



ユーザーガイド

AWS Health



AWS Health: ユーザーガイド

Copyright © 2024 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 での イベント EventBridge	6
AWS Health API	7
組織ビュー	7
概要	8
設定	8
にサインアップする AWS アカウント	8
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	10
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 の設定 EventBridge	20
AWS Health ダッシュボード	22
の計画されたライフサイクルイベント AWS Health	25
計画的ライフサイクルイベントとは？	25

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?	26
レジリエンス維持のための責任分担モデル	28
計画されたライフサイクルイベントへのアクセス	29
の AWS ユーザー通知の設定 AWS Health	30
を使用した他のシステムとの統合 AWS Health API	31
リクエストの AWS Health API エンドポイントの選択	31
AWS Health エンドポイントデモを試す	33
Java デモを試す	33
Python デモを試す	36
リクエストの署名 AWS Health API	39
Java で AWS Health API を使用する例を学ぶ	40
ステップ 1: 認証情報を初期化する	40
ステップ 2: クライアントを AWS Health API 初期化する	40
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	40
セキュリティ	44
データ保護	45
データ暗号化	46
アイデンティティ/アクセス管理	46
対象者	47
アイデンティティを使用した認証	47
ポリシーを使用したアクセスの管理	51
と AWS Health の仕組み IAM	53
アイデンティティベースポリシーの例	59
トラブルシューティング	72
サービスリンクロールの使用	75
AWS の マネージドポリシー AWS Health	76
でのログ記録とモニタリング AWS Health	82
コンプライアンス検証	83
耐障害性	84
インフラストラクチャセキュリティ	84
設定と脆弱性の分析	85
セキュリティに関するベストプラクティス	85
AWS Health ユーザーに最小限のアクセス許可を付与する	85
を表示する AWS Health Dashboard	85
Amazon Chime または Slack AWS Health との統合	86
AWS Health イベントのモニタリング	86

AWS Health イベントの集約	87
前提条件	87
組織ビューの有効化	88
組織ビューの表示	92
組織ビューの無効化	97
委任管理者の組織ビュー	98
組織ビューに委任管理者を登録する	99
組織ビューから委任管理者を削除する	99
を使用したヘルスイベントのモニタリング EventBridge	100
AWS リージョン カバレッジの EventBridge ルールの作成	101
のアカウント固有イベントとパブリックイベントのモニタリング AWS Health	102
AWS Incident Detection and Response を使用するためのサービスにリンクされたロールのインストール	103
関連情報	104
AWS Health イベント Amazon EventBridge スキーマ	104
AWS Health イベントスキーマ	104
公衆衛生イベント - Amazon EC2の運用上の問題	132
アカウント固有の AWS Health イベント - Elastic Load Balancing API の問題	133
アカウント固有の AWS Health イベント - Amazon EC2 Instance Store Drive Performance Degraded	134
での AWS Health イベントのページ分割 EventBridge	135
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	136
AWS Health イベントモニタリングと通知を JIRAおよび と統合する ServiceNow	136
イベントに関する通知を送信する EventBridge ルールの設定	137
複数のサービスおよびカテゴリに対するルールの作成	141
イベントに関する通知を送信する AWS Chatbot ように を設定する	143
前提条件	143
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	145
前提条件	146
のルールを作成する EventBridge	150
モニタリング AWS Health	154
を使用した通話のログ記録 AWS Health API AWS CloudTrail	154
AWS Health の情報 CloudTrail	155
例：AWS Health ログファイルエントリ	156
ドキュメント履歴	158
以前の更新	164

..... clxv

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知ることができます 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適時 AWS Health に提供します。AWS Health 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、トラブルシューティングを加速するためのイベント可視性とガイダンスがほぼ瞬時に得られます。

すべてのお客様は、 を搭載した [AWS Health Dashboard](#) を使用できます AWS Health API。ダッシュボードはセットアップが不要で、[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」](#)の「」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基本 AWS Health と用語については、AWS Health 「」を参照してくださいの[概念 AWS Health](#)。

メモ

- AWS Health Dashboard は、追加料金なしですべての AWS お客様にご利用いただけます。
- すべての AWS お客様は、追加料金なしで Amazon EventBridge 経由で AWS Health イベントを受け取ることができます。
- Business、Enterprise On-Ramp、または Enterprise Support プランがある場合は、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、「[AWS Health APIリファレンス](#)」を参照してください。
- 利用可能な AWS Support プランの詳細については、「」を参照してください[AWS Support](#)。

の概念 AWS Health

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

トピック

- [AWS Health イベント](#)
- [AWS Health 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 での イベント EventBridge](#)
- [AWS Health API](#)
- [組織ビュー](#)

AWS Health イベント

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

Health イベントには 2 つのタイプがあります。

目次

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

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

パブリックイベント

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

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

アカウントをお持ちの場合は、「[AWS Health ダッシュボードの開始方法](#)」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問題など、一般的な認識を提供するイベントについて確認することをお勧めします。AWS Health Dashboard を使用して、アカウントの非推奨リソースなど、ユーザーに直接影響する可能性のあるイベントについて確認することもできます。

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

詳細については、「[AWS Health ダッシュボードの開始方法](#)」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ことをお勧めします。各カテゴリは、異なるタイプのイベントに対して表示されます。[DescribeEventType](#) API オペレーションを使用して、イベントタイプのカテゴリを検索することもできます。

アカウント通知

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

アカウント通知のイベントタイプのコードの例を次に示します。

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

問題

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

次に、問題に関するイベントタイプのコードの例を示します。

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

予定された変更

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

次に、予定された変更に関するイベントタイプのコードの例を示します。

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

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

Tip

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

イベントステータス

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

影響を受けるエンティティ

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

AWS Health Amazon での イベント EventBridge

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

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

AWS Health API

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

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

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

Note

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

組織ビュー

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

をお持ちでない場合は AWS アカウント、[AWS Health ダッシュボード](#) を使用して一般的なサービスの可用性を確認できます。

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ついてより深く理解することをお勧めします。

トピック

- [AWS アカウントの設定](#)
- [AWS Health Dashboard でアカウントイベントを表示する](#)
- [Amazon の設定 EventBridge](#)

AWS アカウントの設定

を有効にする前に AWS Health、が必要で 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/サインアップ> 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、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

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。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用して [ルートユーザーアクセスが必要なタスク](#) を実行してください。

AWS は、サインアッププロセスが完了した後に確認 E メールを送信します。/ に移動し、マイアカウント を選択して、いつでも現在のアカウントアクティビティを表示 <https://aws.amazon.com> し、アカウントを管理できます。

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、 のセキュリティを確保し AWS アカウントのルートユーザー、 を有効にし AWS IAM Identity Center、管理ユーザーを作成して、日常的なタスクにルートユーザーを使用しないようにします。

のセキュリティ保護 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、[「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 デバイスの有効化](#)」を参照してください。IAM

管理アクセスを持つユーザーを作成する

1. IAM Identity Center 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 Identity Center で、ユーザーに管理アクセスを許可します。

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 を使用するため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 Identity Center ユーザーでサインインするには、IAM Identity Center ユーザーの作成時に E メールアドレスに URL 送信されたサインインを使用します。

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 「アクセスポータルへのサインイン」](#)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 Identity Center で、最小権限のアクセス許可を適用するベストプラクティスに従う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「[グループの参加](#)」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. <https://health.aws.amazon.com/health/ホーム> で AWS Health Dashboard を開きます。

2. ナビゲーションペインの [アカウントの状態] で、次のオプションを選択できます。
 - a. [\[未解決の課題と最近の問題\]](#) — 最近開いたイベントと終了したイベントを表示します。
 - b. [\[予定されている変更\]](#) — サービスやリソースに影響する可能性のある、今後予定されているイベントを表示します。
 - c. [\[その他の通知\]](#) — アカウントに影響する可能性のある、過去 7 日間のその他の通知や進行中のイベントをすべて表示します。
 - d. [\[イベントログ\]](#) — 過去 90 日間のすべてのイベントを表示します。

未解決の問題と最近の問題

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

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

表示されたイベントは、タブを問わず、フィルタリストからオプションを選択してフィルタリングできます。例えば、アベイラビリティゾーン、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) の運用上の問題イベント

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

Your account health

Stay informed of important events affecting your AWS resources.

Configure EventBridge

Get notifications for events that might affect your services and resources.

[Go to EventBridge](#) ↗

Open and recent issues (16) | **Scheduled changes (0)** | **Notifications (3)** | **Event log**

Open and recent issues (16)

View events that might affect your AWS infrastructure. **35 issues** were resolved in the past 24 hours.

Service: Elastic Compute Cloud ✕

Clear filter

< 1 >

Event summary

Operational issue - EC2 (Ohio)
 Last update: February 20, 2022 at 11:16:34 PM UTC-8
 us-east-2

Operational issue - EC2 (Ohio)
 Last update: February 17, 2022 at 11:56:09 PM UTC-8
 us-east-2

Operational issue - EC2 (N. Virginia)
 Last update: February 16, 2022 at 1:36:29 AM UTC-8
 us-east-1

Operational issue - EC2 (Ohio) [Back to list view](#) □

Details

Affected resources

Event data

<p>Service EC2</p> <p>Status Open</p> <p>Region / Availability Zone us-east-1</p> <p>Account specific No</p>	<p>Start time February 20, 2022 at 11:16:24 PM UTC-8</p> <p>End time -</p> <p>Category Issue</p> <p>Affected resources 1</p>
--	--

Description

[04:35 AM PST] We are investigating increased EC2 launch failures and networking connectivity issues for some instances in a single Availability Zone (USE1-AZ4) in the US-EAST-1 Region. Other Availability Zones within the US-EAST-1 Region are not affected by this issue.

予定された変更

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

その他の通知

[通知] タブでは、アカウントに影響を及ぼす可能性のある、過去 7 日間のその他の通知や進行中のイベントをすべて確認できます。これには、証明書のローテーション、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。

Event log

Q Add filter

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) X Clear filter

Event	Status	Event category	Region / Zone	Start time	Last update time	Affected resources
Lambda operational issue	Closed	Issue	us-east-1	October 9, 2020 at 2:03:48 AM UTC-7	October 9, 2020 at 3:11:09 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	October 9, 2020 at 1:48:51 AM UTC-7	October 9, 2020 at 11:54:16 AM UTC-7	-
SNS operational issue	Closed	Issue	us-east-1	September 30, 2020 at 8:28:18 AM UTC-7	September 30, 2020 at 11:42:54 AM UTC-7	-
EC2 operational issue	Closed	Issue	us-east-1	September 16, 2020 at 7:30:41 AM UTC-7	September 16, 2020 at 7:45:03 AM UTC-7	-
Storagegateway operational issue	Closed	Issue	us-east-1	September 13, 2020 at 12:46:47 PM UTC-7	September 13, 2020 at 6:32:24 PM UTC-7	-
Deepracer operational issue	Closed	Issue	us-east-1	August 31, 2020 at 6:32:39 PM UTC-7	August 31, 2020 at 9:10:12 PM UTC-7	-

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 リソースに関する以下の情報が表示されます。

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

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

Example の : AWS Health event AWS Lambda

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

The screenshot displays the AWS Health console interface. On the left, the 'Event log' section shows a search filter for 'Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2)' and a list of operational issues. The 'Lambda operational issue' is highlighted. On the right, the 'Lambda operational issue' details are shown, including event data and a description.

