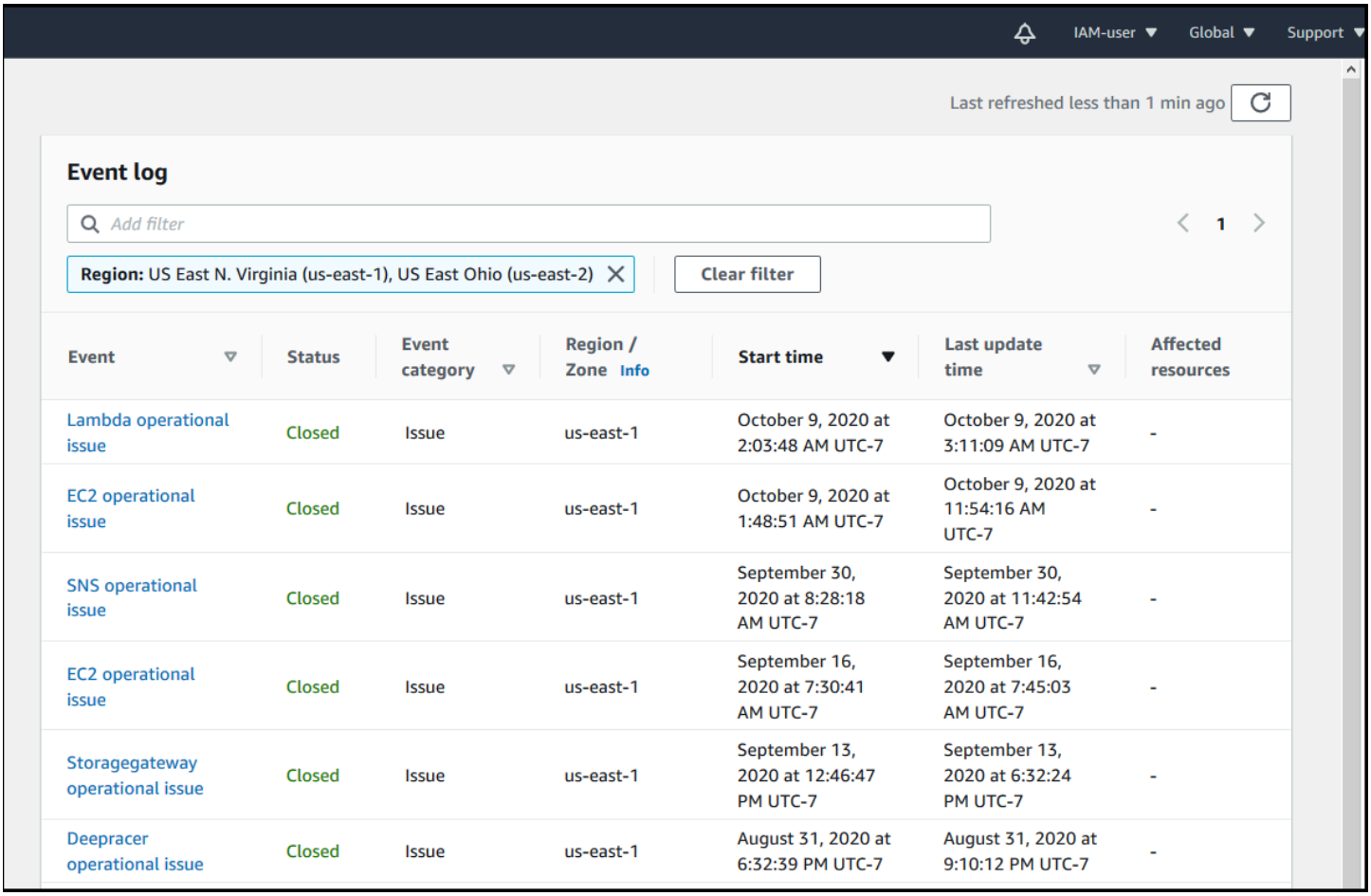
[イベントログ] テーブルでイベントを選択すると、[詳細] ペインにイベントと影響を受けるリソースのリストの情報が示されます。詳細については、「イベントの詳細」を参照してください。

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

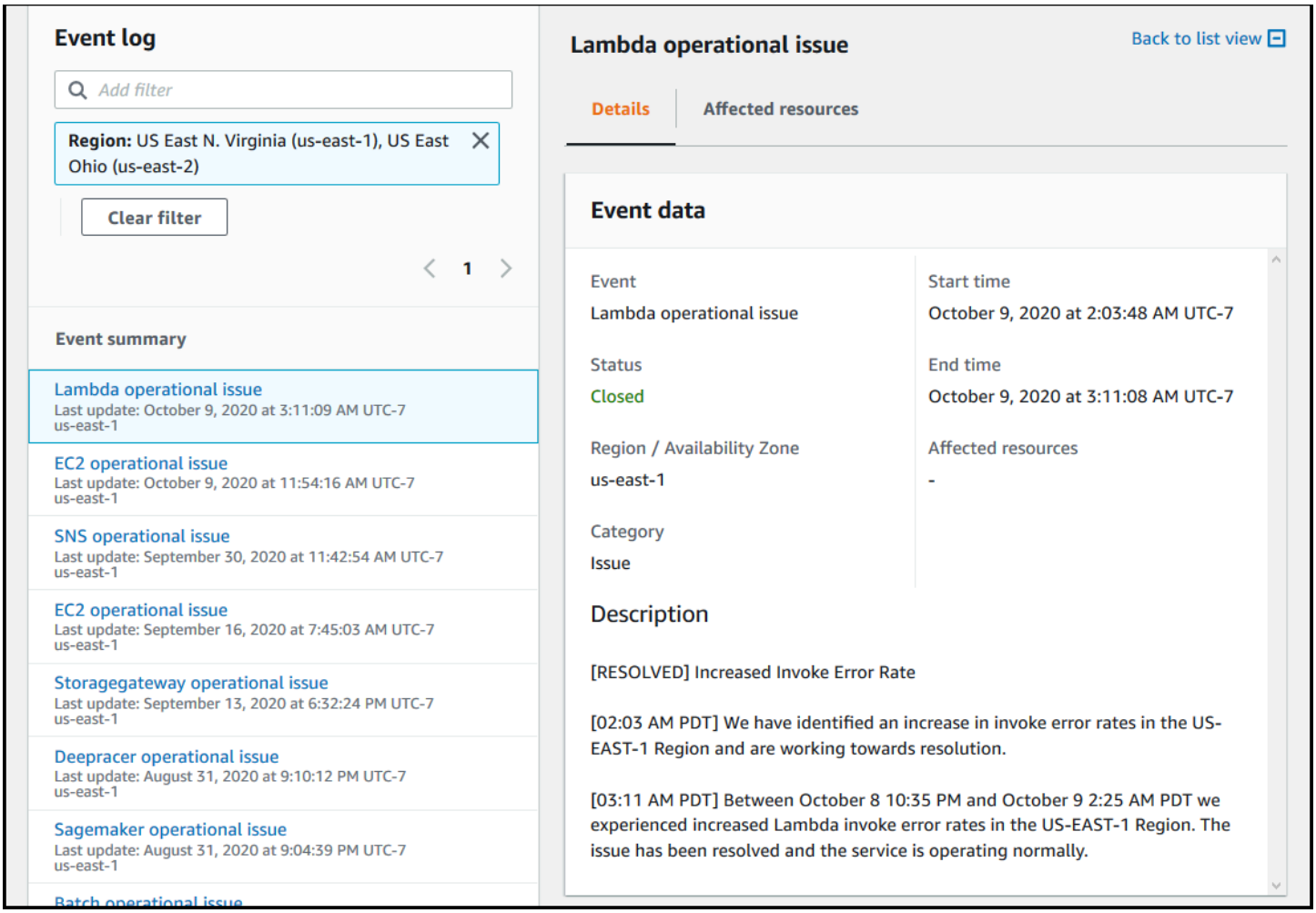
影響を受けるリソースタブには、イベントによって影響を受ける AWS リソースに関する次の情報が表示されます。

- リソース ID (例: `vol-a1b2c34f` などの Amazon EBS ボリューム ID) または Amazon リソースネーム (ARN) (ある場合または該当する場合)。
- 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) も含まれます。このリストは通常 24 時間に 1 回更新されますが、現在のステータスを反映するまでに最大 72 時間かかる場合があります。

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 ARN で結果を絞り込むことができます。

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、 で Amazon EC2 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または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。たとえば、AWS リージョン 使用する の Amazon EC2 インスタンスに問題がある場合、 はイベントと影響を受ける Amazon EC2 インスタンスのリストに関する情報 AWS Health を提供します。

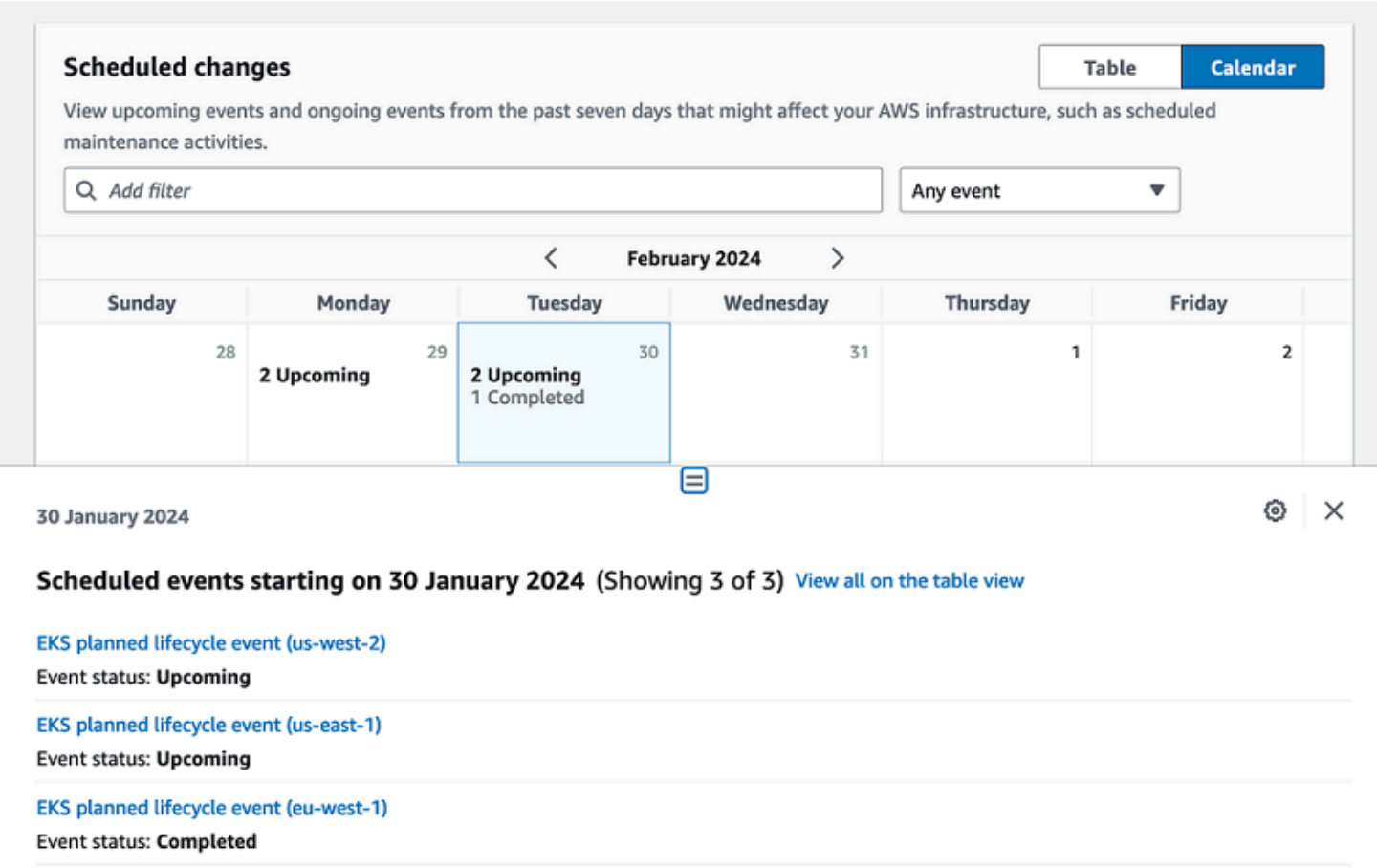
次のオプションを使用して、イベントがパブリックかアカウント固有かを識別できます。

