ユーザーガイド

AWS サポート

API バージョン 2025-01-27

AWS サポート: ユーザーガイド

Table of Contents

の開始方法 AWS サポート

サポート は、 AWS ソリューションの成功と運用の健全性をサポートするツールと専門知識へのアクセスを提供するさまざまなプランを提供します。すべてのサポートプランでは、カスタマーサービス、 AWS ドキュメント、技術文書、サポートフォーラムに 24 時間 365 日アクセスできます。AWS 環境を計画、デプロイ、改善するためのテクニカルサポートやリソースを増やすには、 AWS ユースケースのサポートプランを選択できます。

メモ

- でサポートケースを作成するには AWS Management Console、「」を参照してくださいサポートケースの作成。
- さまざまな AWS サポート プランの詳細については、「プランの比較 AWS サポート」および「」を参照してくださいAWS サポート プランの変更。
- サポートプランでは、サポートケースに対してさまざまな応答時間を提供しています。「緊急度の選択」および「応答時間」を参照してください。

トピック

サポートケースとケース管理の作成

では AWS Management Console、次の 3 種類のカスタマーケースを作成できます サポート。

- アカウントおよび請求のサポートケースは、 AWS のすべてのお客様にご利用いただけます。請求およびアカウントの質問については、ヘルプを参照してください。
- サービスの上限緩和リクエストは、 AWS のすべてのお客様にご利用いただけます。デフォルトの Service Quotas (以前の名称は制限) については、「AWS 全般のリファレンス」の「AWS Service Quotas」を参照してください。

- Technical support (技術サポート) ケースを選択すると、サービスに関連する技術的な問題、状況によってはサードパーティー製アプリケーションについて技術サポートに問い合わせることができます。Basic Support プランをご利用の場合は、技術サポートケースを作成できません。

> メモ
>
> - サポートプランを変更するには、AWS サポート プランの変更 を参照してください。
> - アカウントを解約するには、AWS Billing ユーザーガイドの「アカウントの解約」を参照してください。
> - の一般的なトラブルシューティングトピックについては AWS のサービス、「」を参照してくださいトラブルシューティングリソース。
> - の一部 AWS Partner である の顧客で AWS Partner Network、Resold Support を使用している場合、請求関連の問題については、 AWS Partner に直接お問い合わせください。AWS サポート は、請求やアカウント管理など、Resold Support の非技術的な問題をサポートすることはできません。詳細については、以下の各トピックを参照してください。
>   - AWS パートナーが組織内の計画を決定する AWS サポート 方法
>   - 「AWS Partner-Led Support」

サポートケースの作成

サポートケースは、 AWS Management Consoleのサポートセンターで作成できます。

> メモ
>
> - サポートセンターには、 AWS アカウントのルートユーザーまたは AWS Identity and Access Management (IAM) ユーザーとしてサインインできます。詳細については、「AWS サポート センターへのアクセスを管理する」を参照してください。
> - サポートセンターにサインインしてサポートを作成できない場合は、[お問い合わせ] ページを使用できます。このページでは、請求およびアカウントの問題に関するヘルプを参照できます。

サポートケースを作成するには

1. AWS Support Center Consoleにサインインします。

> **Tip**
>
> では AWS Management Console、疑問符アイコン
> ()
> を選択してから、サポートセンターを選択することもできます。

2. [Create case (ケースを作成)] を選択します。
3. 以下のオプションのいずれかを選択してください：
   - アカウントと請求
   - 技術的
   - Service Quotas の引き上げについては、サービス制限の増加をお探しですか? を選択してから、Service Quotas の引き上げの作成 の指示に従います。
4. [サービス]、[カテゴリ]、および [緊急度] を選択します。