Event log

Search:

Region: US East N. Virginia (us-east-1), US East Ohio (us-east-2) ✕

Clear filter

1

Event summary

- Lambda operational issue**
Last update: October 9, 2020 at 3:11:09 AM UTC-7 us-east-1
- EC2 operational issue**
Last update: October 9, 2020 at 11:54:16 AM UTC-7 us-east-1
- SNS operational issue**
Last update: September 30, 2020 at 11:42:54 AM UTC-7 us-east-1
- EC2 operational issue**
Last update: September 16, 2020 at 7:45:03 AM UTC-7 us-east-1
- Storagegateway operational issue**
Last update: September 13, 2020 at 6:32:24 PM UTC-7 us-east-1
- Deepracer operational issue**
Last update: August 31, 2020 at 9:10:12 PM UTC-7 us-east-1
- Sagemaker operational issue**
Last update: August 31, 2020 at 9:04:39 PM UTC-7 us-east-1
- Batch operational issue**

Lambda operational issue Back to list view

Details | Affected resources

Event data

Event	Start time
Lambda operational issue	October 9, 2020 at 2:03:48 AM UTC-7
Status	End time
Closed	October 9, 2020 at 3:11:08 AM UTC-7
Region / Availability Zone	Affected resources
us-east-1	-
Category	
Issue	

Description

[RESOLVED] Increased Invoke Error Rate

[02:03 AM PDT] We have identified an increase in invoke error rates in the US-EAST-1 Region and are working towards resolution.

[03:11 AM PDT] Between October 8 10:35 PM and October 9 2:25 AM PDT we experienced increased Lambda invoke error rates in the US-EAST-1 Region. The issue has been resolved and the service is operating normally.

イベントタイプ

AWS Health イベントには 2 つのタイプがあります。

- パブリックイベントは、アカウント固有ではないサービスイベントです。例えば、EC2で Amazon に問題がある場合 AWS リージョン、は、そのリージョンでサービスやリソースを使用しなくても、イベントに関する情報 AWS Health を提供します。
- アカウント固有のイベントは、アカウントまたは組織内のアカウントに固有です。例えば、使用するリージョンの Amazon EC2 インスタンスに問題がある場合、はイベントと影響を受ける 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。
- eventScopeCode パラメータを返すには、AWS Health API を使用します。イベントには PUBLIC、ACCOUNT_SPECIFIC、または NONE の値を指定できます。詳細については、AWS Health API リファレンスの「[DescribeEventDetails](#) オペレーション」を参照してください。

カレンダービュー

カレンダービューは、スケジュールされた変更タブで使用でき、AWS Health イベントを月次のカレンダーに投影できます。このビューでは、過去 3 か月前までと今後 1 年の予定されている変更を確認できます。

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

Scheduled changes

Table Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

Any event ▼

< **February 2024** >

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
28	29 2 Upcoming	30 2 Upcoming 1 Completed	31	1	2

30 January 2024
⚙️ ×

Scheduled events starting on 30 January 2024 (Showing 3 of 3) [View all on the table view](#)

[EKS planned lifecycle event \(us-west-2\)](#)
Event status: **Upcoming**

[EKS planned lifecycle event \(us-east-1\)](#)
Event status: **Upcoming**

[EKS planned lifecycle event \(eu-west-1\)](#)
Event status: **Completed**

影響を受けるリソースビュー

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

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

組織ビューにアクセスすると、AWS Health イベントには、含まれているすべてのアカウントの影響を受けるすべてのリソースのステータスの概要が表示されます。概要が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になった後。アカウント番号または保留中のリソースの数を選択すると、アカウントビューの概要が表示されます。アカウントビューの概要には、影響を受けるアカウントの組織リストに戻るためのパンくずリストがあります。影響を受けるリソースステータスの概要は、分割パネルの上部に表示されます。

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

一度にダウンロードできるファイルは 1 つだけです。ファイルは自動的にブラウザのデフォルトのダウンロードフォルダにダウンロードされ、イベントタイトル AWS リージョン、イベント開始日、およびダウンロード日に基づいて事前設定されたファイル名が付けられます。

Open and recent issues (0)
Scheduled changes (1)
Other notifications (0)
Event log

Scheduled changes (1)

Table

Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities. [View scheduled changes that occurred more than 7 days ago.](#)

< 1 >

Event	Status	Region / Zone <small>Info</small>	Start time	End time	Affected resources									
<div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 20%;"> <h2 style="margin: 0;">4</h2> <p style="margin: 0;">Affected resources</p> <p style="font-size: 10px; margin: 0;">Resource data is typically refreshed every 24 hours.</p> </div> <div style="width: 40%;"> <ul style="list-style-type: none"> <li style="margin-bottom: 5px;"> 4 Pending <small>May require action</small> <li style="margin-bottom: 5px;"> 0 Unknown <small>Not able to verify status</small> <li style="margin-bottom: 5px;"> 0 Resolved <small>No actions required</small> </div> <div style="width: 20%; text-align: right;"> <p>100%</p> <p>0%</p> <p>0%</p> </div> </div>														
<h3>Affected resources (4)</h3> <div style="float: right; border: 1px solid #0070C0; padding: 2px 5px; border-radius: 3px;">Download ▾</div> <div style="border: 1px solid #0070C0; padding: 2px; margin-bottom: 5px;"> <input type="text" value="Add filter"/> </div> <div style="text-align: right; margin-bottom: 5px;"> < 1 > </div> <table border="1" style="width: 100%; border-collapse: collapse; text-align: left;"> <thead> <tr> <th style="width: 60%;">Resource ID / ARN</th> <th style="width: 20%;">Resource status</th> <th style="width: 20%;">Last update time</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUJ6P</td> <td style="text-align: center; padding: 5px;">⏸ Pending</td> <td style="text-align: right; padding: 5px;">3 months ago</td> </tr> <tr> <td style="padding: 5px;">arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy</td> <td style="text-align: center; padding: 5px;">⏸ Pending</td> <td style="text-align: right; padding: 5px;">3 months ago</td> </tr> </tbody> </table>						Resource ID / ARN	Resource status	Last update time	arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUJ6P	⏸ Pending	3 months ago	arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy	⏸ Pending	3 months ago
Resource ID / ARN	Resource status	Last update time												
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-AutoUpdateLambda-atNXDvDUJ6P	⏸ Pending	3 months ago												
arn:aws:lambda:us-east-1:959586608611:function:SpringClean-XUG3HH5R-FeatureCheckerFunction-cwZkcPWUtAGy	⏸ Pending	3 months ago												

タイムゾーン設定

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




組織のヘルス

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



詳細については、「[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。

Enable organizational view

Key benefits

 Organization-wide visibility Aggregate your Health events from all member AWS accounts in your AWS organization. This provides a centralized view for all events, such as operational issues, scheduled maintenance, and account notifications.	 API access If you have a Business or Enterprise Support plan, you can integrate with the AWS Health API to programmatically use organizational view and look up details for events that occur in your organization. Learn more	 Chat integration Using the AWS Health API, you can ingest events into your Amazon Chime or Slack channel to get notified when an event occurs. Filter events to get the ones that matter most to your organization. Learn more
--	---	---

Get started

1. Set up AWS Organizations You must have an AWS organization with all features enabled.  Success Manage AWS Organizations  View documentation	2. Enable organizational view for AWS Health After you set up AWS Organizations and sign in to the management account, you can enable AWS Health to aggregate all events. These events appear in the Personal Health Dashboard. Enable organizational view View documentation
--	--

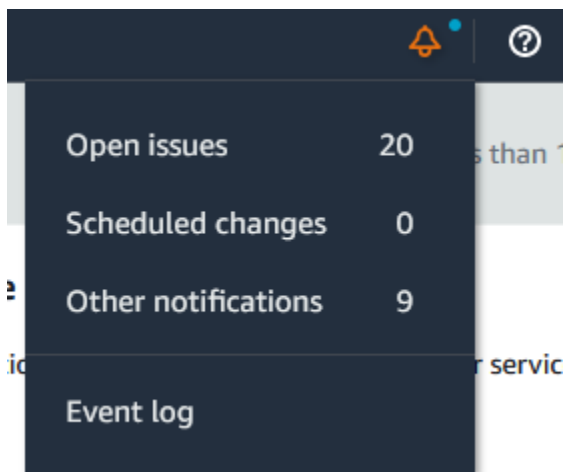
AWS Health イベントのアラート

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、Amazon Relational Database Service (Amazon RDS)、AWS Identity and Access Management (IAM) EC2、などの複数の AWS コンソールに表示されます AWS Trusted Advisor。

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

Example : 未解決のイベント

以下の画像は、アカウントの未解決のイベントと通知イベントを示しています。



Amazon の設定 EventBridge

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。

EventBridge で使用する AWS Health

1. <https://health.aws.amazon.com/health/ホーム> で AWS Health Dashboard を開きます。
2. EventBridge コンソールに移動してルールを作成するには、次のいずれかを実行します。
 - ナビゲーションペインの Health Integrations で、Amazon EventBridgeを選択します。
 - の設定で EventBridge、「に移動 EventBridge」を選択します。

3. この手順に従って、ルールを作成しイベントを監視します。「[Amazon AWS Health を使用したでのイベントのモニタリング EventBridge](#)」を参照してください。

AWS Health ダッシュボード

AWS Health Dashboard – Service Health を使用して、すべての 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。アカウントをすでにお持ちの場合は、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 – サービスのヘルスを表示するには

1. <https://health.aws.amazon.com/health/ステータス> 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
 - イベントの重要度 ([情報]や[低下]など)
 - イベントの最新更新のタイムライン
 - このイベントによって AWS のサービス も影響を受ける のリスト


Note

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

- (オプション) イベントの横にある、このイベントのRSSフィードをサブスクライブRSSすることを選択します。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。
- [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。

- 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。
- (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。イベント列の任意のイベントを選択すると、ポップアップサイドパネルにその特定のイベントに関する詳細情報が表示されます。

Service history

[List of services](#)[List of events](#)

The following table is a running log of AWS service interruptions for the past 12 months. Choose a status icon to see status updates for that service. All dates and times are reported in Pacific Standard Time (PST). To update your time zone, see [Time zone settings](#).

Note

2023年9月以降にパブリックイベントを選択すると、ブラウザURLの にそのパブリック AWS Health イベントへのリンクが入力されます。このリンクを選択したら、そのイベントポップアップ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RSSすることを選択します。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) イベントは、ローカルタイムゾーンまたは で表示できますUTC。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。

の計画されたライフサイクルイベント AWS Health

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

トピック

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

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

Note

この基準を満たすすべての通知は、計画されたライフサイクルイベント AWS Health として を通じて報告されます。

- 動的リソースのバーンダウンとメタデータの改善: AWS Health イベントの存続期間を通じて通知を受信してから、影響を受けるリソースは、特定のエンティティステータスを持つ影響を受ける工

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

Note

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

計画ライフサイクルイベントの通知を受け取ったら、何を予期すべきですか？

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

タイプカテゴリ: 予定されている変更

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

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

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

Note

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

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

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

Note

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

Open and recent issues
Scheduled changes
Other notifications
Event log

Table
Calendar

View upcoming events and ongoing events from the past seven days that might affect your AWS infrastructure, such as scheduled maintenance activities.