- 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」を参照してください。
- AWS Health API を使用して `eventScopeCode`パラメータを返します。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使用でき、 AWS Health イベントを毎月のカレンダーにプロジェクトできます。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] タブに表示されます。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。

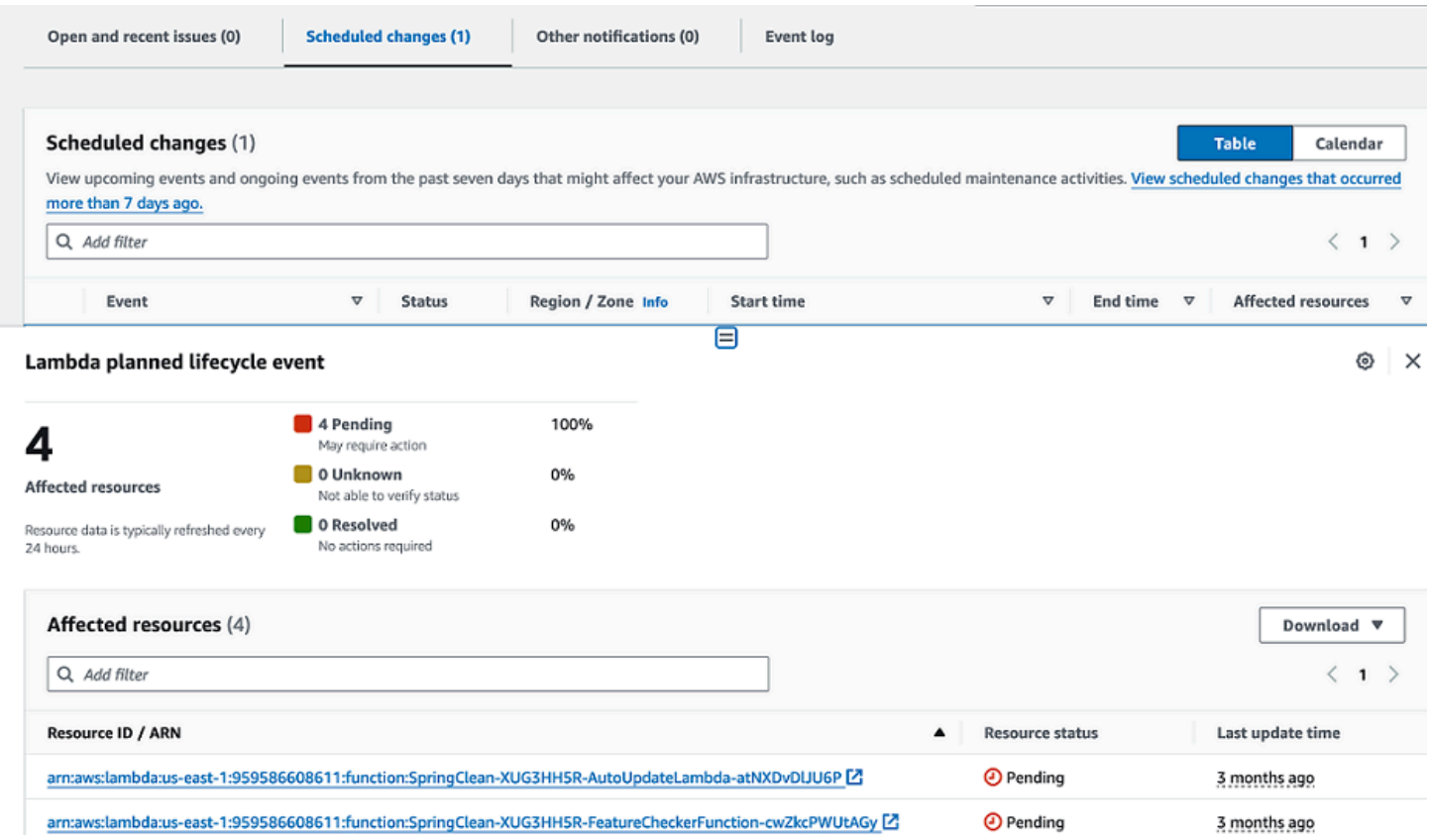
アカウントレベルの AWS Health イベントでは、影響を受けるリソースタブの上部に、影響を受けるリソースのステータスの概要が表示されます。影響を受けるリソースの一覧が、対応するステータスとともにテーブルに表示されます。計画ライフサイクルイベントは、[リソースステータス]フィールドを使用するイベントタイプの一例です。計画されたライフサイクルイベントの詳細については、AWS Healthの計画されたライフサイクルイベントを参照してください。

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] タブで 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内のすべてのリソースが含まれます。組織ビューでアカウントレベルに移動し、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。ダウンロードし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、eventARN、エンティティ名、entityARN、ステータス、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な場合、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 UTC で表示できます。 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。

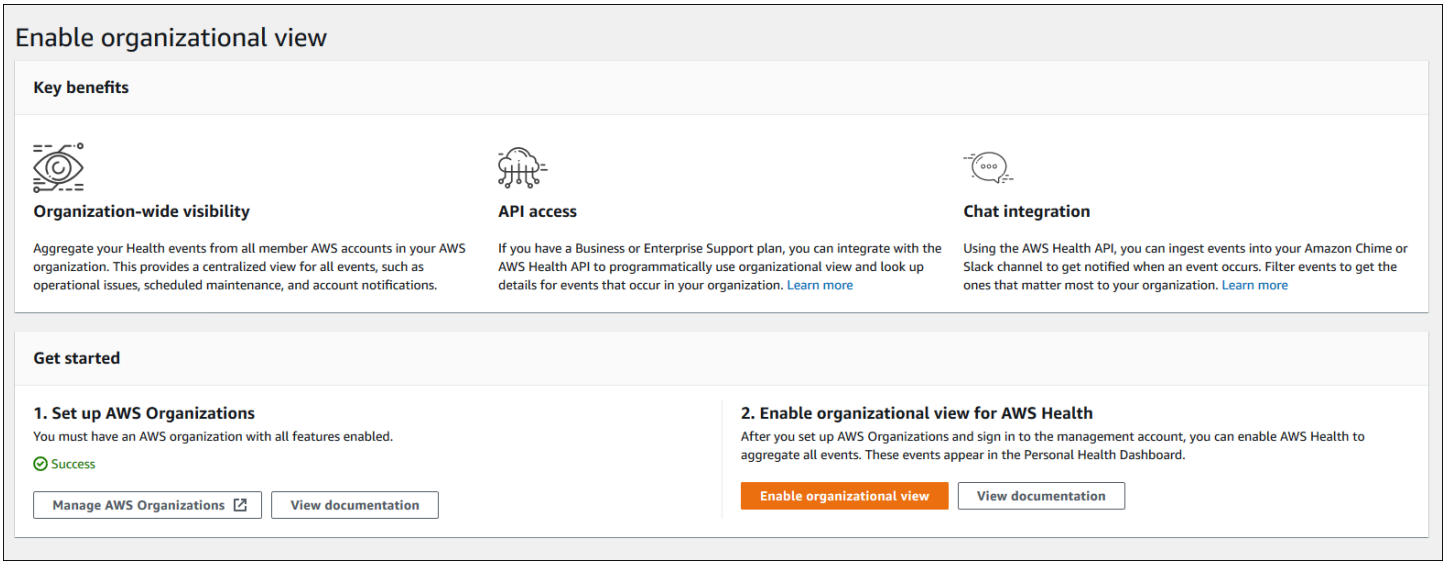
タイムゾーン設定を更新するには

1. AWS Health ダッシュボードを https://health.aws.amazon.com/health/home で開きます。
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、「アカウント間の AWS Health イベントの集約」を参照してください。



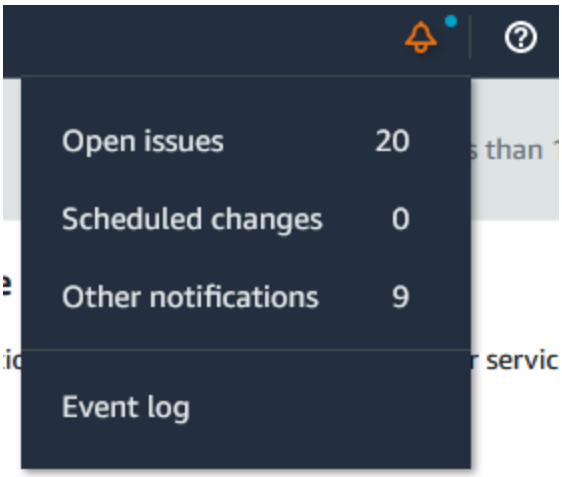
AWS Health イベントのアラート

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は、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 EC2、Amazon Relational Database Service (Amazon RDS)、 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 Dashboard 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。



Amazon EventBridge を設定する

EventBridge を使用して、 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 AWS Health が通知するか、アクションを実行するようにルールを設定できます。

で EventBridge を使用する AWS Health

1. AWS Health ダッシュボードを https://health.aws.amazon.com/health/home で開きます。
2. EventBridge コンソールに移動してルールを作成するには、以下のいずれかの操作を行います。
   - ナビゲーションペインの [Health インテグレーション]から[Amazon EventBridge]を選択します。

- [EventBridge の設定]で、[EventBridge に移動]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 EventBridge AWS Health を使用した でのイベントのモニタリング」を参照してください。

で AWS Health 通知を管理する AWS User Notifications

AWS の マネージド通知 AWS User Notifications を使用すると、 および サービスに影響するイベントに関する通知を受信 AWS アカウント および管理できます。で AWS マネージド通知を使用すると AWS User Notifications、受信する AWS Health イベントカテゴリを指定したり、E メールの組織ビューを設定したり、複数の類似 E メールの代わりに統合通知を取得したりできます。このサービスを有効にする方法については、「 AWS Health の AWS マネージド通知の有効化または無効化 AWS User Notifications」を参照してください。

以下の追加チャネルを選択して、 AWS Health イベントを受信できます AWS User Notifications。

- E メール
- Chat
- へのプッシュ通知 AWS Console Mobile Application

これらの通知は直接 AWS Health ツールほど詳細ではありませんが、問題や変更を利害関係者に通知する効果的な方法を提供します。

> **Note**
>
> 影響を受けるリソース IDs、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、 AWS Health イベントの詳細を包括的に可視化するには、次のいずれかの AWS Health ツールを使用することをお勧めします。
>
> - AWS Health API
> - Amazon EventBridge の aws.health ソース
> - AWS Health Dashboard「 ◆◆
>
> これらのツールは、ワークロードに影響を与え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を提供します。

AWS Health イベントの AWS マネージド通知サブスクリプションを設定する

AWS マネージド通知サブスクリプションを設定するには、次の手順を実行します。

1. User Notifications で を開きますAWS Management Console。
2. ナビゲーションペインで、AWS マネージド通知サブスクリプションを選択します。
3. AWS Health 通知の送信 AWS User Notifications 者として を有効にしていない場合は、 AWS Health 通知を有効にするを選択します。これにより、 からの E メールが無効になり AWS Health 、 からの E メールが有効になります User Notifications。詳細については、「 AWS Health の AWS マネージド通知の有効化または無効化 AWS User Notifications」を参照してください。
4. AWS Health イベント通知はカテゴリ別に管理できます。詳細については、「 での AWS マネージド通知のアカウント連絡先の追加と削除 AWS User Notifications」を参照してください。