> **Tip**
>
> よく寄せられる質問に表示される推奨ソリューションを使用できます。

5. 次のステップ:追加情報を選択します。
6. 追加情報ページの件名に、問題に関するタイトルを入力します。
7. 説明では、プロンプトに従って、次のようにケースを説明します。
   - 受信したエラーメッセージ
   - 使用したトラブルシューティング手順
   - サービスにアクセスした方法
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - API オペレーション
8. (オプション) 添付ファイルを選択して、エラーログやスクリーンショットなど、関連するファイルをケースに追加します。最大 3 つまでのファイルをアタッチできます。各ファイルは、最大 5MB まで可能です。

9. 次のステップ:今すぐ解決するか、お問い合わせくださいを選択します。
10. [Contact us] (お問い合わせ) ページで、希望する言語を選択します。
11. 希望する連絡方法を変更します。次のオプションのいずれかを選択します。

    a. ウェブ – Support Center で返信を受け取ります。

    b. チャット – サポート担当者とライブチャットを開始します。チャットに接続できない場合は、「トラブルシューティング」を参照してください。

    c. Phone (電話) — サポートエージェントが電話をかけます。このオプションを選択した場合は、次の情報を入力します。

    - 国またはリージョン
    - Phone number (電話番号)
    - (オプション) 拡張

> **メモ**
>
> - 連絡先オプションは、ケースのタイプとサポートプランによって異なります。
> - [ドラフトを破棄する] を選択して、サポートケースのドラフトをクリアすることもできます。

12. (オプション) Business、Enterprise On-Ramp、または Enterprise Support プランがある場合は、[追加の連絡先] オプションが表示されます。ケースのステータスが変わったときに通知する場合は、そのユーザーの E メールアドレスを指定します。IAM ユーザーとしてサインインしている場合は、自分の E メールアドレスを含めます。自分の root アカウントの E メールアドレスとパスワードを使用してサインインしている場合は、自分の E メールアドレスを指定する必要はありません。

> **Note**
>
> Basic Support プランをご利用の場合は、[Additional contacts] (追加の連絡先) オプションは使用できません。ただし、[マイアカウント] ページの [代替の連絡先] セクションで [操作] 連絡先を指定した場合、ケースに関するやり取りのコピーがその連絡先に送信されますが、送信されるのはアカウントと請求のケースと技術ケースの特定のケースに関するやり取りだけです。

13. ケースの詳細を確認して、[Submit] (送信) を選択します。ケース ID 番号と概要が表示されます。

問題の説明

できるだけ詳しく説明します。関連するリソース情報と、問題を理解するのに役立つその他の情報を含めてください。たとえば、パフォーマンスのトラブルシューティングの場合は、タイムスタンプとログの情報を含めます。機能のリクエストや一般的なガイダンスの質問の場合は、お使いの環境と目的の説明を含めます。いずれの場合も、ケースの送信フォームに表示される説明の指示に従って入力してください。

できるだけ詳しく説明していただくことで、ケースを迅速に解決できる可能性が高まります。

緊急度の選択

サポートケースを作成する際、常にサポートプランで許容される最大の緊急度で作成しがちです。しかし、最も高い緊急度は、回避できない場合や運用アプリケーションに直接影響する場合に選択することをお勧めします。1 つのリソースが失われてもアプリケーションに影響が及ばないようにサービスを構築する方法については、「Building Fault-Tolerant Applications on AWS」技術文書を参照してください。

次の表に、緊急度、応答時間、問題例を示します。

> メモ
>
> - サポートケースを作成した後は、緊急度コードを変更することはできません。状況が変わったら、サポートケースについて サポート エージェントと連携します。
> - 使用できる緊急度レベルの詳細については、AWS サポート API リファレンスを参照してください。

緊急度	緊急度コード	初回の応答時間	説明とサポートプラン
一般的な質問、または機能要望	`low`	24 時間	開発に関する一般的な質問がある場合、または機能をリクエストしたい場合 (*デベロッパー、