< 1 >

Event	Status	Region / Zone	Start time	End time	Affected resources
EKS planned lifecycle event	Upcoming	us-west-2	January 30, 2024 at 6:00:00 PM UTC-8		9 pending
DMS planned lifecycle event	Upcoming	us-east-1	January 29, 2024 at 6:00:00 PM UTC-8		1 pending
DMS planned lifecycle event	Upcoming	eu-west-1	January 29, 2024 at 6:00:00 PM UTC-8		10 pending
EKS planned lifecycle event	Completed	eu-west-1	January 30, 2024 at 6:00:00 PM UTC-8		-

EKS planned lifecycle event ⚙️ ×

Resource data is typically refreshed every 24 hours. 0 Resolved 0%
No actions required

Affected resources in account 745485236264 (5)

< 1 >

Resource ID / ARN	Resource status	Last update time
arn:aws:eks:us-west-2:745485236264:cluster/prod-ops-cluster	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/nonprod-dev5	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/n-preprd-eks	⏸ Pending	15 days ago
arn:aws:eks:us-west-2:745485236264:cluster/argoworkflows-refactor51	⏸ Pending	15 days ago
arn:aws:eks:us-west-1:745485236264:cluster/prod-refactor	⏸ Pending	15 days ago

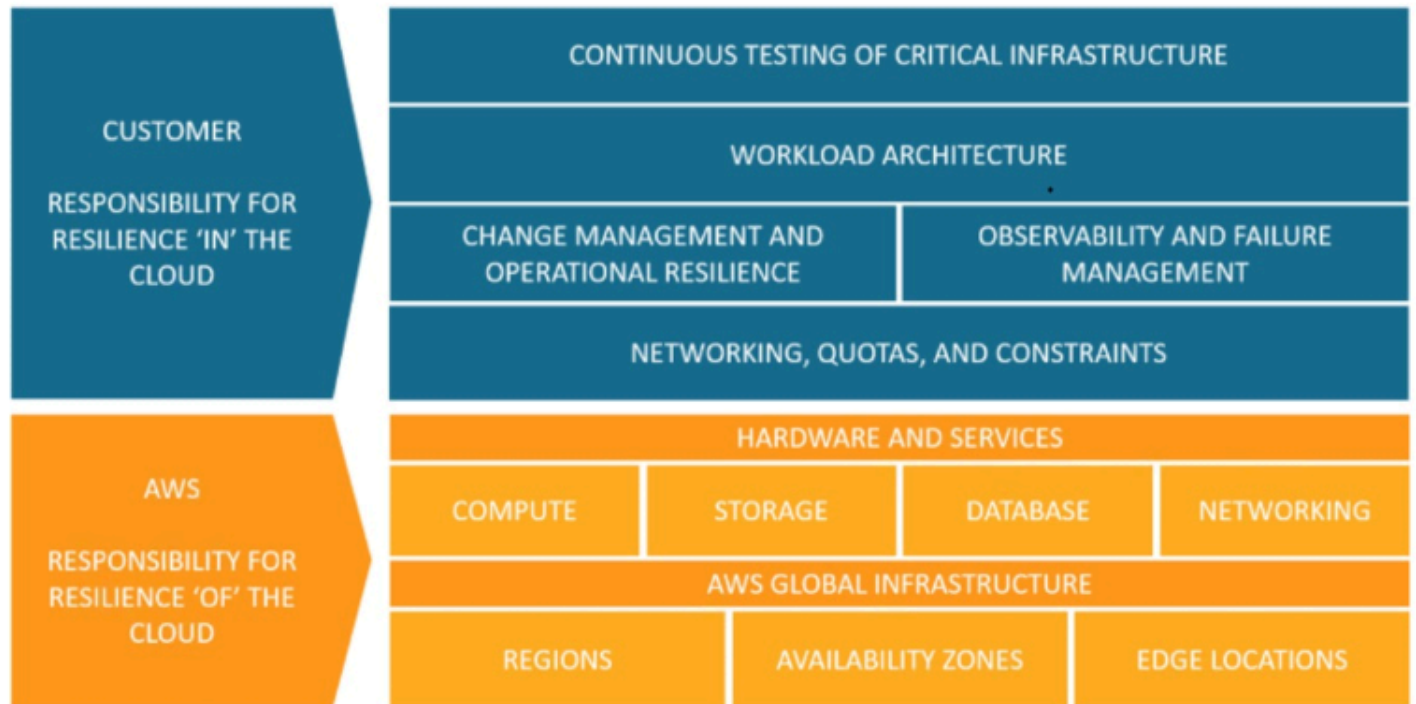
予定されているイベントの日付が過ぎると、

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

レジリエンス維持のための責任分担モデル

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

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



計画されたライフサイクルイベントへのアクセス

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

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

の AWS ユーザー通知の設定 AWS Health

AWS Health は、運用上の問題、計画されたメンテナンス、計画されたソフトウェアライフサイクルイベントなど、サービスオペレーションに関する情報を提供します。影響を受けるリソース、現在のステータス (オープンまたはクローズ) IDs、リソースステータスなど EventBridge、AWS Health イベントの詳細を包括的に可視化するには、Amazon の aws.health ソース AWS Health API、AWS Health ダッシュボードなどの AWS Health エンドポイントを使用することをお勧めします。これらのエンドポイントにより、ワークロードに影響する可能性のある進行中のイベントや変更に関する最も詳細でリアルタイムの情報が取得できます。

[AWS ユーザー通知](#)は、追加の UX チャンネル (AWS コンソールモバイルアプリケーションへの Eメール、チャット、プッシュ通知) を通じて通知します。AWS Health イベント通知には、上記のエンドポイントほど詳細なデータは含まれませんが、問題や変更を利害関係者に通知するシンプルで効果的な方法を提供します。作成したルールで指定した値とイベントが一致すると、ユーザー通知は作成したルールに基づいて通知を作成し、送信します。通知を送信する UX 配信チャンネルを選択し、集計を設定することにより特定のイベントに対して生成される通知の数を減らすことができます。通知は、コンソール通知センターで表示することもできます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど、更新がスケジュールされているリソースが AWS アカウントにあれば、チャット通知を受け取ることができます。

AWS ユーザー通知の設定の詳細については、[AWS 「ユーザー通知の開始方法」](#)を参照してください。

を使用した AWS Health 他のシステムとの統合 AWS Health API

AWS Health は、 をトランスポートHTTPSとして使用し、メッセージのシリアル化形式JSONとして使用するRESTfulウェブサービスです。アプリケーションコードは、AWS Health に直接リクエストを行うことができますAPI。REST API を直接使用する場合は、リクエストに署名して認証するために必要なコードを記述する必要があります。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 Support](#) 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 AWS Health API。Business、Enterprise On-Ramp、または Enterprise Support プランがない AWS アカウント AWS Health APIから を呼び出すと、SubscriptionRequiredExceptionエラーが発生します。

を使用して AWS SDKsAPI呼び出しを AWS Health REST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を処理し、署名をリクエストします。

AWS Health には、イベントと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 ダッシュボード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。

リクエストの AWS Health APIエンドポイントの選択


は AWS Health API、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DNSの検索を実行して、アクティブなエンドポイントと対応する署名 AWS リージョンを決定できます。これにより、コードで使用するエンドポイントを把握できるため、 から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、「[リクエストの署名 AWS Health API](#)」を参照してください。

次の表は、デフォルトの設定を示しています。

説明	署名リージョン	エンドポイント	プロトコル
[アクティブ]	us-east-1	health.us-east-1.a mazonaws.com	HTTPS
パッシブ	us-east-2	health.us-east-2.a mazonaws.com	HTTPS
グローバル	us-east-1	global.health.amaz onaws.com	HTTPS

 **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。

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でDNSルックアップを行いCNAME、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DNSの検索

次のコマンドは、global.health.amazonaws.com エンドポイントDNSの検索を完了します。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、に使用するエンドポイントを示します AWS Health。

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

i 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。

AWS Health エンドポイントデモを試す

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。アクティブなエンドポイントが変更されると、コードはワークフローを再開します。

トピック

- [Java デモを試す](#)
- [Python デモを試す](#)

Java デモを試す

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. 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 GitHub。
2. デモプロジェクトの `high-availability-endpoint/java` ディレクトリに移動します。
3. コマンドラインウィンドウで次のコマンドを入力します。

```
gradle build
```

4. 次のコマンドを入力して、AWS 認証情報を指定します。

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"  
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY"
```

```
export AWS_SESSION_TOKEN="your-aws-token"
```

5. 次のコマンドを入力してデモを実行します。

```
gradle run
```

Example : AWS Health イベント出力

コード例では、過去 7 日間の最近の AWS Health イベントを AWS アカウントで返します。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 Support [1]. Additional sample queries to retrieve the relationship information for the resources listed above is provided in [2].

[1] <https://aws.amazon.com/support>

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

Java リソース

- 詳細については、AWS SDK for Java API「リファレンス」の「[インターフェイス HealthClient](#)」と「[ソースコード](#)」を参照してください。
- このデモでDNSルックアップに使用するライブラリの詳細については、「」の「[dnsjava](#)」を参照してください GitHub。

Python デモを試す

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. 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 GitHub。
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のウェブサイトでの [venv - Creation of virtual environments](#) を参照してください。

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

4. 次のコマンドを入力して仮想環境をアクティブ化します。

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

5. 次のコマンドを入力して依存関係をインストールします。

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

6. 次のコマンドを入力して、AWS 認証情報を指定します。

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

7. 次のコマンドを入力してデモを実行します。

```
python3 main.py
```

Example : AWS Health イベント出力

コード例では、過去 7 日間の最近の AWS Health イベントを AWS アカウントで返します。次の出力は、AWS セキュリティ通知の AWS Health イベントを返します。

```
INFO:botocore.credentials:Found credentials in environment variables.  
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/  
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-  
a9a5-876544042721',  
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',  
'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':  
datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
```

```
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9, 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
(FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
an interruption in service, we encourage you to act now, by ensuring that you
connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
If you need further guidance or assistance, please contact AWS Support [2] or your
Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
with TLS
1.0/1.1?\n\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

- の詳細についてはHealth. Client、[AWS SDK 「 for Python \(Boto3\) APIリファレンス](#)」を参照してください。
- このデモでDNSルックアップに使用するライブラリの詳細については、の [dnspython](#) ツールキットと[ソースコード](#)を参照してください GitHub。

リクエストの署名 AWS Health API

または AWS Command Line Interface (AWS CLI) を使用して AWS SDKs 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、以前の高可用性エンドポイントデモ AWS SDK for Java に 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 を使用する AWS Health API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。

リクエストを行うときは、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。

または を使用しない AWS SDKs場合は AWS CLI、リクエストに自分で署名する必要があります。Signature AWS Version 4 を使用することをお勧めします。詳細については、[AWS API 「」の「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。