> **Note**
>
> AWS Health は、 AWS のマネージド通知に E メール配信を移行しています AWS User Notifications。以下は、重要な日付の一部です。
>
> - 2025 年 9 月 14 日まで: AWS マネージド通知を使用するためのオプトイン期間。
> - 2025 年 9 月 15 日: AWS マネージド通知は既存のすべての に対して有効になっています AWS アカウント。新しい の場合 AWS アカウント、マネージド通知はデフォルトで有効になっています。マネージド通知は、2025 年 12 月 15 日まで有効または無効にできます。
> - 2025 年 12 月 15 日: AWS マネージド通知はすべてのアカウントで有効になっており、無効にすることはできません。
>
> AWS Health イベントの通知を引き続き受信するためにアクションは必要ありません。 AWS マネージド通知を有効にすると、いくつかの変更と機能強化があります。詳細については、『』の AWS 「マネージド通知を有効にした場合の変更点」を参照してくださいAWSAWS ユーザー通知に関するよくある質問の マネージド通知。

AWSAWS ユーザー通知に関するよくある質問の マネージド通知

AWS マネージド通知を有効にすると、どのような変更がありますか？

デフォルトでは、マネージド通知に関する E メールは、既存のアカウントの連絡先 (ルート、オペレーション、請求、セキュリティ E メールアドレス) に送信されます。 AWS マネージド通知から受信する E メールは、 `health@aws.com` の代わりに から送信され`no-reply-aws@amazon.com`、E メールの形式が変更されます。送信者 ID による E メールのルーティングや E メールのコンテンツのスクレイピングなど、 AWS Health 通知の E メールルールを以前に設定した場合は、新しい E メール形式と一致するようにこの設定を更新する必要があります。プッシュ通知による自動化が必要な場合は、マネージド通知の代わりに Amazon EventBridge を介して送信された AWS Health イベントを評価することをお勧めします。

E メールの集約はどのように機能し、この機能を有効にするのですか？

AWS マネージド通知は、同じ AWS Organizations 組織内の複数のアカウントに影響を与える AWS Health イベントを 1 つの集計通知に集約します。集計された組織は、管理アカウントの通知センターで表示できます。マネージド通知は、集約された通知を管理アカウントの連絡先に E メールで送信します。重複する E メールを減らすために、 AWS 管理対象通知は、アカウントの連絡先が管理アカウントとメンバーアカウント間で共有されるときに 1 つの通知を送信します。

集約を有効にするには、管理アカウントと AWS User Notifications サービス間の信頼されたアクセス AWS Organizations を設定して付与する必要があります。

詳細については、「 AWS でのマネージド通知の集約 AWS User Notifications」を参照してください。

AWS マネージド通知から集約された E メールを受信する AWS User Notifications には、 で AWS Organizations 信頼されたアクセスを有効にする必要がありますか？

はい。 AWS User Notifications からの への信頼されたアクセス AWS Organizations が必要です。

AWS Health と AWS Organizations を使用して で信頼されたアクセスを有効にする場合の違いは何ですか AWS User Notifications？

組織の信頼と関連する委任管理者権限は、サービスによって割り当てられ、過度に拡張されたアクセス許可に対するガードレールとして機能します。の信頼されたアクセス AWS Health により AWS Health Dashboard、Amazon EventBridge を介して送信される 、 AWS Health サービス、および AWS Health イベントの組織ビューが可能になります。の信頼されたアクセス AWS User Notifications により、 内の通知を集約 AWS User Notifications して AWS Health 通知できます。信頼

されたアクセスは共有されないため、委任された管理者の設定はサービスごとに個別に追加する必要があります。

マネージド通知はどこで有効にできますか？

からマネージド通知を有効にします AWS Management Console。詳細については、「AWS Health の AWS マネージド通知の有効化または無効化 AWS User Notifications」を参照してください。

特定のユースケースでプレーンテキストの E メールを保持する方法はありますか？

いいえ。移行が完了すると、現在のプレーンテキスト AWS Health E メールは無効になります。E メールルールを使用してさまざまなワークフローを実行する場合は、代わりに Amazon EventBridge を介して送信された AWS Health イベントを評価することをお勧めします。

AWS Health ダッシュボード

AWS Health Dashboard – Service Health を使用して、すべてのヘルスを表示できます AWS のサービス。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 – サービスの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。アカウントがすでにある場合は、サインインして AWS Health Dashboard 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」を参照してください。

AWS Health ダッシュボードを表示するには – サービスの状態

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

   > **Note**
   >
   > AWS アカウントページに既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。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。例えば、[運用上の問題 — Amazon Elastic Compute Cloud (バージニア北部)]
   - サービス名
   - 影響または低下などのイベントの重要度
   - イベントの最新更新のタイムライン
   - このイベントの影響も受け AWS のサービス ている 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。

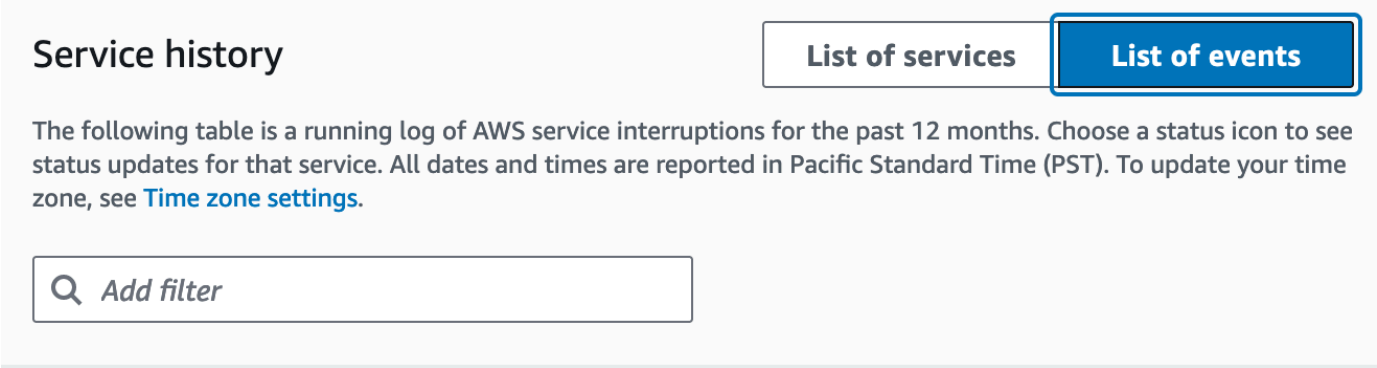
3. (オプション) イベントの横にある [RSS] を選択すると、そのイベントの RSS フィードをサブスクライブできます。指定された で、この特定のサービスに関する通知を受け取ります AWS リージョン。
4. [サービス履歴] を選択すると、[サービス履歴] テーブルが表示されます。この表は、過去 12 か月間のすべての AWS のサービス 中断を示しています。

> **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。イベント列のイベントを選択すると、その特定のイベントに関する詳細情報がポップアップサイドパネルに表示されます。



> **Note**
>
> 2023 年 9 月以降の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後、そのイベントポップアップでイベントのリストビューに移動します。

7. (オプション) RSS フィードをサブスクライブするには、[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」を参照してください。

AWS Healthの計画されたライフサイクルイベント

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？
- 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?
- レジリエンス維持のための責任分担モデル
- 計画されたライフサイクルイベントへのアクセス

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を与える可能性のある重要な変更を伝達します。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実行します。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 のサービス 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、 は、アップグレードやアプリケーションへの影響を回避するためのアクションを実行する必要がある場合 AWS に通知します。
  - 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。

> **Note**
>
> この基準に一致するすべての通知は、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け取った時点から、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**
>
> - 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。
> - 動的な更新が提供されない例外では、リソースには、「PENDING」または「RESOLVED」ステータスのリソースはなく、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び、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。

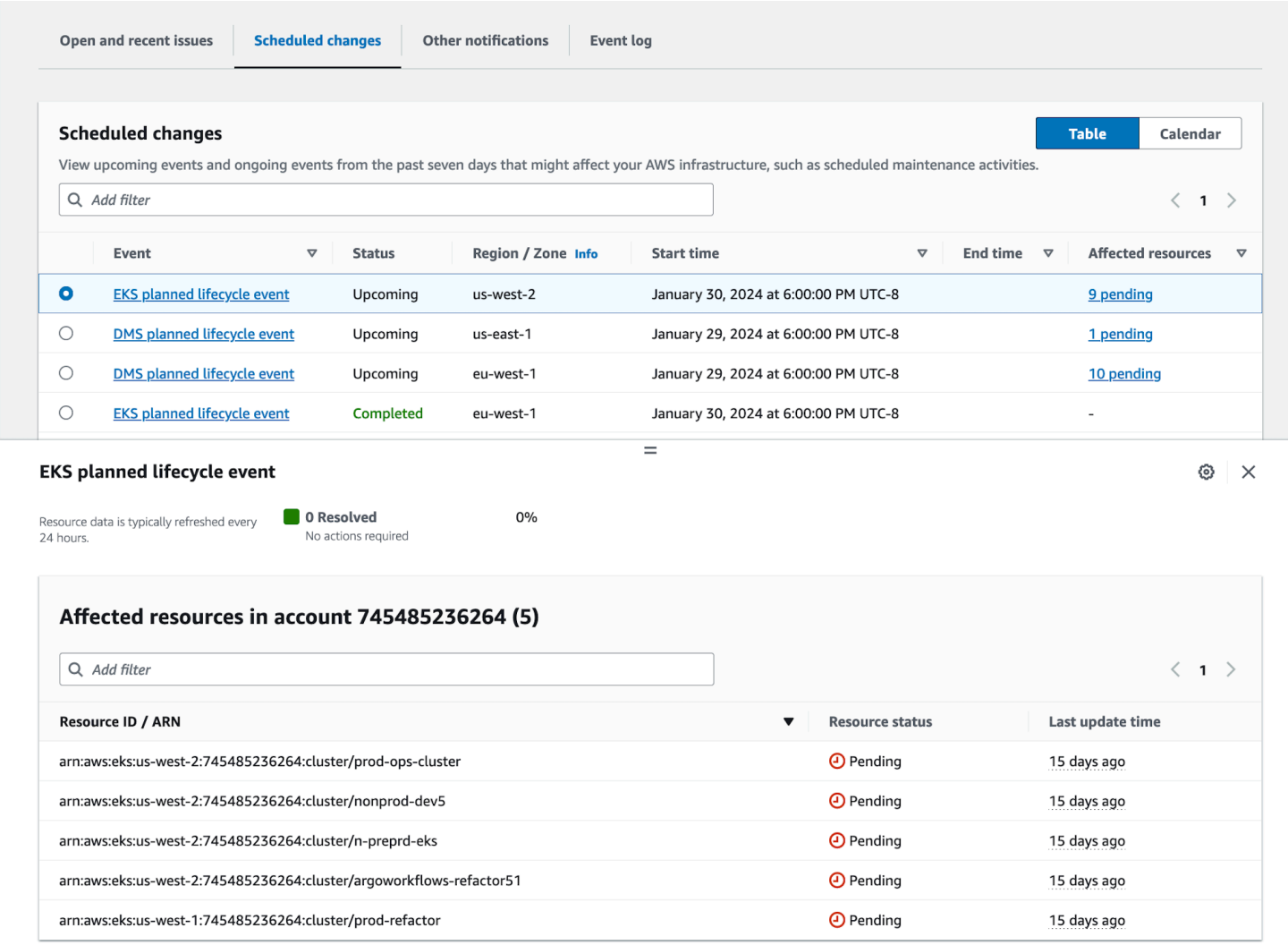
イベント終了時刻： イベント終了時刻は、すべての AWS リソースで変更が終了した日付です。終了時間は必ずしも指定されるわけではないことに注意してください。開始時間を変更日として扱うことが重要です。