緊急度	緊急度コード	初回の応答時間	説明とサポートプラン
			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)
問題発生中、または開発中の急ぎの問い合わせ	`normal`	12 時間ごと	アプリケーションの重要ではない機能が正常に動作していない場合、または開発に関して短期間で回答が必要な質問がある場合 (*デベロッパー、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)
本番環境の重要な機能に障害発生中	`high`	4 時間	アプリケーションの重要な機能に、障害またはデグレードが発生している場合 (Business、Enterprise On-Ramp、または Enterprise Support プラン)
本番環境のシステム停止中	`urgent`	1 時間	ビジネスに重大な影響が出ている場合。アプリケーションの重要な機能を使用できない場合 (Business、Enterprise On-Ramp、または Enterprise Support プラン)
本番環境のビジネスクリティカルなシステム停止中	`critical`	15 分	ビジネスが危険な状態になっている場合。アプリケーションの重要な機能は利用できません (Enterprise Support プラン)。これは、Enterprise On-Ramp Support プランでは 30 分であることにご留意ください。

応答時間

お客様の初回のリクエストには、所定の時間内に応答するよう取り組んでいます。各 サポート プランのサポート範囲については、「AWS サポート の機能」を参照してください。

ビジネスプラン、エンタープライズ On-Ramp、またはエンタープライズサポートプランをご利用の場合は、年中無休 24 時間体制でテクニカルサポートにアクセスできます。*デベロッパーサポートの場合、目標応答時間は営業時間内で計算されています。営業時間は通常、お客様の国の祝日および週末を除いた午前 8:00 から午後 6:00 に定義されています。タイムゾーンが複数ある国/地域で

は、営業時間は変わる可能性があります。お客様の国情報は、 AWS Management Consoleの [My Account] (アカウント) ページにある [Contact Information] (連絡先情報) セクションに表示されています。