Java で AWS Health APIを使用する例を学ぶ

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

と通信するには、有効な認証情報が必要です AWS Health API。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](#) インスタンスの作成と初期化 :

```
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: クライアントを AWS Health API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.amazonaws.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、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

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

- クラウドのセキュリティ – クラウドで AWS 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。は、安全に使用できるサービス AWS も提供します。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。に適用されるコンプライアンスプログラムの詳細については AWS Health、「[コンプライアンスAWS プログラムによる対象範囲内のサービスコンプライアンス](#)」を参照してください。
- クラウドのセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます AWS Health。以下のトピックでは、セキュリティとコンプライアンスの目標を達成 AWS Health するため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と保護に役立つ他の 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](#)
- [での回復力 AWS Health](#)
- [AWS Health内のインフラストラクチャセキュリティ](#)
- [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](#)、のデータ保護に適用されます AWS Health。このモデルで説明されているように、AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS 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 FAQ](#)」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 「責任共有モデル」と GDPR](#) AWS 「セキュリティブログ」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 () を使用して個々のユーザーを設定することをお勧めします IAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1.2 が必要で TLS、1.3 TLS をお勧めします。
- を使用して 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。証 CloudTrail 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 「証跡の操作」](#) を参照してください。
- AWS 暗号化ソリューションと、内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合は API、FIPS エンドポイントを使用します。使用可能な FIPS エンドポイントの詳細については、「[連邦情報処理標準 \(FIPS\) 140-3](#)」を参照してください。

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

データ暗号化

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

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

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

保管中の暗号化

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

転送中の暗号化

送受信されるすべてのデータは、転送中に暗号化 AWS Health 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 AWS のサービス 使用できる です。

トピック

- [対象者](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [と AWS Health の仕組み IAM](#)
- [AWS Health ID ベースのポリシーの例](#)

- [AWS Health ID とアクセスのトラブルシューティング](#)
- [AWS Healthのサービスにリンクされたロールの使用](#)
- [AWS の マネージドポリシー AWS Health](#)

対象者

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

サービスユーザー – AWS Health サービスを使用してジョブを実行する場合、管理者は必要な認証情報とアクセス許可を提供します。より多くの AWS Health 機能を使用して作業を行う際には、追加のアクセス許可が必要になる場合があります。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、へのフルアクセスがある可能性があります 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できるかを判断するのは、お客様の仕事です。その後、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、の基本概念を理解しますIAM。で使用する方法の詳細については AWS Health、IAM 「」を参照してくださいと [AWS Health の仕組み IAM](#)。

IAM 管理者 – IAM管理者の場合は、へのアクセスを管理するためのポリシーの作成方法の詳細を知りたい場合があります AWS Health。で使用できる AWS Health アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してください [AWS Health ID 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、アイデンティティ認証情報 AWS を使用してにサインインする方法です。として、ユーザーとして、またはロールを引き受けることで認証 (にサインイン AWS) される必要があります。AWS アカウントのルートユーザー IAM IAM

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、フェデレーテッド ID の例です。フェデレーテッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用してにアクセスすると、間接的にロールを引き受けることになります。

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

AWS プログラムでにアクセスする場合、はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号化して署名します。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。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの「[リクエストの署名 AWS API](#)」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、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「[多要素認証の使用](#)」および「[ユーザーガイド](#)」の「[多要素認証の使用 \(MFA\) AWS](#)」を参照してください。IAM

AWS アカウントルートユーザー

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 ID 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してアクセスします。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM 「ユーザーガイド」の「[ルートユーザーの認証情報を必要とするタスク](#)」を参照してください。

IAM ユーザーとグループ

[IAM ユーザー](#)とは、1 人のユーザーまたはアプリケーションに対して特定のアクセス許可 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持つIAMユーザーを作成する代わりに、一時的な認証情報に依存することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、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ユーザーのコレクションを指定する ID です。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、

という名前のグループがありIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、IAM ユーザーガイドの [\(ロールではなく\) IAM ユーザーを作成するタイミング](#) 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。ユーザーと似ていますがIAM、特定の人物には関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、[でロールを一時的に引き受けることができます](#)。または オペレーションを AWS CLI AWS API呼び出すか、カスタム を使用してロールを引き受けることができますURL。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方法](#)」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、IAM ユーザーガイドの「[サードパーティー ID プロバイダーのロールの作成](#)」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証された後にアクセスできる内容を制御するために、IAM Identity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「[アクセス許可セット](#)」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、特定のタスクに対して異なるアクセス許可を一時的に引き受けるIAMロールを引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントの誰か (信頼できるプリンシパル) が自分のアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS 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のロールとリソースベースのポリシーの違いについては、IAM「ユーザーガイド」の「[のクロスアカウントリソースアクセスIAM](#)」を参照してください。
- クロスサービスアクセス – 他の の機能 AWS のサービス を使用するものもあります AWS のサービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実

行EC2したりAmazon S3にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して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と 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のリクエストを使用します。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権限が必要です。FAS リクエストを行う際のポリシーの詳細については、[「アクセスセッションの転送」](#)を参照してください。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける[IAMロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、IAM「ユーザーガイド」の[「にアクセス許可を委任するロールの作成 AWS のサービス」](#)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、サービスにリンクされたロールのアクセス許可を表示することはできますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、IAM「ユーザーガイド」の[IAM「ロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与する」](#)を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、IAM ユーザーガイドの[\(ユーザーではなく\) IAMロールを作成するタイミング](#)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には、ポリシー AWS を作成し、AWS アイデンティティ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 として保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「[ユーザーガイド](#)」の [JSON「ポリシーの概要」](#) を参照してください。IAM

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

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するには、IAM 管理者は IAM ポリシーを作成できます。その後、管理者は IAM ポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

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

アイデンティティベースのポリシー

ID ベースのポリシーは、IAM ユーザー、ユーザーのグループ、ロールなどの ID にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーを作成する方法については、「[ユーザーガイド](#)」の [IAM「ポリシーの作成」](#) を参照してください。IAM

アイデンティティベースのポリシーは、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。マネージドポリシーは、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を選択する方法については、IAM ユーザーガイドの [「マネージドポリシーとインラインポリシーの選択」](#) を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロール信頼ポリシーと Amazon S3 バケットポリシーがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、[プリンシパルを指定する](#)必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または `arn:aws:iam::aws:policy` 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IAMでは、`arn:aws:iam::aws:policy` から AWS 管理ポリシーを使用することはできません。

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

詳細については、「[リソース](#)」を参照してください。

アクセスコントロールリスト

アクセスコントロールリスト (ACLs) は、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アクセス許可を持っているかを制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式は使用されません。

Amazon S3、および Amazon VPCは AWS WAF、`arn:aws:iam::aws:policy` をサポートするサービスの例ですACLs。の詳細についてはACLs、「Amazon Simple Storage Service デベロッパーガイド」の「[アクセスコントロールリスト \(ACL\) 概要](#)」を参照してください。

AWS Health は `arn:aws:iam::aws:policy` をサポートしていませんACLs。

その他のポリシータイプ

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

- **アクセス許可の境界** – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できる最大アクセス許可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 (SCPs) をアカウントのいずれかまたはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します AWS アカウントのルートユーザー。Organizations との詳細については SCPs、AWS Organizations 「ユーザーガイド」の「[サービスコントロールポリシー](#)」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合があります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「ユーザーガイド」の「[セッションポリシー](#)」を参照してください。IAM

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が AWS を決定する方法については、「ユーザーガイド」の「[ポリシー評価ロジック](#)」を参照してください。IAM

と AWS Health の仕組み IAM

IAM を使用して へのアクセスを管理する前に AWS Health、 で使用できるIAM機能を理解しておく必要があります AWS Health。AWS Health およびその他の AWS のサービスが とどのように連携するかの概要についてはIAM、IAM ユーザーガイドの[AWS「と連携するのサービスIAM」](#)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 ID ベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。は、特定のアクション、リソース、および条件キー AWS Health をサポートします。JSON ポリシーで使用するすべての要素については、IAM ユーザーガイドの [IAMJSON 「ポリシー要素リファレンス」](#) を参照してください。

アクション

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

JSON ポリシーの Action 要素は、ポリシー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を記述します。ポリシーアクションは通常、関連付けられた AWS API オペレーションと同じ名前です。一致する API オペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

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

のポリシーアクションは、アクションの前に次のプレフィックス AWS Health を使用します: health:。例えば、[DescribeEventDetails](#) API オペレーションで指定されたイベントに関する詳細情報を表示するアクセス許可をユーザーに付与するには、health:DescribeEventDetails アクションをポリシーに含めます。

ポリシーステートメントには、Action または NotAction element 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

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

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[名前 \(ARN\) 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 リソース名前 (ARN) 形式があります。

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

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

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

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

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

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

一部の AWS Health アクションは、特定のリソースに対して実行できません。このような場合は、ワイルドカード * を使用する必要があります。

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

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

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

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

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

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

条件キー

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

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの [条件演算子](#) を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1つのステートメントに複数の Condition 要素を指定する場合、または1つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれら进行评估します。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 を评估します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

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

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

AWS Health は独自の条件キーのセットを定義し、一部のグローバル条件キーの使用もサポートします。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドの[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 ID 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 ID 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、どの条件下で実行できるかを指定するJSONポリシードキュメントです。は、ヘルスイベントのリソースベースのアクセス許可ポリシー AWS Health をサポートします。リソースベースのポリシーでは、リソースごとに他のアカウントに使用許可を付与することができます。リソースベースのポリシーを使用して、AWS サービスが AWS Health イベントにアクセスすることを許可することもできます。

クロスアカウントアクセスを有効にするには、リソース[ベースのポリシーのプリンシパル](#)として、別のアカウントのアカウントまたはIAMエンティティ全体を指定できます。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の違い」](#)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 は、リソースのタグ付けやタグに基づくアクセスの制御をサポートしていません。

AWS Health IAM ロール

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

での一時的な認証情報の使用 AWS Health

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

AWS Health は一時的な認証情報の使用をサポートしています。

サービスリンクロール

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

AWS Health は、 と統合するサービスにリンクされたロールをサポートします AWS Organizations。サービスにリンクされたロールは、 `AWSServiceRoleForHealth_Organizations` と呼ばれます。ロールにアタッチされているのは [Health_OrganizationsServiceRolePolicy](#) AWS managed ポリシーです。AWS マネージドポリシーでは AWS Health、 が組織内の他の AWS アカウントからヘルスイベントにアクセスできるようにします。

[EnableHealthServiceAccessForOrganization](#) オペレーションを使用して、アカウントにサービスにリンクされたロールを作成できます。ただし、この機能を無効にする場合は、まず [DisableHealthServiceAccessForOrganization](#) オペレーションを呼び出す必要があります。その後、IAM コンソール、API または AWS Command Line Interface () IAM から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。

サービスロール

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

AWS Health はサービスロールをサポートしていません。

AWS Health ID ベースのポリシーの例

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

これらのポリシードキュメント例を使用して IAM ID ベースの JSON 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

- [ポリシーのベストプラクティス](#)

- [AWS Health コンソールを使用する](#)
- [自分の権限の表示をユーザーに許可する](#)
- [AWS Health Dashboard と へのアクセス AWS Health API](#)
- [リソースおよびアクションに基づく条件](#)

ポリシーのベストプラクティス

ID ベースのポリシーは、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、最小権限のアクセス許可に移行 – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらはで利用できます 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「[管理AWS ポリシー](#)」または ジョブ機能の 管理ポリシーを参照してください。 [AWS](#)
- 最小権限のアクセス許可を適用する - IAMポリシーでアクセス許可を設定する場合、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、IAM 「ユーザーガイド」の「[のポリシーとアクセス許可IAM](#)」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。また、 などの特定の を通じて サービスアクションが使用されている場合 AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「ユーザーガイド」の[IAMJSON 「ポリシー要素: 条件」](#)を参照してください。 IAM
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的なレコメンデーションが用意されています。詳細については、IAM 「ユーザーガイド」の[IAM 「Access Analyzer ポリシーの検証」](#)を参照してください。

- 多要素認証が必要 (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、 をオンにMFA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MFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細については、IAM 「ユーザーガイド」の[MFA 「保護APIアクセスの設定」](#)を参照してください。

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

AWS Health コンソールを使用する

AWS Health コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、AWS アカウント内の AWS Health リソースの詳細を一覧表示および表示できます。最低限必要なアクセス許可よりも制限の厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (IAMユーザーまたはロール) に対してコンソールは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 AWS Health コンソールを引き続き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せん。

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

Example : AWSHealthFullAccess

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

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

Note

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

AWS CLI または のみ呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません AWS API。代わりに、実行しようとしているAPIオペレーションに一致するアクションのみへのアクセスを許可します。

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

自分の権限の表示をユーザーに許可する

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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 とへのアクセス AWS Health API

AWS Health Dashboard はすべての AWS アカウントで使用できます。AWS Health API は、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、「[AWS Support](#)」を参照してください。

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

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

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

Note

表示するアクセス許可を持つIAMユーザーは AWS Health Dashboard、アカウント上のすべての AWS サービスでヘルス情報に読み取り専用でアクセスできます。これには、Amazon EC2インスタンス、EC2インスタンス IP アドレスIDs、一般的なセキュリティ通知IDsなどの AWS リソースが含まれますが、これらに限定されません。

例えば、IAMポリシーが AWS Health Dashboard および AWS Health にのみアクセスを許可する場合API、ポリシーが適用されるユーザーまたはロールは、他のIAMポリシーがそのアクセスを許可していない場合でも、AWS サービスおよび関連リソースについて投稿されたすべての情報にアクセスできます。

APIs には の 2 つのグループを使用できます AWS Health。

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

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

個々のアクション

IAM ポリシーの Action要素を に設定することができますhealth:Describe*。これにより、AWS Health Dashboard および へのアクセスが許可されます AWS Health。 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 オペレーションへのアクセスを許可しますDescribe* AWS Health API。例えば、このポリシーを持つIAMユーザーは、AWS Health Dashboard の にアクセスして AWS Management Console DescribeEventsAPIオペレーションを AWS Health 呼び出すことができます。

Example : アクセスの説明

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

アクセスを拒否する

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

Example : アクセスを拒否する

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

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

組織ビュー

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

IAM ポリシーの Action 要素には、次のアクセス許可が含まれている必要があります。

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

各に必要な正確なアクセス許可を理解するにはAPIs、IAM ユーザーガイドの「[で AWS Health APIs 定義されるアクションと通知](#)」を参照してください。

Note

組織の管理アカウントの認証情報を使用して、AWS Health APIs のにアクセスする必要があります 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

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

AWS Health 組織ビューへのアクセス拒否

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

Example : AWS Health 組織ビューへのアクセスを拒否する

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

Note

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

リソースおよびアクションに基づく条件

AWS Health は、 [DescribeAffectedEntities](#) および [DescribeEventDetails](#) API オペレーション [IAMの条件](#) をサポートします。リソースおよびアクションベースの条件を使用して、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。

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

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

- eventTypeId
- 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、「サービス認証リファレンス」の [「およびの通知の AWS Health APIs アクション、リソース、および条件キー」](#) を参照してください。

Example : アクションベースの条件

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

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

Example : リソースベースの条件

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

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