> **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済みの、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、組織に多数の影響を受ける AWS アカウント またはリソースがある場合、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け取った時点から、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、可能な場合は経時的にステータスの更新を提供します。
> - 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。

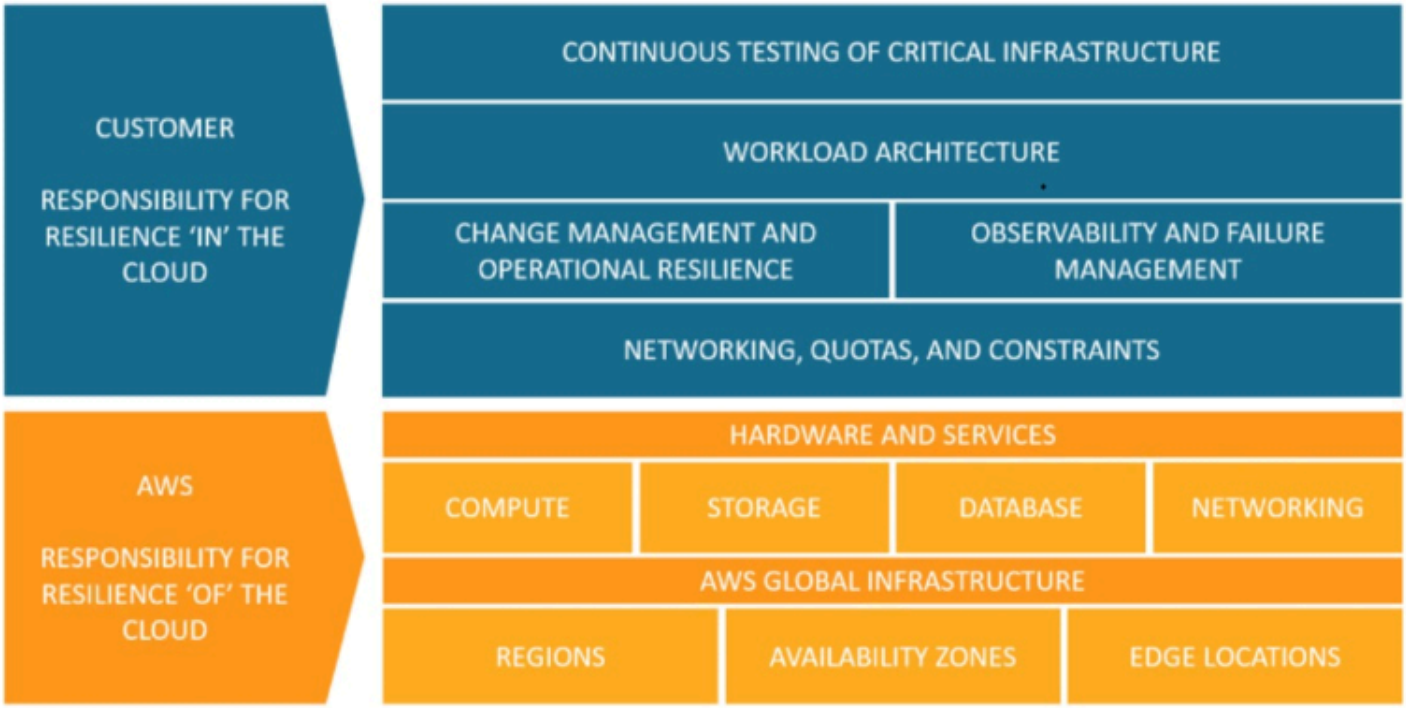


予定されているイベントの日付が過ぎた場合

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 イベントはステータス に変わります`Closed`。
3. 変更日以降に未解決のリソースが解決されない場合、 AWS Health イベントはイベントの開始日または終了日から 4 年間 (いずれか遅い方) 開いたままになります。この時間が経過すると、AWS Health 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 と顧客の間で共有される責任です。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、 AWS 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的なセキュリティまで、コンポーネントを運用、管理、制御するためです。お客様は、 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 (更新プログラム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 AWS。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 EventBridge の使用
- 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 API を使用した AWS Health 他のシステムとの統合

AWS Health は、トランスポートとして HTTPS を使用し、メッセージのシリアル化形式として JSON を使用する RESTful 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 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 AWS サポートを使用するには、 からビジネス、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。Business、Enterprise On-Ramp、または Enterprise Support プランがない AWS 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。

AWS SDKs を使用して REST API AWS Health コールをラップできるため、アプリケーション開発を簡素化できます。 AWS 認証情報を指定すると、これらのライブラリが認証とリクエストの署名を処理します。

AWS Health には、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するために AWS Management Console 使用できる の AWS Health Dashboard も用意されています。「AWS Health ダッシュボードの開始方法」を参照してください。

トピック

- AWS Health API リクエストの署名
- AWS Health API リクエストのエンドポイントの選択
- デモ: 過去 7 日間の AWS Health イベントデータをプログラムで取得する
- チュートリアル: AWS Health API と Java の使用例

AWS Health API リクエストの署名

AWS SDKs または AWS Command Line Interface （ AWS CLI) を使用して にリクエストを行うと AWS、これらのツールはツールの設定時に指定したアクセスキーを使用して自動的にリクエストに

署名します。例えば、前の高可用性エンドポイントデモ AWS SDK for Java で を使用する場合、リクエストに自分で署名する必要はありません。

Java コードの例

で AWS Health API を使用する方法のその他の例については AWS SDK for Java、このサンプルコードを参照してください。

リクエストを行う場合は、 への定期的なアクセスに 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 AWS Health。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 SDKs または を使用しない場合は AWS CLI、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、『』のAWS 「 API リクエストの署名」を参照してくださいAWS 全般のリファレンス。

AWS Health API リクエストのエンドポイントの選択

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/パッシブ設定に 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と対応する署名 AWS リージョンを判断できます。これにより、コードで使用するエンドポイントがわかり、最新情報を取得できます AWS Health。

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 AWS へのアクセス認証情報を指定し、リージョンの署名を設定する必要があります。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。

IPv6-onlyリクエストの場合は、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 を判断し AWS リージョン 、そのリージョンで IPv6 がサポートするデュアルスタックエンドポイントを呼び出すことをお勧めします。

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
アクティブ	us-east-1	health.us-east-1.amazonaws.com (IPv4 のみ) health.us-east-1.api.aws (IPv4 および IPv6 をサポート)	HTTPS
パッシブ	us-east-2	health.us-east-2.amazonaws.com (IPv4 のみ) health.us-east-2.api.aws (IPv4 および IPv6 をサポート)	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、どのエンドポイントを使用するかを示します AWS Health。

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

> **Tip**
> アクティブエンドポイントとパッシブ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。

デモ: 過去 7 日間の AWS Health イベントデータをプログラムで取得する

次のコード例では、 はグローバルエンドポイントに対する DNS ルックアップ AWS Health を使用して、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決定します。 はこの情報 AWS Health を使用して、過去 7 日間のイベントデータのレポートを取得します。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

- デモ: Java を使用して過去 7 日間の AWS Health イベントデータを取得する
- デモ: Python を使用して過去 7 日間の AWS Health イベントデータを取得する

デモ: Java を使用して過去 7 日間の AWS Health イベントデータを取得する

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. AWS 認証情報を指定するには、次のコマンドを入力します。

```
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 event 出力

このコード例では、 AWS アカウント内の過去 7 日間の最近の 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 ###
# [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。

デモ: Python を使用して過去 7 日間の AWS Health イベントデータを取得する

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. AWS 認証情報を指定するには、次のコマンドを入力します。

```
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 event 出力

このコード例では、 AWS アカウント内の過去 7 日間の最近の 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 #### [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。

チュートリアル: AWS Health API と Java の使用例

次の Java コード例は、 AWS Health クライアントを初期化し、イベントとエンティティに関する情報を取得する方法を示しています。

ステップ 1: 認証情報を初期化する

AWS Health API と通信するには、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任意の 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を活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。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 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 AWS 責任があります。 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。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。が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。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、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、 を使用する際の責任共有モデルの適用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 AWS Health ように 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 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
- でのロ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。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR の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 (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」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を、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含めないことを強くお勧めします。これは、コンソール AWS Health 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を操作する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL 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 暗号化する方法に関する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。転送中のデータは、Transport Layer Security (TLS) を使用して保護することも、クライアント側の暗号化を使用して保存することもできます。

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 のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Health リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス 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
- が IAM と AWS Health 連携する方法
- 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、作業内容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提供されます。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。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を使用する方法の詳細については AWS Health、「」を参照してくださいが IAM と AWS Health 連携する方法。

IAM 管理者 - 管理者は、 AWS Healthへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる 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。

アイデンティティを使用した認証

認証は、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 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場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーの種類に応じて、 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、「 AWS サインイン ユーザーガイド」の「 へのサインイン AWS アカウント方法」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を暗号化して署名します。AWS ツールを使用しない場合は、自分でリクエストに署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。たとえば、 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 AWS 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「IAM ユーザーガイド」の「IAM のAWS 多要素認証」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 のサービス完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

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 ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。

例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」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 ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。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 URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド 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については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (プロキシとしてロールを使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の は他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプ

リケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、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アクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする と組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンク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 EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」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、ID AWS 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、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。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 API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、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 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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーに

よって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

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

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、 AWS Health Dashboard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。

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 (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

AWS Health は ACLs をサポートしていません。

その他のポリシータイプ

AWS は、一般的で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ポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。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) の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、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 AWS アカウント です。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

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

が IAM と AWS Health 連携する方法

IAM を使用して へのアクセスを管理する前に AWS Health、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 IAM と連携する方法の概要を把握するには、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

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を指定でき、さらにアクションが許可または拒否された条件を指定できます。 AWS Health は、特定のアクション、リソース、および条件キーをサポートします。JSON ポリシーで使用するすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」を参照してください。

アクション

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない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アクセス許可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:。たとえば、DescribeEventDetails API オペレーションを使用して、指定し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、IAM ユーザーガイドの「 で定義されるアクション AWS Health」を参照してください。

リソース

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの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
```

たとえば、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 ARN を使用します。

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

特定のアカウントに属する Amazon EC2 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/*/*"
```

ARN の形式の詳細については、「Amazon リソースネーム (ARNs 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、複数のリソースを含めることができます。たとえば、DescribeEvents オペレーションは、指定し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。これは、IAM ユーザーが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ることを意味します。

複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

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

AWS Health は、ヘルスイベントと DescribeAffectedEntities および DescribeEventDetails API 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 ARNs「 で定義されるリソース AWS Health」を参照してください。 どのアクションで各リソースの ARN を指定できるかについては、AWS Healthで定義されるアクションを参照してください。

条件キー

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに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して、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 ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

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

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

DescribeAffectedEntities および DescribeEventDetails API 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ています。

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、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシー

にクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる 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、IAM ユーザーガイドの「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

AWS Health は、DescribeAffectedEntities および DescribeEventDetails API 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く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する、IAM 役割を引き受ける、またはクロスアカウント役割を引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

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。

サービスにリンクされた役割

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。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの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。ロールには Health_OrganizationsServiceRolePolicy AWS 管理ポリシーがアタッチされています。管理ポリシーにより AWS Health 、 AWS は組織内の他の 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、IAM API、または AWS Command Line Interface () を使用してロールを削除できますAWS CLI。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使用」を参照してください。

詳細については、「アカウント間の AWS Health イベントの集約」を参照してください。

サービス役割

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役割を引き受けることが許可されます。この役割により、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。サービス役割は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 管理者はこの役割の権限を変更できます。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 ユーザーおよびロールには、 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 AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限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。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

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

トピック

- ポリシーに関する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 AWS Health API へのアクセス
- リソースおよびアクションに基づく条件