```

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

```

Example : eventTypeCode condition

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_*。

```

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

```

Important

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

AWS Health ID とアクセスのトラブルシューティング

以下の情報を使用して、およびの使用時に発生する可能性のある一般的な問題を診断 AWS Health および修正しますIAM。

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 を実行する権限がありません。PassRole](#)
- [アクセスキーを表示したい](#)
- [管理者であり、他のユーザーにアクセスを許可したい AWS Health](#)
- [AWS アカウント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

がアクションを実行する権限がないと AWS Management Console 指示した場合は、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。

には、からのビジネス、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 AWS Health APIが必要で[AWS Support](#)。Business、Enterprise On-Ramp、または Enterprise Support プランがないアカウント AWS Health APIから を呼び出すと、次のエラーコードが返されます。SubscriptionRequiredException

iam を実行する権限がありません。PassRole

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

一部の AWS 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、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次のエラー例は、 という名前のIAMユーザーがコンソールを使用して marymajor でアクションを実行しようとするると発生します AWS Health。ただし、このアクションをサービスが実行するには、

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

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

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

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

アクセスキーを表示したい

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

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

Important

[正規のユーザー ID を確認する](#)ためであっても、アクセスキーを第三者に提供しないでください。これにより、誰かにへの永続的なアクセスを許可できます AWS アカウント。

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

管理者であり、他のユーザーにアクセスを許可したい AWS Health

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

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

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

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

詳細については、以下を参照してください。

- がこれらの機能 AWS Health をサポートしているかどうかについては、「」を参照してくださいと [AWS Health の仕組み IAM](#)。
- 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。
- サードパーティー にリソースへのアクセスを提供する方法については AWS アカウント、IAM ユーザーガイドの [「サードパーティー AWS アカウント が所有する へのアクセスを提供する」](#) を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの [「外部認証されたユーザーへのアクセスを提供する \(ID フェデレーション \)」](#) を参照してください。

- クロスアカウントアクセスにロールとリソースベースのポリシーを使用する違いについては、IAM ユーザーガイドの「[のクロスアカウントリソースアクセスIAM](#)」を参照してください。

AWS Healthのサービスにリンクされたロールの使用

AWS Health は AWS Identity and Access Management (IAM) [サービスにリンクされたロール](#) を使用します。サービスにリンクされたロールは、 に直接リンクされる一意のタイプの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、特に定義されていない限り、 はロールのみを引き受け AWS Health ることができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

AWS Healthのサービスリンクロールのアクセス許可

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

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

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

AWS Healthのサービスリンクロールの作成

を作成する必要はありません。AWSServiceRoleForHealth_Organizations サービスにリンクされたロール。[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。

を手動で作成する必要があります AWSServiceRoleForHealth_EventProcessor アカウント内のサービスにリンクされたロール。詳細については、[「ユーザーガイド」の「サービスにリンクされたロールの作成」](#)を参照してください。IAM

AWS Healthのサービスにリンクされたロールの編集

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

AWS Healthのサービスリンクロールの削除

を削除するには AWSServiceRoleForHealth_Organizations ロールの場合、まず [DisableHealthServiceAccessForOrganization](#) オペレーションを呼び出す必要があります。その後、IAMコンソール、APIまたは AWS Command Line Interface () IAM からロールを削除できます AWS CLI。

を削除するには AWSServiceRoleForHealth_EventProcessor に問い合わせ、AWS インシデント検出 AWS Support とレスポンスからワークロードをオフボードするように依頼します。このプロセスが完了したら、IAMコンソール、IAMAPIまたは を通じていずれかのロールを削除できます AWS CLI。

関連情報

詳細については、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。

AWS の マネージドポリシー AWS Health

AWS マネージドポリシーは、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 マネージドポリシーは、多くの一般的なユースケースに対するアクセス許可を提供するように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、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権限のアクセス許可を付与しない場合がありますことに注意してください。ユースケース別に [カスタムマネージドポリシー](#) を定義して、マネージドポリシーを絞り込むことをお勧めします。

AWS マネージド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 マネージドポリシーで AWS 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最も高いです。

詳細については、「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。IAM

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 マネージドポリシー : AWSHealthFullAccess](#)
- [AWS HealthAWS マネージドポリシーの更新](#)

AWS マネージドポリシー : AWSHealth_EventProcessorServiceRolePolicy

AWS Health は を使用します。 [AWSHealth_EventProcessorServiceRolePolicy](#) AWS マネージドポリシー。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 インシデント検出とレスポンスの Amazon EventBridge ルール AWS Health へのアクセスを許可する以下のアクセス許可があります。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

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

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

ポリシーへの変更のリストについては、「[AWS HealthAWS マネージドポリシーの更新](#)」を参照してください。

AWS マネージドポリシー : Health_OrganizationsServiceRolePolicy

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

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

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

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- organizations – Organizations AWS 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。

```
{
  "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 マネージドポリシーの更新](#)」を参照してください。

AWS マネージドポリシー : AWSHealthFullAccess

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

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

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

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

```

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

```

ポリシーへの変更のリストについては、「[AWS HealthAWS マネージドポリシーの更新](#)」を参照してください。

AWS HealthAWS マネージドポリシーの更新

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 AWS の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 フィードにサブスクライブしてください。

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 マネージドポリシー : AWSHealthFullAccess – 既存ポリシーへの更新	AWS Health は AWSHealth FullAccess、ポリシーを AWS GovCloud (US) Regions および中国リージョンに拡張しました。	2023 年 10 月 16 日
AWS マネージドポリシー : Health_OrganizationsService	AWS Health に新しい AWS Organizations アクションが追加され、サービスにリンクさ	2023 年 7 月 19 日

変更	説明	日付
eRolePolicy – 既存ポリシーへの更新	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なりました AWS Organizations。	
変更ログが発行されました	AWS Health マネージド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、 をモニタリングし AWS Health、問題が発生したときに報告し、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。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのCPU使用状況やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、[「Amazon CloudWatch ユーザーガイド」](#)を参照してください。
- Amazon EventBridge は、 near-real-time AWS resources. EventBridge enables 自動イベント駆動型コンピューティングの変更を記述するシステムイベントのストリームを提供します。これらのイベントが発生したときに、特定のイベントを監視し、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 AWS Health を使用した でのイベントのモニタリング EventBridge」](#)を参照してください。
- AWS CloudTrail は、アカウントによって、または AWS アカウントに代わって行われたAPI呼び出しおよび関連イベントをキャプチャし、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信します。と呼ばれる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、呼び出しが発生した日時を特定できます。詳細については、[AWS CloudTrail ユーザーガイド](#)をご参照ください。

詳細については、[「モニタリング AWS Health」](#)を参照してください。

のコンプライアンス検証 AWS Health

AWS 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スコープ」](#)の「」の「」を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードすることができます AWS Artifact。詳細については、「」の [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、データの機密性、会社のコンプライアンス目的、および適用される法律と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。

- [セキュリティとコンプライアンスのクイックスタートガイド](#) – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境を にデプロイする手順について説明します。
- [Amazon Web Services HIPAA のセキュリティとコンプライアンスのためのアーキテクチャ](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA の対象となるアプリケーションを作成する方法について説明します。

Note

すべての AWS のサービス がHIPAA対象となるわけではありません。詳細については、[HIPAA「対象サービスリファレンス」](#)を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界とロケーションに適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council ()、国際標準化機構 (ISO) などPCI) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- AWS Config 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 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確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、[Security Hub のコントロールリファレンス](#)を参照してください。
- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出できます。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検出要件を満たすことでDSS、PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクと規制や業界標準へのコンプライアンスの管理を簡素化できます。

での回復力 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ゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、高冗長ネットワークに接続されている複数の物理的に分離され、分離されたアベイラビリティゾーンを提供します。アベイラビリティゾーンでは、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ゾーンに格納され、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、[Amazon Web Services: セキュリティプロセスの概要](#)ホワイトペーパーで説明されている AWS グローバルネットワークセキュリティ手順によって保護されています。

AWS 公開されたAPI呼び出しを使用して、ネットワーク AWS Health 経由で にアクセスします。クライアントは Transport Layer Security (TLS) 1.0 以降をサポートする必要があります。1.2 TLS 以降をお勧めします。また、クライアントは、エフェメラルディフィヘルマン (PFS) や楕円曲線エフェメラルディフィヘルマン () など、完全なフォワードシークレット (DHE) を持つ暗号スイートもサポートする必要がありますECDHE。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリンIAM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。

の設定と脆弱性の分析 AWS Health

設定と IT コントロールは、AWS お客様とお客様の責任を共有します。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

の操作については、以下のベストプラクティスを参照してください AWS Health。

AWS Health ユーザーに最小限のアクセス許可を付与する

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

詳細については、「[AWS Health ID 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

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するには、 を AWS Health Dashboard 頻繁にチェックします。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が表示される場合があります。

詳細については、「[AWS Health ダッシュボードの開始方法](#)」を参照してください。

Amazon Chime または Slack AWS Health との統合

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、「」の [AWS Health 「ツール」](#) を参照してください [GitHub](#)。

AWS Health イベントのモニタリング

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

場合によっては、AWS Health イベントのリージョンが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。このリージョンで CloudWatch イベントを設定して、これらのイベントを確実にモニタリングできます。

詳細については、「[Amazon AWS Health を使用したでのイベントのモニタリング EventBridge](#)」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、およびサービスのイベントを表示できます。

イベントを集計し、運用イベントの影響を受けている組織内のアカウントや、セキュリティの脆弱性の通知を受けている組織内のアカウントを特定できます。また、この情報を使用して、組織全体のリソースメンテナンスイベントを事前に管理および自動化することもできます。この機能を使用して、更新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について常に把握します。

[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、運用チームが組織内の 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用すると、管理アカウントを制限したままにし、チームが AWS Health イベントに対処するために必要な可視性を提供できます。

Important

- AWS Health は、組織ビューを有効にする前に組織内で発生したイベントを記録しません。例えば、この機能を有効にする前に、組織内のメンバーアカウント (111122223333) が Amazon Elastic Compute Cloud (Amazon EC2) のイベントを受信した場合、このイベントは組織ビューに表示されません。
- 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、AWS Health や Organizations アクションへのアクセスを許可するIAMポリシーを使用します。[AWSHealthFullAccess](#) ポリシー。詳細については、「[AWS Health ID 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](#)
- [組織ビューの表示](#)
- [組織ビューの無効化](#)

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の一元化されたビューを取得できます。

組織ビューは、すべての AWS Support 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場合は、[AWSHealthFullAccess](#) ポリシー。詳細については、「[AWS Health ID 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. <https://health.aws.amazon.com/health/ホーム> 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、[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

- この機能の有効化は非同期プロセスであり、完了するまでに時間がかかります。組織内のアカウント数によっては、アカウントの読み込みに数分かかる場合があります。そのままにして、後で AWS Health コンソールを確認することができます。
- Business、Enterprise On-Ramp、または Enterprise Support プランがある場合は、[DescribeHealthServiceStatusForOrganization](#) API オペレーションを呼び出してプロセスのステータスを確認できます。
- この機能を有効にすると、Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを持つ AWSServiceRoleForHealth_Organizations サービスにリンクされたロールが組織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)

[EnableHealthServiceAccessForOrganization](#) API オペレーションを使用して組織ビューを有効にできます。

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

- を呼び出すには、[Business](#)、[Enterprise On-Ramp](#)、または [Enterprise Support](#) プランが必要です AWS Health API。
- 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、for version Java 2.0 を使用できます AWS SDK。

```
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.EnableHealthServiceAccessForOrganizationRequest;
import
software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationResponse;
```



```
import
software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequest;
import
software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResponse;

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 デベロッパーガイド」](#)を参照してください。

この機能を有効にすると、Health_OrganizationsServiceRolePolicy AWS マネージドポリシーを持つAWSServiceRoleForHealth_Organizations [サービスにリンクされたロール](#)が組織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、プロセスのステータスを確認できます。

組織ビューの表示

AWS Health コンソールを使用して、AWS 組織内のヘルスイベントの一元化されたビューを取得できます。

組織ビューは、すべての AWS Support 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場合は、[AWSHealthFullAccess](#) ポリシー。詳細については、「[AWS Health ID 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 を組織ビューに自動的に追加します。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。カスタムアクションを EventBridge ルールとともに使用して、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、閉じたアカウントを再度開くと、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元します。
- 詳細については、「[アカウントの解約](#)」を参照してください。

Important

AWS GovCloud (US) リージョンの顧客の場合：

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

Note

この機能を有効にすると、AWS Health コンソールは、過去 7 日間の [AWS Health Dashboard – Service Health](#) から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ごと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 および最近の問題タブを使用して、への変更 AWS のサービス や組織に影響を与えるリソースなど、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. ホームで AWS Health Dashboard を開きます。 <https://health.aws.amazon.com/health/>
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

スケジュールされた変更

[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]

イベントログタブを使用して、組織ビューの AWS Health イベントを表示することもできます。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. ホームで AWS Health Dashboard を開きます。 <https://health.aws.amazon.com/health/>

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) インスタンスメンテナンスのイベントが近づいている場合、Amazon EC2インスタンスを持つ組織内のアカウントが詳細タブに表示されます。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/ホーム> 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内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。カスタムアクションを EventBridge ルールとともに使用して、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、閉じたアカウントを再度開くと、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元します。
- 詳細については、「[アカウントの解約](#)」を参照してください。

Important

AWS GovCloud (US) リージョンの顧客の場合 :

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

オペレーションを使用して、組織ビューからイベントを AWS Health API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、管理アカウントからこの機能をオフにするか、[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約を停止します。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/ホーム> 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、API または AWS Command Line Interface (CLI) IAM を通じ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

Organizations [DisableAWSServiceAccess](#) API オペレーションを使用して、組織機能を無効にすることもできます。このオペレーションを呼び出し後、AWS Health は、組織内の他のすべてのアカウントのイベントの集計を停止します。組織ビューのオペレーションを AWS Health API 呼び出すと、`error. AWS Health continues` を AWS Health 返し、アカウントのヘルスイベントを集計します AWS。

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) IAM コンソール、API または を通じ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。

委任管理者の組織ビュー

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

目次

- [組織ビューに委任管理者を登録する](#)
- [組織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、メンバーは委任された管理者アカウントになり、AWS Health ダッシュボードからAWS Health組織ビューにアクセスできるようになります。アカウントに[ビジネス](#)、[エンタープライズ On-Ramp](#)、または[エンタープライズ](#)サポートプランがある場合、委任された管理者はAWS HealthAPIを使用してAWS Health組織ビューにアクセスできます。

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

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

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

組織ビューから委任管理者を削除する

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

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

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

Amazon AWS Health を使用した でのイベントのモニタリング EventBridge

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

メモ

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

AWS Health ワークフロー EventBridge の一部として、 の複数のターゲットタイプを選択できます。これには、以下が含まれます。

- 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) 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 チャン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 SNS ときに Amazon に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、「」の [AWS Health 「ツール」](#) を参照してください GitHub。

トピック

- [AWS リージョン カバレッジの EventBridge ルールの作成](#)
- [のアカウント固有イベントとパブリックイベントのモニタリング AWS Health](#)
- [AWS Incident Detection and Response を使用するためのサービスにリンクされたロールのインストール](#)
- [AWS Health イベント Amazon EventBridge スキーマ](#)
- [での AWS Health イベントのページ分割 EventBridge](#)
- [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 と統合する ServiceNow](#)
- [のイベントに関する通知を送信する EventBridge ルールの設定 AWS Health](#)
- [でイベントに関する通知を送信する AWS Chatbot ように を設定する AWS Health](#)
- [のイベントにตอบสนอง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 AWS Health](#)

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「ヘルスのパブリックイベントについて」](#)を参照してください。標準AWSパーティション内のすべてのリージョンについて、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、イベントを受信し続けるためにバックアップとして米国西部 (オレゴン) にルールを設定できます。米国西部 (オレゴン) のバックアップリージョンは米国東部 (バージニア北部) です。

例えば、欧州 (フランクフルト) リージョンでイベントをモニタリングしていて、そのリージョンが一時的に利用できない場合、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 EventBridge ルールの設定 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、() に AWS Identity and Access Management 送信されたイベントが含まれますIAM。グローバルイベントを受信するには、米国東部 (バージニア北部)

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

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

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

から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。

- アカウント固有のイベントは、Amazon EC2インスタンスへの必要な更新やその他のスケジュールされた変更イベントを通知するイベントなど、アカウントとリソースに影響します。
- 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。イベントARNを使用して AWS Health イベントを重複排除することをお勧めします。また、バックアップリージョンに送信される AWS Health メッセージでは、イベントの重複は一貫している `communicationId` ためです。

`eventScopeCode` パラメータを使用して EventBridge、イベントが でパブリックかアカウント固有かを特定できます。イベントには、 `PUBLIC` または `ACCOUNT_SPECIFIC` を含めることができます。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 EC2 での Amazon 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"
  }
}
```

AWS Incident Detection and Response を使用するためのサービスにリンクされたロールのインストール

アカウントに AWS Incident Detection and Response を使用する場合は、アカウントに [AWSServiceRoleForHealth_EventProcessor](#) サービスにリンクされたロールをインストールする必要があります。

このロールは `event-processor.health.amazonaws.com` サービスプリンシパルを信頼してそのロールを引き受けます。このロールにアタッチされているのは、`AWSHealth_EventProcessorServiceRolePolicy` AWS マネージドポリシーです。このポリシーは、ロールが実行できるアクセス許可を一覧表示します。例えば、他の AWS のサービス を呼び出すなどです。

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

関連情報

詳細については、以下のトピックを参照してください。

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

AWS Health イベント Amazon EventBridge スキーマ

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

AWS Health イベントスキーマ


AWS Health イベントスキーマ


パラメータ	説明	必須
バージョン	EventBridge バージョン、現在「0」	可能
id	イベントの <code>uniqueEventBridge</code> 識別子	可能

パラメータ	説明	必須
detail-type	ディテールタイプを記述します。AWS Health イベントの場合、これは &AWS Health Event または AWS Health Abuse Event になります。	可能
source	イベントバースソース。AWS Health イベントの場合、これは aws.health	可能


パラメータ	説明	必須
account	<p>AWS Health イベント accountId が送信されたへの。</p> <div data-bbox="1068 495 1273 1772"><p> Note</p><p>組織ビューの場合、管理アカウントまたは委任管理者アカウントで受信 affectedAccount された場合、これはとは異なる</p></div>	可能

パラメータ	説明	必須
	りま す。	
time	通知が に送 信された時 刻 EventBrid ge。形式: yyyy-mm-d dThh:mm:s sZ 。	可能

パラメータ	説明	必須
region	<p>通知 AWS リージョンが配信されたを識別します。</p> <div data-bbox="1068 495 1273 1860"><p> Note</p><p>このフィールドは、この AWS Health イベントの影響を受けるリージョンを示しません。これは「detail.eventRegion」によって提供さ</p></div>	可能

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

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


パラメータ		説明	必須
	eventArn	<p>特定のリージョンのAWS Health イベントの一意的識別子には、リージョンとイベントIDが含まれます。</p> <div data-bbox="1068 682 1274 1621" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>eventArn は、特定の顧客アカウントまたはリージョンに一意的ではありません。</p></div>	可能

パラメータ	説明	必須	
	service	AWS Health イベントによって 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 などです。	可能

パラメータ		説明	必須
	eventTypeCode	<p>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 を含むイベント MAINTENANCE_SCHEDULED は通常、の約 2 週間前にプッシュアウトされます。startTime。</p> <div data-bbox="1068 1409 1269 1873" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>新たに予定されているライフサイクル</p> </div>	可能

パラメータ		説明	必須
		<p>ルイベン トには すべ てイ ベ ント タイ プAWS_{S ICE}_PL NED_LIFI YCLE_EVI T が あ りま す。</p>	
	eventTypeCategory	<p>イベントのカ テゴリコード 指定できる値 は、issue、ac tificatio n、investig tion、sched Change で す。</p>	可能


パラメータ		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。想定される値は、ACCOUNT_SPECIFIC または PUBLIC です。	可能

パラメータ		説明	必須
	communicationId (新規)	<p>AWS Health イベントのこの通信の一意の識別子。</p> <p>同じメッセージ communicationId は、1 つの AWS Health イベントのバックアップメッセージまたはページである可能性があります。この識別子は、メッセージの重複排除に役立つ accountId ように使用できます。</p> <div data-bbox="1068 1339 1269 1852" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>ページ分割機能のリリースでは、には</p> </div>	可能


パラメータ	説明	必須
	ページ番号 communicationId が含まれており、1234567890-1 など、ページ間でcommunicationId一意なを保持します。詳細については、 「でのAWS Health イベントのページ	

パラメータ	説明	必須
	<p>分割 EventBridge 「ge」 を参 照し てく ださ い。</p>	

パラメータ	説明	必須
	<p>startTime</p>	<p>可能</p>


 **Note**

予定されているイベントの開始時間は、未来であってもかまいません。

パラメータ	説明	必須
endTime	<p>形式の AWS Health イベントの終了時刻: DoW, DD MMM YYYY HH:MM:SS TZ。</p> <div data-bbox="1068 590 1273 1482"><p> Note</p><p>endTime は、将来設定されるイベントには提供されない場合があります。</p></div>	不可

パラメータ	説明	必須	
	lastUpdatedTime	形式の AWS Health イベントの最終更新時刻: DoW, DD MMM YYYY HH:MM:SS TZ。	可能
	statusCode	AWS Health イベントのステータス。 使用できない値は open、closed または upcoming です。	可能
	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。	可能

パラメータ	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。	可能
	language	可能


パラメータ	説明	必須
	<p>latestDescription</p> <p>AWS Health イベントが AWS Health API からレンダリングされるときに記述され、通常は AWS Health ダッシュボードに表示されます。</p> <div data-bbox="1068 779 1271 1818"><p> Note</p><p>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</p></div>	可能

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

パラメータ	説明	必須
	<p data-bbox="591 226 846 260"><metadata key 1></p> <p data-bbox="1068 226 1235 449">メタデータ キー、値文 字列"keyst ring1": "keyvalue1"</p> <div data-bbox="1068 495 1269 1812" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p data-bbox="1101 533 1219 567">Note</p><p data-bbox="1149 590 1243 1766">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。</p></div>	不可

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

KNOWN

パラメータ		説明	必須
	page (新規)	<p>このメッセージが表すページ。詳細については、「での AWS Health イベントのページ分割 EventBridge」を参照してください。</p> <div data-bbox="1068 730 1269 1869" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>ページ分割はリソース上でのみ行われます。256 KB のサイズ制限違反のその他の原因として、通</p></div>	可能

パラメータ	説明	必須
	信が失敗する原因があります。	

パラメータ		説明	必須
	totalPages (新規)	<p>このヘルスイベントのページの総数。詳細については、「での AWS Health イベントのページ分割 EventBridge」を参照してください。</p> <div data-bbox="1068 779 1271 1869"><p>Note</p><p>これを使用して、あるアカウントについて複数ページにわたる通信の全ページを受信した</p></div>	可能