ポリシーに関するベストプラクティス

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

- AWS 管理ポリシーを開始し、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の付与を開始するには、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することで、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な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 を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

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。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (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 管理ポリシー 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

JSON

```
{
    "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、 が組織内の他のアカウントのイベントを表示 AWS Health 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 AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

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

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

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

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、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のアカウントでのみ使用できます。詳細については、「サポート」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 AWS Health API へのアクセス許可を付与できます。

デフォルトでは、IAM ユーザーは AWS Health Dashboard または AWS Health API にアクセスできません。IAM ポリシーを単一のユーザー、ユーザーのグループ、またはロールに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、「ID (ユーザー、グループ、ロール)」と「IAM ポリシーの概要」を参照してください。

IAM ユーザーを作成したら、こ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 IDs、EC2 インスタンス IP アドレス、一般的なセキュリティ通知などの AWS リソース IDsが含まれますが、これらに限定されません。
> たとえば、IAM ポリシーが AWS Health Dashboard および AWS Health API にのみアクセスを許可する場合、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 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。

API の 2 つのグループを使用できます APIs AWS Health。

- 個々のアカウント – DescribeEvents や DescribeEventDetails などのオペレーションを使用して、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 および DescribeEventDetailsForOrganization などのオペレーションを使用して、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` エレメントを `health:Describe*` に設定できます。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。 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 AWS Health 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 および任意の `Describe*` AWS Health API オペレーションへのアクセスを許可します。たとえば、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 `DescribeEvents` API オペレーションを AWS Management Console AWS Health 呼び出すことができます。

Example : アクセスの説明

JSON

```
{
  "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 AWS Health API へのアクセスを拒否します。このポリシーを持つ IAM ユーザーは、 AWS Health Dashboard で を表示できず AWS Management Console 、 AWS Health API オペレーションを呼び出すこともできません。

Example : アクセスを拒否する

JSON

```
{
  "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 APIs、IAM ユーザーガイドのAWS Health APIs で定義されるアクションと通知」を参照してください。

> **Note**
>
> API にアクセスするには、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 Health APIs AWS Organizations。詳細については、「アカウント間の AWS Health イベントの集約」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

JSON

```
{
    "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

JSON

```
{
    "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 DescribeEventDetails API オペレーションの IAM 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、 AWS Health API がユーザー、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。

これを行うには、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 DescribeEventDetails API 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 DescribeEventDetailsForOrganization API 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、「サービス認可リファレンス」のAWS Health APIs と通知のアクション、リソース、および条件キー」を参照してください。

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 EC2 に関連する AWS Health イベントへのアクセスを拒否します。

JSON

```
{
    "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。

JSON

```
{
  "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 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、 に一致する を持つ AWS Health イベントへのアクセスを拒否`eventTypeCode`します`AWS_EC2_*`。

JSON

```
{
    "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て、 AWS Health イベントへの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 IAM 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。

トピック

- でアクションを実行する権限がありません AWS Health
- iam: PassRole を実行する権限がない
- 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ありません AWS Health

で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、ユーザーが 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を持ってい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。

AWS Health API には、 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 サポート。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のないアカウントから AWS Health API を呼び出すと、次のエラーコードが返されます。SubscriptionRequiredException

iam: PassRole を実行する権限がない

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して 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 のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに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。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して AWS Healthでアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。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。サインイン資格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後は、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、 への永続的なアクセス権をユーザーに付与できます 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、IAM ユーザーに新規アクセスキーを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。手順を表示するには、IAM ユーザーガイドの「アクセスキーの管理」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

他のユーザーにアクセスを許可するには 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。 AWS IAM Identity Center を使用して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ている IAM ロールに自動的に IAM ポリシーを作成して割り当てます。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。

IAM アイデンティティセンターを使用していない場合は、アクセスを必要としている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 AWSにアクセスします。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 アイデンティティ」と「IAM のポリシーとアクセス許可」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 (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- 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が IAM と AWS Health 連携する方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」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、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 のサービス 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。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

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 のサービス ます。このロールにアタッチされているのは、 `Health_OrganizationsServiceRolePolicy` AWS 管理ポリシーです。
- 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ているのは、 `AWSHealth_EventProcessorServiceRolePolicy` AWS 管理ポリシーです。サービスプリンシパルは、 ロールを使用して、 AWS Incident Detection and Response 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 にアラーム状態変更情報を配信 AWS アカウント 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、 はアカウントでこのサービスにリンクされたロール AWS Health 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、「IAM ユーザーガイド」の「サービスリンクロールの作成」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、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

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、IAM API、または AWS Command Line Interface () 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、 AWS サポート に連絡して、AWS Incident Detection and Response からワークロードをオフボードするように依頼します。この処理の完了後、IAM コンソール、IAM API、または AWS CLIを使用してロールを削除できます。

関連情報

詳細については、IAM ユーザーガイドの「サービスリンクロールの使用」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、ロールに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。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可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 マネージド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) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

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 マネージドポリシー: Health_OrganizationsServiceRolePolicy
- AWS 管理ポリシー: AWSHealthFullAccess
- AWS HealthAWS 管理ポリシーの更新

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、 AWS Health が AWS Incident Detection and Response の Amazon EventBridge ルールにアクセスすることを許可する次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説明および更新します。

JSON

```
{
    "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、 が Health Organizational ビューに必要な AWS Organizations 詳細にアクセス AWS Health できるようにす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 のサービス 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。

JSON

```
{
    "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 管理ポリシー: 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` – 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 AWS Health し、管理アカウントの組織単位 (OU) を表示します。

- `health` – AWS Health API オペレーションと通知へのアクセス
- `iam` – AWS Health サービスにリンクした IAM ロールを作成します

JSON

```
{
    "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 AWS Health してからの の AWS 管理ポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、のドキュメント履歴 AWS Health ページの RSS フィードを購読してください。

次の表は、2022 年 1 月 13 日以降の 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 管理ポリシー: AWSHealthFullAccess – 既存ポリシーへの更新	AWS Health は、AWSHealthFullAccess 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_OrganizationsServiceRolePolicy – 既存ポリシーへの更新	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 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。	2023 年 7 月 19 日

変更	説明	日付
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、 およびその他の AWS Health AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS には、監視 AWS Health、問題発生時の報告、および必要に応じてアクションを実行するための以下のモニタリングツールが用意されています。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、CloudWatch で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動することができます。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。
- Amazon EventBridge は、 AWS リソースの変更を記述するシステムイベントのnear-real-timeストリームを提供します。EventBridge は、自動化されたイベント駆動型のコンピューティングを可能にします。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記述できます。詳細については、「Amazon EventBridge AWS Health を使用した でのイベントのモニタリング」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信します。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

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 のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、AWS のサービス 「コンプライアンスプログラムによる対象範囲内」を参照して、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 「 Compliance ProgramsAssurance」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、「Downloading Reports in AWS Artifact」を参照してください。

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

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、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の機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA AWS のサービス の対象となるわけではありません。
- 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。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST) AWS のサービス 、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスにマッピングするためのベストプラクティスをまとめたものです。
- 「 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、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、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 – 不審な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モニタリングすることで AWS アカウント、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。

- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 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、および高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。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それらにアクセスできます。 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手順で保護されています。

AWS が公開した API コールを使用して、ネットワーク AWS Health 経由で にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

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 お客様と当社のお客様との間の責任共有です。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。

ユーザーに AWS Health 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。たとえば、 AWS Identity and Access Management (IAM) ユーザーに へのアクセスを許可できます 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、更新する必要がある 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ことがあります。

詳細については、「AWS Health ダッシュボードの開始方法」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、ユーザーとチームは 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、GitHub の「AWS Health のツール」ページを参照してください。

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 Events がルールに一致するイベントを検出すると、通知を受け取り、アクションを実行できます。CloudWatch Events 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に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決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。このリージョンに CloudWatch Events を設定して、これらのイベントを確実に監視できます。

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

アカウント間の AWS Health イベントの集約

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。を使用する場合は AWS Organizations、組織全体で AWS Health イベント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、特定の AWS リージョン、アカウント、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、更新やコード変更が必要になる可能性のある AWS サービスに対する今後の変更を常に把握できます。

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 組織内のアカウントに対して送信されたイベントは、1 つ以上のアカウントが組織を離れていても、イベントが使用可能である限り、最大 90 日間組織ビューに表示されます。
> - 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 ロールを引き受けます。

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

- 組織ビューの有効化
- 組織ビューを表示する
- 組織ビューの無効化
- 組織の委任管理者ビューを管理する

組織ビューの有効化

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できます。

組織ビューは、すべての AWS サポート プランで追加料金なしで AWS Health コンソールで利用できます。

> **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。

Enabling organizational view (Console)

AWS Health コンソールから組織ビューを有効にできます。 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. AWS Health ダッシュボードを https://health.aws.amazon.com/health/home で開きます。
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) AWS 組織単位 (OUs) の作成など、組織に変更を加える場合は、 の管理 AWS Organizations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**
>
> - AWS Health 組織ビューを有効にすると、最初のアカウントロードプロセスがバックグラウンドで実行され、完了までに数分かかる場合があります。プロセスが終了するのを待つ必要がないため、 AWS Health コンソールを閉じて後で戻ることができます。履歴ヘルスイベント (この機能を有効にする前に作成されたイベント) が組織ビューに表示されるまでに最大 24 時間かかる場合があります。
> - 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 管理ポリシーを持つ`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。

Enabling organizational view (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、Business、Enterprise On-Ramp、または Enterprise Support 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、 AWS SDK for バージョン Java 2.0 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 管理ポリシーを持つ`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。

組織ビューを表示する

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できます。

組織ビューは、すべての AWS サポート プランで追加料金なしで AWS Health コンソールで利用できます。

> **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。

Viewing organizational view events (Console)

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

アカウントが組織に参加すると、 はアカウント AWS Health を自動的に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、アカウントのポリシーデータを保持します。90 日間の終了時に、 はアカウントのすべてのポリシーデータ AWS 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。

- がポリシーデータ AWS を保持する限り、閉鎖されたアカウントを再開すると、 はアカウントをサービス管理者として AWS 再割り当てし、アカウントのサービスポリシーデータを復旧します。
- 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) リージョンのお客様向け：
>
> - 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 Dashboard – Service Health から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 ダッシュボードからのイベント – サービスのヘルスは、 AWS サービスのリージョンでの可用性に関する公開情報を提供します。

次のページで組織ビューイベントを表示できます。

未解決の問題と最近の問題

Open and recent issues タブを使用して、組織に影響を与える やリソースの変更 AWS のサービス など、 AWS インフラストラクチャに影響を与え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 Dashboard 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

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。

[Event Log]

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 Dashboard を開きます。
2. ナビゲーションペインの [組織の状態] で、[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

Viewing affected accounts and resources (Console)

[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 Dashboard 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。

Viewing organizational view events (CLI)

この機能を有効にすると、 は組織内のアカウントに影響するイベントの記録 AWS Health 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 は、組織ビューを有効にする前に組織で発生したイベントを記録しません。

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、アカウントのポリシーデータを保持します。90 日間の終了時に、 はアカウントのすべてのポリシーデータ AWS 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。
- がポリシーデータ AWS を保持する限り、閉鎖されたアカウントを再開すると、 はアカウントをサービス管理者として AWS 再割り当てし、アカウントのサービスポリシーデータを復旧します。
- 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) リージョンのお客様向け：
>
> - 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
```

組織ビューの無効化

組織のイベントを集約しない場合は、この機能を管理アカウントから無効にするか、DisableHealthServiceAccessForOrganization API オペレーションを使用して組織ビューを無効にすることができます。

Disabling organizational view events (Console)

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 Dashboard 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、 は組織からのイベントを集約 AWS Health 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 () を使用して削除するまで管理アカウントに残りますAWS CLI。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。

Disabling organizational view events (CLI)

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すと、 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 AWS Health 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、 は error. AWS Health continues を AWS Health 返し、 AWS アカウントのヘルスイベントを集約します。