パラメータ	説明	必須
	かどうかを判断できません。	

パラメータ		説明	必須
	affectedAccount (新規)	<p>これは accountId、影響を受けるアカウントのです。</p> <div data-bbox="1068 493 1269 1871" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note</p> <p>これは、このヘルスイベントがの一部であるアカウントに送信 AWS Organizations され、管理アカウントまたは委任された管</p> </div>	可能

パラメータ		説明	必須
		理者 アカ ウン トで 受信 され る場 合、 「 アカ ウン ト」 フィー ルド とは 異な る場 合 があ りま す。	

公衆衛生イベント - 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"
}
}
```

アカウント固有の AWS Health イベント - Amazon EC2 Instance Store Drive Performance Degraded

```
{
  "version": "0",
  "id": "121345678-1234-1234-1234-123456789012",
  "detail-type": "AWS Health Event",
  "source": "aws.health",
  "account": "123456789012",
  "time": "2022-06-03T06:27:57Z",
  "region": "us-west-2",
  "resources": [
    "i-abcd1111"
  ],
  "detail": {
    "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
    "service": "EC2",
    "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
    "eventTypeCategory": "issue",
    "eventScopeCode": "ACCOUNT_SPECIFIC",
    "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
    "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
    "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
```

```
    "statusCode": "open",
    "eventRegion": "us-west-2",
    "eventDescription": [{
      "language": "en_US",
      "latestDescription": "A description of the event will be provided here"
    }],
    "affectedEntities": [{
      "entityValue": "i-abcd1111"
    }],
    "page": "1",
    "totalPages": "1",
    "affectedAccount": "123456789012"
  }
}
```

での AWS Health イベントのページ分割 EventBridge

AWS Health は、「リソース」または affectedEntities 「」のリストによってメッセージのサイズが EventBridge のメッセージサイズ制限の 256KB 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。以前 AWS Health は、この制限を超えた場合、はリソースの完全なリストをイベントと通信しませんでした。

AWS Health メッセージにすべての「リソース」と「詳細 affectedEntities」が含まれるようになりました。この「リソース」と「詳細 affectedEntities」のリストが 256KB を超える場合、はヘルスイベントを複数のページに AWS Health 分割し、これらのページを個々のメッセージとしてに発行します EventBridge。各ページは同じイベント ARN を保持し communicationId、すべてのページが受信された後に「リソース」または「詳細 affectedEntities」のリストを再結合するのに役立ちます。

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

ページネーションの起動をサポートするために、いくつかのスキーマ変更が含まれています。各には、ページが 1 ページしかない場合でも communicationId、の後にハイフンで囲まれたページ番号が含まれる communicationId ようになりました。また、現在のページ番号と AWS Health イベントのページ総数を記述 totalPages する、Detail.page と detail の 2 つの新しいフィールドもあります。ページ分割された各メッセージに含まれる情報は、「詳細 affectedEntities」または「リソース」の

ストを除いて同じです。これらのリストは、すべてのページを受信した後で再構築できます。影響を受けるリソースやエンティティのページは、順序に依存しません。

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

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

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

で組織ビューと委任された管理者アクセスを有効にする方法の詳細については AWS Health、「イベントを[集約する AWS Health](#)」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 と統合する ServiceNow

AWS Health イベントを JIRA および と統合 ServiceNow すると、サービス管理コネクタ () を使用して、運用情報とアカウント情報を受信したり、スケジュールされた変更の準備をしたり、ヘルスイベントを管理したりできます SMC。と SMC の統合では、を通じて送信されたヘルスイベントを使用して、JIRA チケット ServiceNow とインシデント EventBridge を自動的に作成、マッピング、更新 AWS Health できます。

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

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

を使用した JIRA Management Cloud の統合の詳細については SMC、「[AWS Health 「」の JIRA 「](#)」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 EventBridge ルールの設定

AWS Health

アカウント内の AWS Health イベントの通知を受け取る EventBridge ルールを作成できます。のイベントルールを作成する前に AWS Health、以下を実行します。

- のイベント、ルール、ターゲットについて理解します EventBridge。詳細については、[「Amazon ユーザーガイド」の「Amazon EventBridgeとは」と「新しい EventBridge - AWS リソースの変更を追跡して対応」](#)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. で Amazon EventBridge コンソールを開きます <https://console.aws.amazon.com/events/>。
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. イベントソースのイベントパターンの構築ページで、AWS イベントと EventBridge パートナーイベントを選択します。
8. [イベントパターン] 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 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 EC2。
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。
- 特定のイベントタイプカテゴリ (複数可) を選択し、問題、accountNotificationなどの値をリストから選択します。scheduledChange。

 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。
 - 特定のリソース (複数可) を選択し、1つ以上のリソースIDsのを入力します。例えば、次のような Amazon EC2 インスタンス ID を指定できます。 *i-EXAMPLEa1b2c3de4*。このリソースのみに影響するイベントをモニタリングします。
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. [Next (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. [Next (次へ)] を選択します。
18. (オプション) [Configure tags] (タグの設定) ページで、いずれかのタグを追加し、[Next] (次へ) を選択します。
 - 注: タグは現在、の aws.health ソースによって送信されません EventBridge。
19. [Review and create] (確認および作成) ページで、ルールの設定を確認し、イベントモニタリング要件を満たしていることを確認してください。
20. ルールの作成を選択します。

Example : すべての Amazon EC2 イベントのルール

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

Event pattern [Info](#)

Event pattern form Custom patterns (JSON editor)

AWS service
The name of the AWS service as the event source

Health

Event type
The type of events as the source of the matching pattern

Specific Health events

i This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2

Any event type category

Specific event type category(s)

Any resource

Specific resource(s)

Event pattern

Event pattern, or filter to match the events1 {
2 "source": ["aws.health"],
3 "detail-type": ["AWS Health Event"],
4 "detail": {
5 "service": ["EC2"]
6 }
7 }

Copy Test pattern Edit pattern

Example : 特定の Amazon EC2 イベントのルール

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

- Amazon EC2 サービス
- scheduledChange イベントタイプカテゴリ
- 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

AWS service
The name of the AWS service as the event source

Health ▼

Event type
The type of events as the source of the matching pattern

Specific Health events ▼

i This builder helps to build an event pattern to get events from AWS Health regarding health status of other AWS services.

Any service

Specific service(s)

EC2 ▼

Any event type category

Specific event type category(s)

scheduledChange ▼

Any event type code

Specific event type code(s)

▼

AWS_EC2_INSTANCE_TERMINATION_SC X
HEDULED

AWS_EC2_INSTANCE_RETIREMENT_SCH X
EDULED

Any resource

Specific resource(s)

i-EXAMPLEa1b2c3de4

複数のサービスおよびカテゴリに対するルールの作成

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

次のオプションの 1 つを使用できます。

既存のルールにサービスとカテゴリを追加するには

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

新しいルールにサービスとカテゴリを追加するには

1. 「[「のイベントに関する通知を送信する EventBridge ルールの設定 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 EventBridge ルールの設定 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、AWS CLI コマンドリファレンスの [put-rule](#) を参照してください。

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 issue、Amazon EC2 Auto Scaling accountNotification、EC2Amazon 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 VPC。

```
{
```

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

でイベントに関する通知を送信する AWS Chatbot ように 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、アプリケーションとインフラストラクチャに影響を与える可能性のある最近の AWS サービスの問題を特定できます AWS。その後、[AWS Health Dashboard](#) にサインインして、更新に関する詳細情報を確認できます。例えば、AWS アカウントの AWS_EC2_INSTANCE_STOP_SCHEDULED イベントタイプをモニタリングしている場合、AWS Health イベントは Slack チャンネルに直接表示されることがあります。

前提条件

開始する前に、以下のものがが必要です。

- で設定されたチャットクライアント AWS Chatbot。Amazon Chime と Slack を設定できます。詳細については、AWS Chatbot 管理者ガイドの [AWS Chatbot の開始方法](#) を参照してください。
- 作成し、サブスクライブしている Amazon SNS トピック。既にトピックがある場合は、既存の SNS トピックを使用できます。詳細については、[「Amazon Simple Notification Service デベロッパーガイド」の「Amazon の使用開始 SNS」](#) を参照してください。

で AWS Health イベントを受信するには AWS Chatbot

1. 「[「のイベントに関する通知を送信する EventBridge ルールの設定 AWS Health」](#)」の手順をステップ 13 まで実行します。
 - a. ステップ 13 でイベントパターンの設定が完了したら、パターンの最後の行にカンマを追加し、次の行を追加してページ分割された AWS Health イベントから不要なチャットメッセージを削除します。「[での AWS Health イベントのページ分割 EventBridge](#)」を参照してください。



```
"detail.page": ["1"]
```
 - b. [ステップ 14](#) でターゲットを選択するときは、SNSトピックを選択します。AWS Chatbot コンソールで同じ SNS トピックを使用します。
 - c. 残りの手順を完了して、ルールを作成します。
2. [AWS Chatbot コンソール](#)に移動します。
3. Slack チャンネル名など、チャットクライアントを選択し、[Edit] (編集) を選択します。
4. 通知 - オプションセクションのトピック で、ステップ 1 で指定したトピックと同じ SNS トピックを選択します。
5. [Save] を選択します。



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

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

Example :Slack に送信された AWS Health イベント

以下は、Slack チャン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。

**AWS** APP 11:46 AM
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)
Event type code: AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED
EC2 has detected degradation of the underlying hardware hosting your Amazon EC2 instance associated with this event in the us-east-1 region. Due to this degradation your instance could already be unreachable. We will stop your instance after 2021-03-19 18:36:40 PST. Please take appropriate action before this time.\\n\\nYou can find more information about retirement events scheduled for your EC2 instances in the AWS Management Console <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Events>\\n\\n* What will happen to my instance?\\nYour instance will be stopped after the specified retirement date. You can start it agai...
[Show more](#)
Start time: Sat, 20 Mar 2021 01:35:40 GMT
End time: Sat, 20 Mar 2021 01:36:40 GMT

**AWS** APP 12:08 PM
 [AWS Health Event | us-east-1 | Account: 123456789012 | open](#)
Event type code: AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
We are writing to notify you that you may have exposed your S3 bucket/s to a larger audience than you intended. AWS recommends that you review your bucket permissions and ACLs to determine whether the access is appropriate. S3 bucket permissions should never contain \\\\"Principal\\\\": \\\\"*\\\\" unless you intend to grant public access to your data. Additionally, S3 bucket ACLs should be appropriately scoped to prevent unintended access to \\\\"Authenticated Users\\\\" or \\\\"Everyone\\\\" unless your use case requires it.\\n\\nThe list of buckets with this configuration is associated with this event.\\n\\nThe following links provide an overv...
[Show more](#)
Start time: Sat, 20 Mar 2021 01:35:40 GMT
End time: Sat, 20 Mar 2021 01:36:40 GMT

のイベントにตอบสนอง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 AWS Health

Amazon EC2インスタンスのスケジュールされたイベントにตอบสนองするアクションを自動化できます。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 オートメシヨンドキュメントなどのターゲットを呼び出して、ユーザーに代わってアクションを自動化できます。

例えば、Amazon EC2Elastic Block Store (Amazon EBS) でバックアップされたEC2インスタンスに Amazon インスタンスのリタイアイベントが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 ダッシュボードに送信します。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インスタンスのアクションを自動化するには、インスタンスを Systems Manager によって管理する必要があります。

詳細については、「[Amazon ユーザーガイド](#)」の「[EC2で Amazon を自動化 EventBridgeする](#)」を参照してください。 EC2

前提条件

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してからルールを作成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 コンソールで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、 でIAMコンソールを開きます<https://console.aws.amazon.com/iam/>。
2. ナビゲーションペインで、ポリシー を選択します。
3. [ポリシーの作成] を選択します。
4. JSON タブを選択します。
5. 以下をコピーしJSON、エディタJSONのデフォルトを置き換えます。

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



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

- a. Resource パラメータで、Amazon リソースネーム (ARN) に AWS アカウント ID を入力します。
- b. ロール名を置き換えることも、デフォルトを使用することもできます。この例では、を使用します。AutomationEVRole.

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. ポリシーの確認ページで、次のような名前を入力します。 *AutomationEVRolePolicy* およびオプションの説明。
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、「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

IAM ロールを作成する

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、 でIAMコンソールを開きます <https://console.aws.amazon.com/iam/>。
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を選択 で、AWS サービス を選択します。
4. このロールの引き受けを許可するサービスEC2を選択します。
5. [Next: Permissions] (次へ: アクセス許可) を選択します。
6. 次のような、作成したポリシー名を入力します。 *AutomationEVRolePolicy*、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. [Next: Tags] (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. ロール名 には、 と入力します。 *AutomationEVRole*。この名前は、作成したIAMポリシーARNの に表示される名前と同じである必要があります。
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、「[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。

IAM

信頼ポリシーの更新

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

ロールの信頼ポリシーを更新するには

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

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

6. 信頼ポリシーの更新 を選択します。

詳細については、IAM「[ユーザーガイド](#)」の「[ロール信頼ポリシーの変更 \(コンソール\)](#)」を参照してください。

のルールを作成する EventBridge

以下の手順に従って EventBridge コンソールにルールを作成し、廃止が予定されているEC2インスタンスの停止と開始を自動化できるようにします。

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

1. で Amazon EventBridge コンソールを開きます<https://console.aws.amazon.com/events/>。
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. 特定のサービス (複数可) を選択し、 を選択しますEC2。
9. 特定のイベントタイプカテゴリ (複数可) を選択し、 を選択しますscheduledChange。
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でバックアップされたインスタンスの場合は、 を選択します**AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED**。Amazon EC2インスタンスストアバックインスタンスの場合は、 を選択します**AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**。

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 オートメシヨンドキュメントターゲットを追加します。ターゲットの選択のターゲットで、SSMオートメシヨンを選択します。
13. [ドキュメント] で、[AWS-RestartEC2Instance] を選択します。
14. [Configure automation parameters(s)] (オートメシヨ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. 既存のロールを使用する を選択し、作成したIAMロールを選択します。AutomationEVRole.

ターゲットは以下の例のようになります。

Target Remove

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SSM Automation

Document

AWS-RestartEC2Instance

▶ Configure document version

▼ Configure automation parameter(s)

No Parameter(s)

Constant

Input Transformer