この機能を無効にすると、 は組織からのイベントを集約 AWS Health 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 を使用して削除するまで管理アカウントに残ります AWS CLI。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。

組織の委任管理者ビューを管理する

を使用すると AWS Health、 の委任管理者機能を活用して、管理アカウント以外のアカウントが AWS Health Dashboard で集約 AWS Health イベントを表示したり、 AWS Health API を介してプログラムでイベントを表示 AWS Organizations したりできます。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。セキュリティの AWS ベストプラクティスとして、可能な場合は管理アカウント外に責任を委任します。

目次

- 組織ビューに委任管理者を登録する
- 組織ビューから委任管理者を削除する

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、アカウントは委任された管理アカウントになり、 AWS Health Dashboard から AWS Health 組織ビューにアクセスできます。アカウントに Business、Enterprise On-Ramp、または Enterprise Support プランがある場合、委任管理者は AWS Health API を使用して AWS Health 組織ビューにアクセスできます。

委任された管理者を確立するには、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。次のコマンド例では、ACCOUNT_ID を AWS Health サービスプリンシパル「health.amazonaws.com」とともに登録する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 EventBridge AWS Health を使用した でのイベントのモニタリング

Amazon EventBridge を使用して、 AWS Health イベントを検出して対応できます。そうすると、作成されたルールに基づいて、イベントがルールで指定されている値に一致するときに、EventBridge が 1 つ、または複数のターゲットアクションを呼び出します。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。イベントが常に EventBridge に配信されるとは限りません。
> - 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。
> - EventBridge ルールを作成した後、パブリックヘルスイベントの送信が開始されるまでに最大 1 時間かかる場合があります。

AWS Health ワークフローの一部として、EventBridge の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 EventBridge 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、GitHub のAWS Health ツールを参照してください。

トピック

- AWS リージョン カバレッジの EventBridge ルールの作成
- AWS Healthのアカウント固有イベントとパブリックイベントをモニタリングする
- EventBridge での AWS Health イベントのページ分割リストの表示
- 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 イベントモニタリングと通知を JIRA および ServiceNow と統合する
- のイベントに関する通知を送信するように EventBridge ルールを設定する AWS Health
- のイベントに関する通知を送信するようにチャットアプリケーションで Amazon Q Developer を設定する AWS Health
- のイベントに応じて EC2 インスタンスでオペレーションを自動的に実行する AWS Health
- リファレンス： AWS Health イベント Amazon EventBridge スキーマ

AWS リージョン カバレッジの EventBridge ルールの作成

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。

たとえば、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、 AWS Health 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、のイベントに関する通知を送信するように EventBridge ルールを設定する 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。

AWS Healthのアカウント固有イベントとパブリックイベントをモニタリングする

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、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 Dashboard — 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 メッセージで一貫性が保たれるためです。

eventScopeCode パラメーターを使用することにより EventBridge でイベントが公開なのかアカウント固有なのかを識別できます。イベントには `PUBLIC` または `ACCOUNT_SPECIFIC` のパラメータがあります。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"

    }
}
```

EventBridge での AWS Health イベントのページ分割リストの表示

AWS Health は、 `resources`または のリスト`affectedEntities`によってメッセージのサイズが EventBridge の 256KB 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。

AWS Health には、メッセージ内のすべての フィールド`resources`と `detail.affectedEntities`フィールドが含まれます。この `resources`と `detail.affectedEntities`の値のリストが 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別のメッセージとして EventBridge に発行します。すべてのページが受信された後に `resources` または `detail.affectedEntities` のリストを再度組み合わせることができるよう、各ページでは同じ `eventARN` と `communicationId` の値が保持されます。

このような追加のメッセージは、例えば EventBridge ルールが電子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送信された場合など、不要なメッセージを生成する可能性があります。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。

スキーマでは、各 communicationId にページが 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。フィールド`detail.page`とは、 AWS Health イベントの現在のページ番号と合計ページ数を`detail.totalPages`記述します。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` のリスト以外、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 EventBridge で公開された AWS Health イベントの組織ビューと委任管理者アクセスをサポートします。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。管理アカウントに組織ビューと EventBridge ルールを設定しても、組織内の他のアカウントの EventBridge ルールは無効になりません。

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、AWS Health 「イベントの集約」を参照してください。

AWS Health イベントモニタリングと通知を JIRA および ServiceNow と統合する

AWS Health イベントを JIRA および ServiceNow と統合して、サービス管理コネクタ (SMC) を使用して、運用情報とアカウント情報を受信し、スケジュールされた変更に備え、ヘルスイベントを管理できます。との SMC 統合では、EventBridge を介して送信されたヘルスイベントを使用して、JIRA チケットと ServiceNow インシデントを自動的に作成、マッピング、更新 AWS Health できます。

組織ビューと委任管理者アクセスを使用して、JIRA および ServiceNow 内の組織全体のヘルスイベントを簡単に管理し、 AWS Health の情報をチームのワークフローに直接組み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、ServiceNow AWS Health での統合」を参照してください。

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

のイベントに関する通知を送信するように EventBridge ルールを設定する AWS Health

EventBridge ルールを作成して、アカウントの AWS Health イベントの通知を受け取ることができます。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。

- EventBridge のイベント、ルール、ターゲットに精通しておいてください。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge とは」および「新しい EventBridge – AWS リソース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. Amazon EventBridge コンソールの https://console.aws.amazon.com/events/ を開いてください。
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。

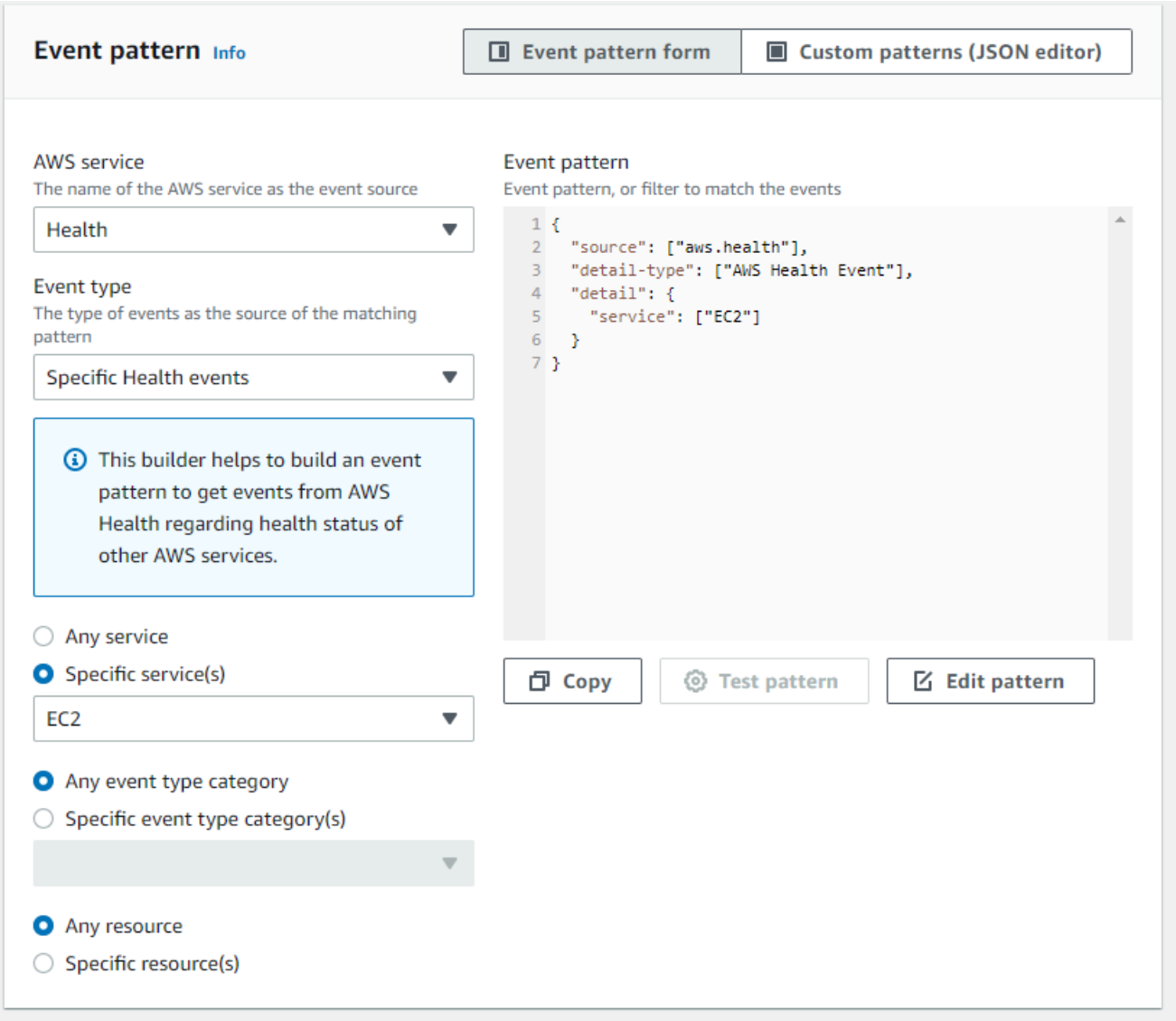
3. ナビゲーションペインで [ルール] を選択します。
4. [Create rule] (ルールを作成) を選択します。
5. [Define rule detail] (ルールの詳細を定義) ページで、ルールの名前と説明を入力します。
6. [Event bus] (イベントバス) と [Rule type] (ルールタイプ) のデフォルト値を維持して、[Next] (次へ) を選択します。
7. イベントパターンを構築 ページの イベントソース で、AWS イベントまたは EventBridge パートナーイベント を選択します。
8. [イベントパターン] で、[イベントソース] に [AWS のサービス] を選択します。
9. イベントパターン の [AWS のサービス] 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 のサービス、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] を選択します。
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、EventBridge の aws.health ソースから送信されません。
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. [ルールを作成] を選択します。

Example : すべての Amazon EC2 イベントに対するルール

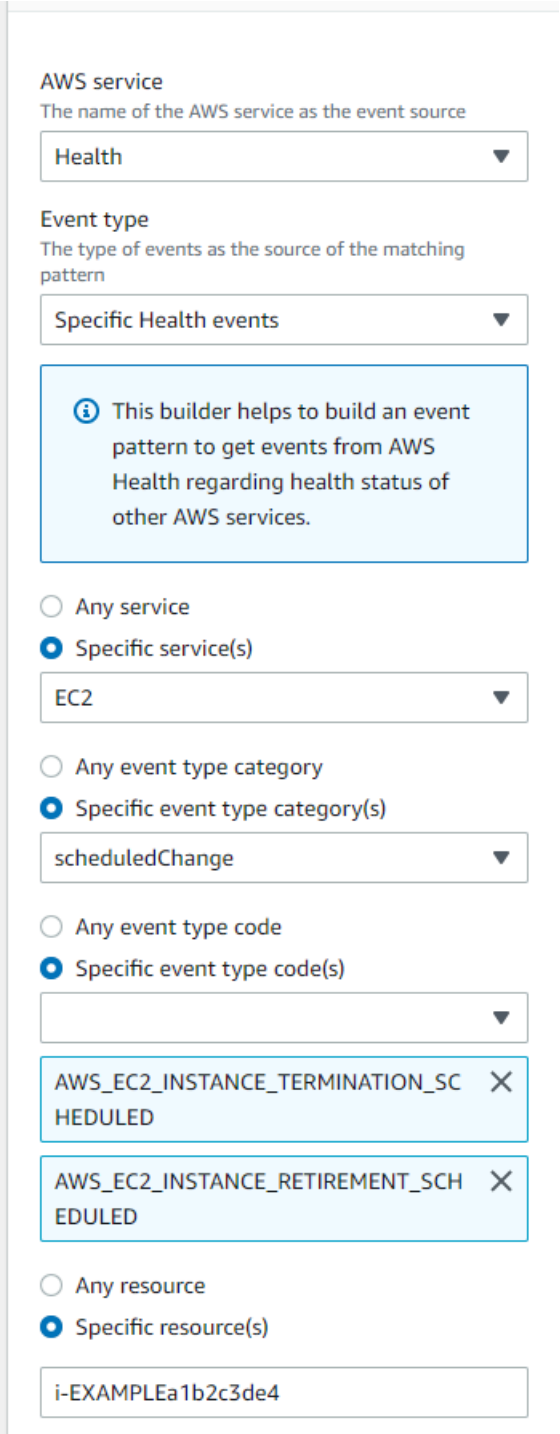
以下の例は、イベントタイプのカテゴリ、イベントコード、およびリソースなど、EventBridge がすべての Amazon EC2 イベントを管理するためのルールを作成します。



Example : 特定の Amazon EC2 イベントに対するルール

以下の例は、EventBridge が以下を監視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 [Rules] (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. 「のイベントに関する通知を送信するように EventBridge ルールを設定する 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、「のイベントに関する通知を送信するように EventBridge ルールを設定する 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、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。 AWS CLI コマンドの例については、「 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