```
["Instances": "$resources"]
```

```
["InstanceId": <Instances>]
```

EventBridge needs permission to call SSM Start Automation Execution with your supplied Automation document and parameters. By continuing, you are allowing us to do so.

Create a new role for this specific resource

Use existing role

AutomationEVRole

Note

必要な EC2と Systems Manager のアクセス許可と信頼関係を持つ既存のIAMロールがない場合、ロールはリストに表示されません。詳細については、「[前提条件](#)」を参照してください。

18. [Create] (作成) を選択します。

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

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

Amazon を使用すると EventBridge、サービスやリソースに影響を与える可能性のある AWS Health イベントについて通知を受け取ることができます。例えば、が Amazon EC2 インスタンスに関するイベント AWS Health を発行する場合、これらの通知を使用してアクションを実行し、必要に応じてリソースを更新または置き換えることができます。詳細については、[「Amazon AWS Health を使用したでのイベントのモニタリング EventBridge」](#)を参照してください。

- AWS CloudTrail は、アカウントによって、または AWS アカウントに代わって行われた API 呼び出しおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。と呼ばれる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、呼び出しが発生した日時を特定できます。詳細については、[AWS CloudTrail ユーザーガイド](#)をご参照ください。

トピック

- [を使用した通話のログ記録 AWS Health API AWS CloudTrail](#)

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

AWS Health は、ユーザー AWS CloudTrail、ルール、または AWS のサービスによって実行されたアクションの記録を提供するサービスであると統合されています AWS Health。CloudTrail キャプチャでは、を AWS Health イベントとして API 呼び出します。キャプチャされた呼び出しには、AWS Health コンソールからの呼び出しとオペレーションへのコード呼び出しが含まれます AWS Health API。証跡を作成する場合は、の CloudTrail イベントを含む Amazon S3 バケットへのイベントの継続的な配信を有効にできます AWS Health。証跡を設定しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して

CloudTrail、に対して行われたリクエスト AWS Health、リクエスト元の IP アドレス、リクエスト者、リクエスト日時、その他の詳細を確認できます。

の設定方法や有効化方法など CloudTrail、の詳細については、[AWS CloudTrail ユーザーガイド](#)を参照してください。

AWS Health の情報 CloudTrail

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

のイベントなど、AWS アカウント内のイベントの継続的な記録については AWS Health、証跡を作成します。証跡により CloudTrail、はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータを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 サポートされているサービスと統合](#)
- [の Amazon SNS Notifications の設定 CloudTrail](#)
- [複数のリージョンからの CloudTrail ログファイルの受信](#)と複数のアカウントからのログファイルの[受信 CloudTrail](#)

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

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

- リクエストがルートまたは IAM 認証情報で行われたかどうか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか

- リクエストが別の AWS サービスによって行われたかどうか

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

Amazon S3 バケットにログファイルを任意の期間、保存することができます。また、Amazon S3 ライフサイクルのルールを定義して、自動的にログファイルをアーカイブまたは削除することもできます。デフォルトでは、ログファイルは Amazon S3 サーバー側の暗号化 () で暗号化されます SSE。

ログファイルの配信時に通知を受け取るには、新しいログファイルの配信時に Amazon SNS 通知を発行 CloudTrail するようにを設定できます。詳細については、[「の Amazon SNS 通知の設定 CloudTrail」](#) を参照してください。

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

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

例：AWS Health ログファイルエントリ

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

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

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/JaneDoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JaneDoe",
        "sessionContext": {"attributes": {
```

```
        "mfaAuthenticated": "false",
        "creationDate": "2016-11-21T07:06:15Z"
    }},
    "invokedBy": "AWS Internal"
},
"eventTime": "2016-11-21T07:06:28Z",
"eventSource": "health.amazonaws.com",
"eventName": "DescribeEntityAggregates",
"awsRegion": "us-east-1",
"sourceIPAddress": "203.0.113.0",
"userAgent": "AWS Internal",
"requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
"responseElements": null,
"requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
"eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abc29b",
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012"
}
],
...
}
```

のドキュメント履歴 AWS Health

次の表に、の今回のリリースのドキュメントを示します AWS Health。

- API バージョン : 2016-08-04

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

変更	説明	日付
Amazon JSON による AWS Health イベントのモニタリングで EventBridge 修正	詳細については、「 Amazon による AWS Health イベントのモニタリング EventBridge 」を参照してください。	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しました	詳細については、「 影響を受けるリソースビュー 」を参照してください。	2024 年 7 月 27 日
セキュリティセクションの AWS Health ドキュメントから Internetnetwork 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 — 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 「Dashboard – Service Health」 と「 の計画されたライフサイクルイベント AWS Health 」を参照してください。	2024 年 2 月 15 日
の EventBridge ルールの作成で重複する箇条書きを削除しました AWS Health	「 の EventBridge ルールの作成 」の「 重複する箇条書き AWS Health 」を削除しました。	2023 年 12 月 4 日

計画されたライフサイクルイベントに関するドキュメントを追加しました	詳細については、 AWS Health の計画されたライフサイクルイベント を参照してください。	2023 年 10 月 31 日
AWSHealthFullAccess のドキュメントの更新	これで、AWS GovCloud (US) Regionsで AWSHealth FullAccess のマネージドポリシーを使用できるようになりました。の AWS マネージドポリシーを参照してください AWS Health 。	2023 年 10 月 16 日
で AWS ユーザー通知を設定するためのドキュメントを追加しました AWS Health 。	で AWS ユーザー通知を設定できるようになりました AWS Health。詳細については、「 のAWS ユーザー通知を設定する AWS Health 」を参照してください。	2023 年 8 月 30 日
委任管理者機能のドキュメントを AWS Health イベントの集約セクションに追加しました。	詳細については、「 委任された管理者の組織図 」を参照してください。	2023 年 7 月 27 日
SLR ポリシーの更新	AWS マネージドポリシーの更新: Health_OrganizationsServiceRolePolicy。詳細については、「 AWS HealthのAWS マネージドポリシー 」を参照してください。	2023 年 7 月 19 日

AWS Health スキーマがイベントメタデータをサポートするようになりました	イベントから AWS Health イベントメタデータを受信できるようになりました。詳細については、 「Amazon によるイベントのモニタリング AWS Health EventBridge」 を参照してください。	2023 年 6 月 20 日
Amazon のドキュメントを更新しました EventBridge	Amazon EventBridge ルールを使用して、アカウント固有のイベントとパブリックイベントの両方をモニタリングできるようになりました。詳細については、 「Amazon によるイベントのモニタリング AWS Health EventBridge」 を参照してください。	2023 年 5 月 2 日
AWS 管理ポリシーのドキュメントを追加	「 AWS HealthのAWS マネージドポリシー 」と「 AWS Healthのサービスリンクロールの使用 」に関するドキュメントを追加しました。	2023 年 1 月 18 日
タイムゾーン設定に関するドキュメントを追加しました	新しいタイムゾーン機能を使用して、ローカルタイムゾーンまたはで AWS Health ダッシュボードを表示します UTC。詳細については、 AWS Health 「ダッシュボードの開始方法 – アカウントのヘルス」 および AWS Health 「ダッシュボード – サービスのヘルス」 を参照してください。	2022 年 9 月 21 日

更新版	対応 AWS Health に関するドキュメントを追加しました。詳細については、「 AWS Health Aware 」を参照してください。	2022 年 5 月 25 日
更新版	Service Health Dashboard と AWS Personal Health Dashboard は、AWS Health Dashboard にブランド変更されました。 詳細については、 AWS Health 「ダッシュボードの開始方法 – アカウントのヘルス」 および AWS Health 「ダッシュボード – サービスのヘルス」 を参照してください。	2022 年 2 月 28 日
Amazon のドキュメントを更新しました EventBridge	Amazon を使用して Health イベント EventBridge をモニタリング AWS Health するための新しいトピック。詳細については、「 Amazon によるイベントのモニタリング AWS Health EventBridge 」を参照してください。	2022 年 2 月 3 日
更新版	Enterprise On- Ramp Support プランをお持ちの場合は、使用できません AWS Health API。	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

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

[更新版](#)

以下のトピックが更新されました。 2021 年 1 月 29 日

- [AWS Health イベントの集計](#)に関するトピックを更新しました
- [Amazon CloudWatch Events による AWS Health イベントのモニタリングトピック](#)を再編成して更新しました
- [リソースおよびアクションに基づく条件](#)セクションを更新しました

[AWS Health コンソールに組織ビューの AWS Health ダッシュボードを追加](#)

AWS Health コンソールを使用して、組織ビュー機能を有効にできます。その後、AWS 組織内のメンバーアカウントのヘルスイベントを表示できます。 2020 年 12 月 14 日

[高可用性エンドポイントのデモ](#)

サンプルコードを使用して、のアクティブなリージョン エンドポイントと署名 AWS リージョンを決定できます AWS Health。 2020 年 10 月 22 日

[AWS Health ユーザーガイドの更新](#)

組織が を更新し、RSS フィードを追加しました。これにより、AWS Health ドキュメントの最新の更新をサブスクライブできます。 2020 年 8 月 28 日

以前の更新

変更	説明	日付
組織ビューのトピックを更新し、例を含めました。	「 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
によって提供されるイベントの制限を説明する新しいセクション「リソースベースおよびアクションベースの条件」を追加しました AWS Health API。	「 AWS Healthのためのアイデンティティおよびアクセス管理 」を参照してください。	2018 年 8 月 2 日
AWS Health 情報の可視性に関するメモを追加しました。	「 AWS Healthのためのアイデンティティおよびアクセス管理 」を参照してください。	2017 年 8 月 16 日
サービスのリリース。	AWS Health がリリースされました。	2016 年 12 月 1 日

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。