```
{
```

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

のイベントに関する通知を送信するようにチャットアプリケーションで Amazon Q Developer を設定する AWS Health

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。たとえば、 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場合があります。

前提条件

開始する前に、以下のものが必要です。

- チャットアプリケーションで Amazon Q Developer で設定されたチャットクライアント。Amazon Chime と Slack を設定できます。詳細については、「Amazon Q Developer in chat applications 管理者ガイド」の「Getting started with Amazon Q Developer in chat applications」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。

チャットアプリケーションで Amazon Q Developer で AWS Health イベントを受信するには

1. 「のイベントに関する通知を送信するように EventBridge ルールを設定する 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。「EventBridge での AWS Health イベントのページ分割リストの表示」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。この同じ SNS トピックは、チャットアプリケーションコンソールの Amazon Q Developer で使用します。

   c. 残りの手順を完了して、ルールを作成します。

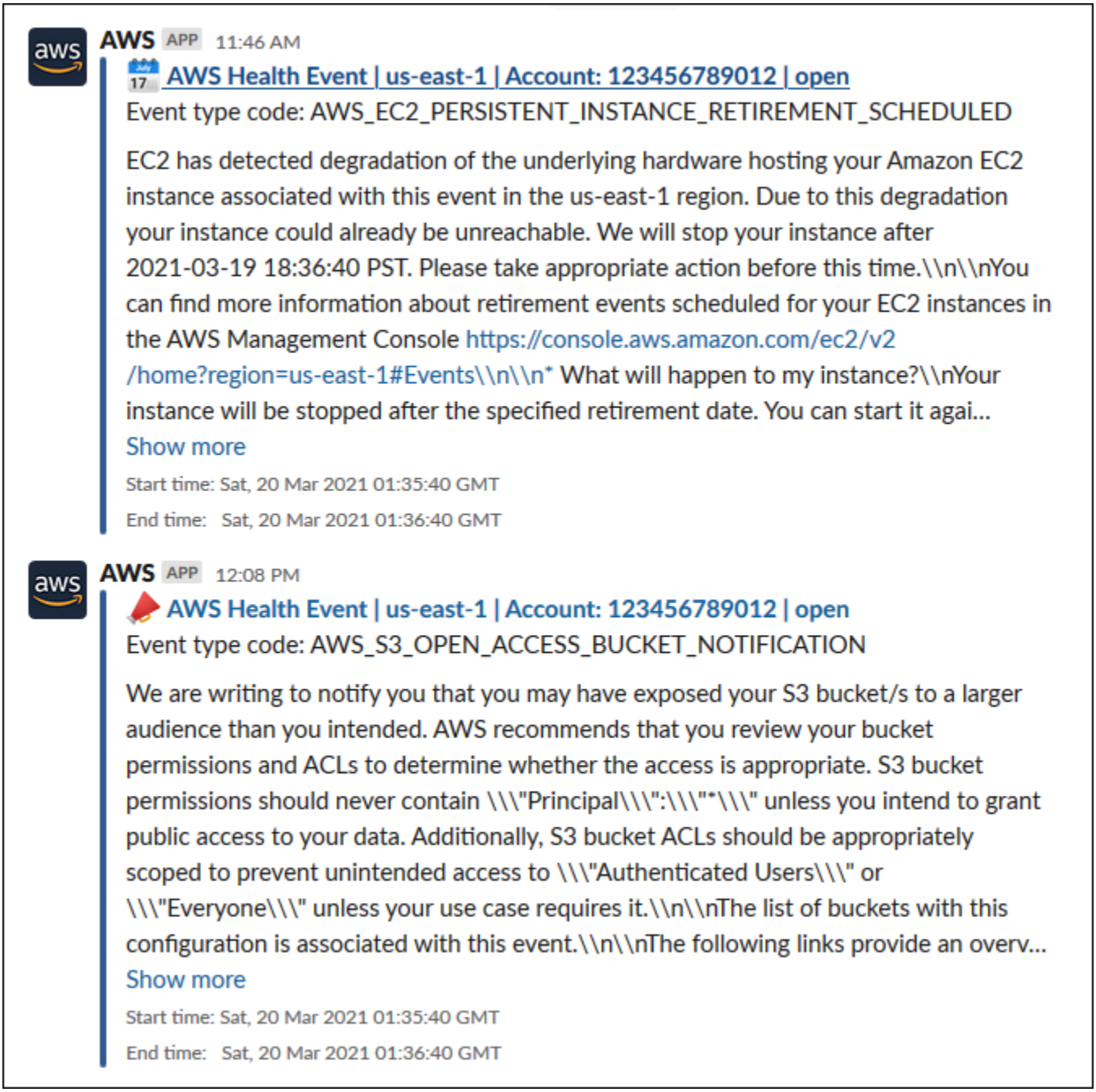
2. チャットアプリケーションコンソールで Amazon Q Developer に移動します。
3. Slack チャネル名など、チャットクライアントを選択し、[Edit] (編集) を選択します。
4. [Notifications - optional] (通知 – オプション) セクションの [Topics] (トピック) で、ステップ 1 で指定したものと同じ SNS トピックを選択します。
5. [保存] を選択します。

   がルールに一致するイベントを EventBridge 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。



のイベントに応じて EC2 インスタンスでオペレーションを自動的に実行する AWS Health

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 AWS アカウントにイベント AWS Health を送信すると、EventBridge ルールは AWS Systems Manager 自動化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「EventBridge で Amazon EC2 を自動化する」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 を選択してください。
3. [Create policy] (ポリシーを作成) 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。

   JSON

```
{
```

```
  "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. [Next: Tags] (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. [Review policy] (ポリシーの確認) ページで、*`AutomationEVRolePolicy`* などの [Name] (名前) と、オプションの [Description] (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. [Next: Permissions] (次のステップ: 許可) を選択します。
6. 作成したポリシー名 (*`AutomationEVRolePolicy`* など) を入力してから、その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。この手順を完了して、EventBridge コンソールでこのロールを選択できるように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 Roles (ロール) を選択してください。
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。

   JSON

```
{
    "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。

EventBridge のルールを作成する

EventBridge コンソールでこの手順を実行してルールを作成し、使用停止がスケジュールされている 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 自動アクションのための EventBridge のルールを作成する

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) 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。

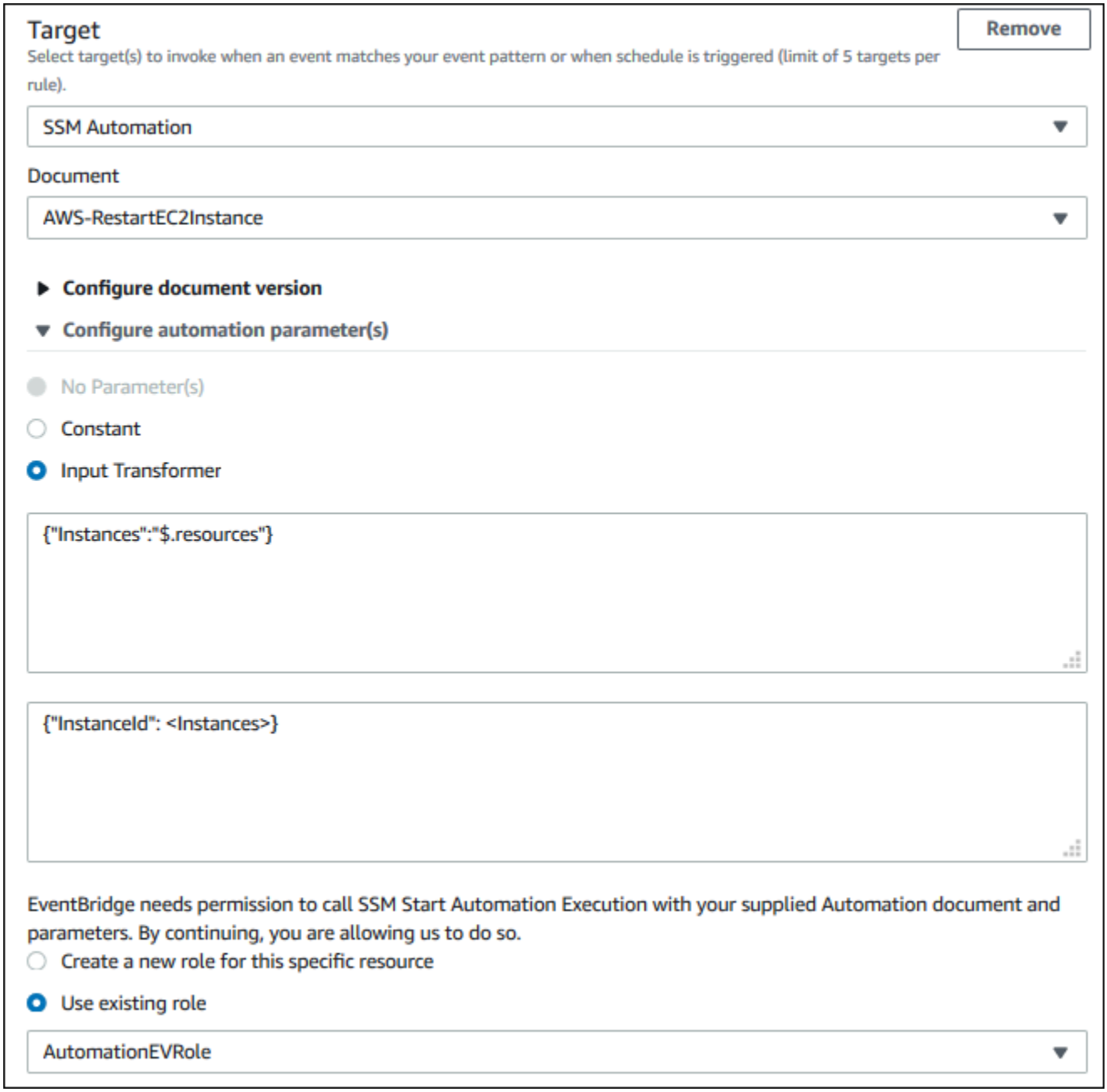
    [Event pattern] (イベントパターン) は以下の例のようになります。

    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. [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内で発生すると、EventBridge が指定されたターゲットにイベントを送信します。

リファレンス： AWS Health イベント Amazon EventBridge スキーマ

以下は、 AWS Health イベントのスキーマです。detail パラメータの内容については、2 番目のテーブルを参照してください。サンプルペイロードは、スキーマテーブルの後に記載されています。

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
version	EventBridge バージョン、現在は「0」。	はい
id	EventBridge イベントの一意の識別子。	はい
detail-type	detail のタイプ。 AWS Health イベントの場合、サポートされている値は &AWS Health Eventおよび です。 AWS Health	はい

パラメータ	説明	必須
	`Abuse Event`	
source	イベントバスソース。AWS Health イベントの場合、サポートされている値は です。`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アカウント ID。 Note 組織ビューでは、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、これは影響を受けるアカウントとは別の	はい

パラメータ	説明	必須
	アカウントです。	
time	通知が EventBridge に送信された時刻。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 。 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。この情報は detail.e entRegio に表	はい

パラメータ	説明	必須
	示されます。	
resources	アカウント内の影響を受けるリソース (存在する場合) のリストを示します。 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です。	いいえ
detail	この直後の表で説明されているように、AWS Health イベントの詳細を含む セクション。	はい

「detail」パラメータのスキーマ内容

次の表は、 AWS Health イベントスキーマの詳細パラメータの内容を示しています。

AWS Health イベントスキーマ: パラメータコンテンツの詳細

「detail」パラメータの内容	説明	必須
eventArn	リージョンと AWS Health イベント ID を含む、特定のリー	はい

「detail」パラメータの内容	説明	必須
	ジョンのイベントの一意の識別子。 Note イベント ARN は、特定の AWS アカウントまたはリージョンに固有ではありません。	
service	AWS Health イベントの AWS のサービス 影響を受ける 。例えば、Amazon EC2、Amazon Simple Storage Service、Amazon Redshift、Amazon Relational Database Service。	はい

「detail」パラメータの内容	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、開始時間の約 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トにはすべてイベントタイプ`AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT` があります。	はい
eventTypeCategory	イベントのカテゴリコード サポートされている値は、`issue`、`accountNotification` 、`investigation` 、`scheduledChange` です。	はい

「detail」パラメータの内容	説明	必須
eventScopeCode	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。サポートされている値は `ACCOUNT_SPECIFIC` または `PUBLIC` です。	はい
communicationId	AWS Health イベントのこの通信の一意の識別子。 同じ通信 ID 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場合があります。この識別子をアカウント ID 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。 AWS Health イベントページ分割のサポートにより、通信 ID には、12345678910-1 など、ページ間で通信 ID を一意に保つためのページ番号が含まれます。詳細については、「EventBridge での AWS Health イベントのページ分割リストの表示」を参照してください。	はい
startTime	形式の AWS Health イベントの開始時刻`DoW, DD, MMM, YYYY, HH:MM:SS TZ`。 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

「detail」パラメータの内容	説明	必須
endTime	AWS Health イベントの終了時刻。形式は ですDoW, DD MMM YYYY HH:MM:SS TZ。 将来の時刻にスケジュールされたイベントに終了時間を指定することはできません。	いいえ
lastUpdatedTime	AWS Health 形式のイベントの最終更新時刻DoW, DD MMM YYYY HH:MM:SS TZ。	はい
statusCode	AWS Health イベントのステータス。 サポートされている値は、open、closed、upcoming です。	はい
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

「detail」パラメータの内容	説明	必須
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。 • language – AWS Health イベントで使用される言語のコード。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。例えば、`us-east-1` リージョンでは、これは通常 en_US です。 • 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ません。	はい

「detail」パラメータの内容	説明	必須
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。 • <メタデータキー 1> – メタデータキーと値のペア文字列：「keystring1」:「keyvalue1」 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
affectedEntities	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。 • entityValue – リソース/エンティティ ID。 • lastUpdatedtime – 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 (`DoW, DD MMM YYYY HH:MM:SS TZ` の形式)。 • status – 影響を受けたリソース/エンティティのステータス。サポートされている値は、`IMPAIRED`、`UNIMPAIRED` 、`PENDING`、`RESOLVED`、`U` です。	いいえ

「detail」パラメータの内容	説明	必須
page	このメッセージが表すページ。詳細については、「EventBridge での AWS Health イベントのページ分割リストの表示」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。別の理由で 256KB のサイズ制限を超えた場合、通信は失敗します。	はい
totalPages	このヘルスイベントのページの総数。詳細については、「EventBridge での AWS Health イベントのページ分割リストの表示」を参照してください。 これの値を使用して、1 つのアカウントに関する複数ページにわたる通信のすべてのページを受信したかどうかを判断できます。	はい

「detail」パラメータの内容	説明	必須
affectedAccount	影響を受けるアカウントのアカウント ID です。 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管理者アカウントで受信された場合、 `account` フィールドの値とは異なることがあります。	はい

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"
    }
}
```

モニタリング AWS Health

モニタリングは、 およびその他の AWS Health AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS には、監視 AWS Health、問題発生時の報告、および必要に応じてアクションを実行するための以下のモニタリングツールが用意されています。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。詳細については、『Amazon CloudWatch ユーザーガイド』を参照してください。

  Amazon EventBridge を使用すると、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 EventBridge AWS Health を使用した でのイベントのモニタリング」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

トピック

- を使用した AWS Health API コールのログ記録 AWS CloudTrail

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

AWS Health は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS Health。CloudTrail は、 AWS Health の API コールをイベントとしてキャプチャします。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 AWS Health API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、イベントを含む Amazon S3 バケットへの CloudTrail 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。CloudTrail によって収集された情報を使

用して、リクエストの実行元の IP アドレス AWS Health、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

設定や有効化の方法など、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 CloudTrail の情報

CloudTrail は、 AWS アカウントの作成時に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イベント履歴の他の AWS サービスイベントとともに CloudTrail 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、CloudTrail イベント履歴での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さらに分析して処理するように、他の AWS サービスを設定できます。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 がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成
- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS Health API オペレーションは CloudTrail によってログに記録され、 AWS Health API リファレンスに記載されています。たとえば `DescribeEvents`、`DescribeEventDetails`、および `DescribeAffectedEntities` の各オペレーションへのコールは、CloudTrail ログファイル内にエントリを生成します。

AWS Health は、CloudTrail ログファイルのイベントとして次のアクションのログ記録をサポートします。

- リクエストが、ルートと IAM 認証情報のどちらを使用して送信されたか

- リクエストが、ロールとフェデレー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 Amazon S3 のサーバー側の暗号化 (SSE) を使用して、ログファイルが暗号化されます。

ログファイルの配信時に通知を受け取りたい場合は、新しいログファイルの配信時に Amazon SNS 通知が発行されるように CloudTrail を設定できます。詳細については、「CloudTrail用のAmazon SNS通知の設定」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と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

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、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の情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出し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。

DescribeEntityAggregates オペレーションを示す CloudTrail ログエントリの例を次に示します。

```
{
   "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、こ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

次の表に、2020 年 8 月 28 日以降の AWS Health ドキュメントの重要な更新を示します。RSS フィードにサブスクライブすると、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
更新されたセクション: Amazon EventBridge AWS Health を使用した でのイベントのモニタリング	トピック「Installing a service-linked role to use AWS Incident Detection and Response in Monitoring events in AWS Health with Amazon EventBridge」を削除しました。	2025 年 8 月 8 日
更新されたセクション: Amazon EventBridge AWS Health を使用した でのイベントのモニタリング	「Notes」セクションに、Public Health Events の通知の受信を開始するまでに最大 1 時間の遅延が発生する可能性があることを示す情報を追加しました。詳細については、「Amazon EventBridge AWS Health を使用した でのイベントのモニタリング」を参照してください。	2025 年 7 月 22 日
更新されたセクション: 組織ビューの有効化	組織ビューを有効にすると、が組織全体の過去のすべてのヘルスイベント AWS Health を自動的に集計することを示す情報をメモセクションに追加しました。履歴イベントが組織ビューに表示されるま	2025 年 6 月 27 日

	でに最大 24 時間かかる場合があります。詳細については、「組織ビューの有効化」を参照してください。	
更新されたセクション: アカウント間の AWS Health イベントの集約	組織ビューを有効にする前に発生したイベントが表示され AWS Health ないことに注意してください。詳細については、「アカウント間の AWS Health イベントの集約」を参照してください。	2025 年 6 月 27 日
WorkDocs が廃止されました	計画されたライフサイクルイベントで廃止された WorkDocs への参照を削除しました。 AWS Health	2025 年 6 月 19 日
AWS マネージド通知の移行タイムラインに関する注意事項を追加	の AWS マネージド通知への E メール移行の主な日付に関するメモを追加しました AWS User Notifications。詳細については、「 で AWS Health 通知を管理する AWS User Notifications」を参照してください。	2025 年 4 月 28 日

計画されたライフサイクルイベントの更新	計画されたライフサイクルイベントを更新し、未解決のリソースの AWS Health イベントが 90 日ではなく 4 年間開いたままであることを示します。詳細については、「Planned Lifecycle events for」の「What should I expect when I receive a planned Lifecycle event notification?」セクションを参照してください。 AWS Health	2025 年 4 月 18 日
計画されたライフサイクルイベントの影響を受けるリソースリストの説明を更新しました	計画されたライフサイクルイベントの影響を受けるリソースリストは、通常 24 時間に 1 回更新されますが、現在のリソースステータスを反映するまでに最大 72 時間かかる場合があります。詳細については、AWS Health 「ダッシュボードでのアカウントイベントの表示」の「イベントの詳細」セクションを参照してください。	2025 年 4 月 7 日
で AWS Health 通知を管理するためのよくある質問を追加しました AWS User Notifications	詳細については、「よくある質問」の「通知の管理 AWS User Notifications」を参照してください。	2025 年 2 月 18 日
エンドポイントへの IPv6-only リクエストに関する情報を追加しました。	詳細については、AWS Health 「API リクエストのエンドポイントの選択」を参照してください。	2025 年 1月 28 日

で AWS Health 通知を管理する AWS User Notifications	詳細については、「 で通知を管理する AWS User Notifications」を参照してください。	2025 年 1 月 16 日
Amazon EventBridge による AWS Health イベントのモニタリングで JSON を修正	詳細については、「Amazon EventBridge による AWS Health イベントのモニタリング」を参照してください。	2024 年 9 月 3 日
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	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	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 ダッシュボードを更新 – AWS Health ドキュメントのサービスのヘルスと計画されたライフサイクルイベントを更新しました。	詳細については、「AWS Health ダッシュボード – サービスのヘルス」と「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。	2024 年 2 月 15 日
「 AWS Healthの EventBridge ルールの作成」の重複する箇条書きを削除	EventBridge ルールの作成 AWS Health」の重複する箇条書きを削除しました。	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 ポリシー更新	AWS 管理ポリシーの更新: 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 EventBridge による AWS Health イベントのモニタリング」を参照してください。	2023 年 6 月 20 日

Amazon EventBridge 関するドキュメントを更新しました	Amazon EventBridge ルールを使用して、アカウント固有のイベントと公開イベントの両方を監視できるようになりました。詳細については「Amazon EventBridge による AWS Health イベントのモニタリング」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 UTC で AWS Health Dashboard を表示します。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」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	Aware AWS Health の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 EventBridge 関するドキュメントを更新しました	Amazon EventBridge を使用してヘルスイベントをモニタリング AWS Health するためのの新しいトピック。詳細については「Amazon EventBridge による AWS Health イベントのモニタリング」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、AWS Health API を使用できます。	2021 年 11 月 24 日
ドキュメントを追加	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

CloudWatch Events のドキュメントの更新	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
CloudWatch Events のドキュメントの更新	Amazon CloudWatch Events ルールの AWS Systems Manager アクションを自動化するために 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
CloudWatch Events のドキュメントの更新	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、「チャットアプリケーションで Amazon Q Developer と AWS Health イベントを受信する」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 を使用した AWS Health イベントのモニタリングに関する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、アクティブなリージョンエンドポイントと署名 AWS リージョンを決定できます AWS Health。	2020 年 10 月 22 日
AWS Health ユーザーガイドの更新	Organization は 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。	「アカウント間の AWS Health イベントの集約」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。	「アカウント間の AWS Health イベントの集約」を参照してください。	2019 年 12 月 18 日
AWS Health API 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「リソースとアクションベースの条件」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。	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

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。