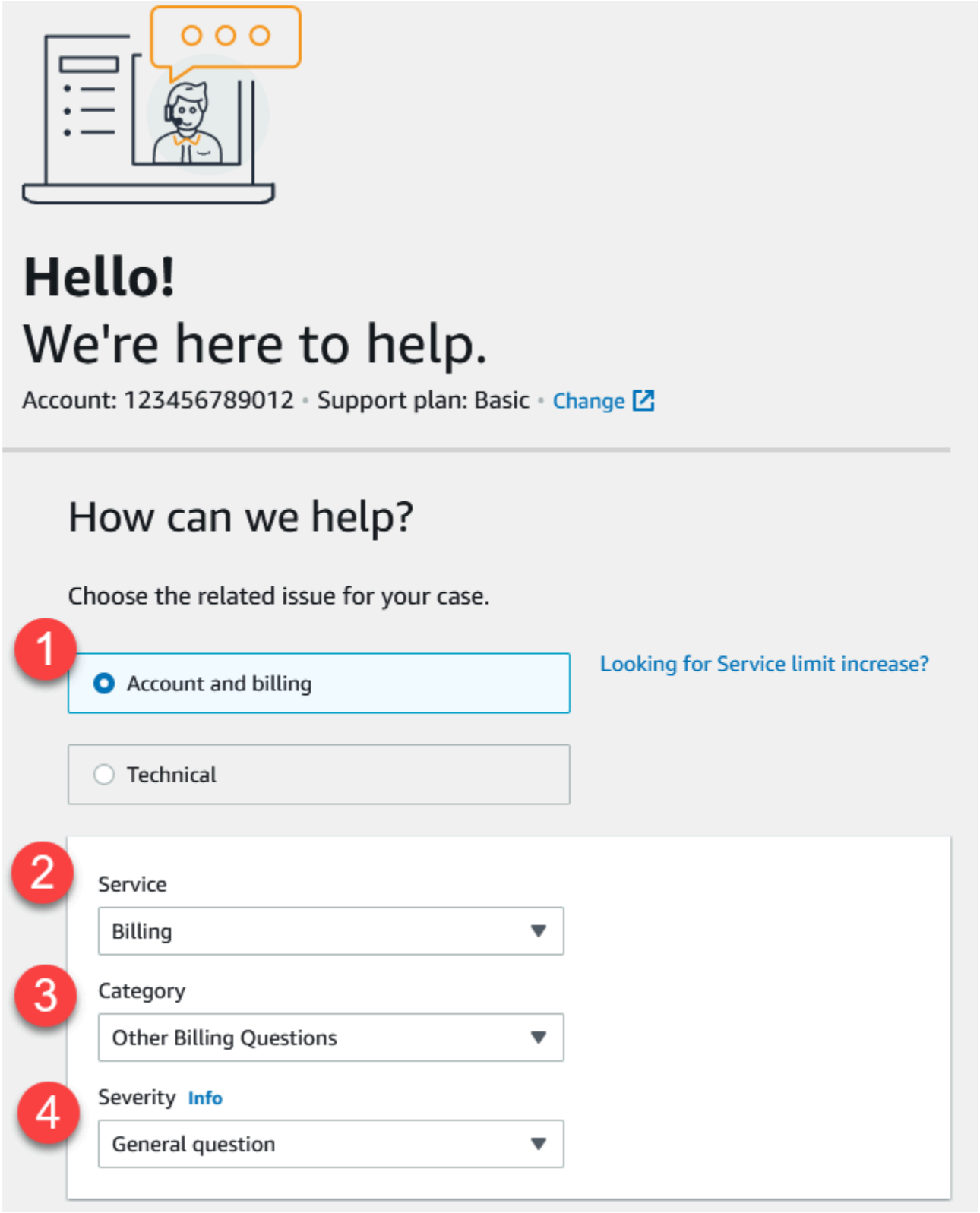
> **Note**
>
> サポートケースに連絡する際の希望言語として、日本語を選択した場合、以下のサポートを日本語でご利用いただけます。
>
> - テクニカルサポート以外のケースでカスタマーサービスが必要な場合や、デベロッパーサポートプランに加入していてテクニカルサポートが必要な場合は、祝日と週末を除き、日本標準時間の午前 9:00 から午後 6:00 (GMT+9) の営業時間内に、日本語サポートをご利用いただけます。
> - ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートプランをご利用の場合は、年中無休 24 時間体制で日本語のテクニカルサポートにアクセスできます。
>
> サポートケースに連絡する際の希望言語に中国語を選択した場合は、以下のように中国語サポートを受けられます。
>
> - テクニカルサポート以外のサポートケースでのカスタマーサービスが必要な場合は、祝日と週末を除き、午前 9:00から午後 6:00 (GMT+8) まで中国語サポートをご利用いただけます。
> - デベロッパーサポートプランに加入している場合、中国語でのテクニカルサポートは、通常、[アカウント] で設定されているご自身の国での、休日と週末を除く午前 8:00 から午後 6:00 までの営業時間内にご利用いただけます。タイムゾーンが複数ある国/地域では、営業時間が変わる可能性があります。
> - Business、Enterprise On-Ramp、または Enterprise サポートプランをご利用の場合は、年中無休 24 時間体制で中国語のテクニカルサポートが利用できます。
>
> サポートケースで希望言語として韓国語を選択している場合、以下のように韓国語でのサポートをご利用いただけます。
>
> - テクニカルサポート以外のケースでカスタマーサービスが必要な場合、休日と週末を除き、韓国標準時間 (GMT+9) の午前 9:00 から午後 6:00 までの営業時間内に、韓国語でのサポートをご利用いただけます。
> - デベロッパーサポートプランに加入している場合、韓国語でのテクニカルサポートは、通常、[アカウント] で設定されているご自身の国での、休日と週末を除く午前 8:00 から午後

6:00 までの営業時間内にご利用いただけます。タイムゾーンが複数ある国/地域では、営業時間が変わる可能性があります。

- Business、Enterprise On-Ramp、または Enterprise サポートプランをご利用の場合は、年中無休 24 時間体制で韓国語語のテクニカルサポートを受けられます。

例: アカウントと請求のサポートケースを作成します。

次の例は、請求およびアカウントの問題に対するサポートケースです。



1. ケースの作成 — 作成するケースのタイプを選択します。この例では、ケースのタイプはアカウントと請求です。

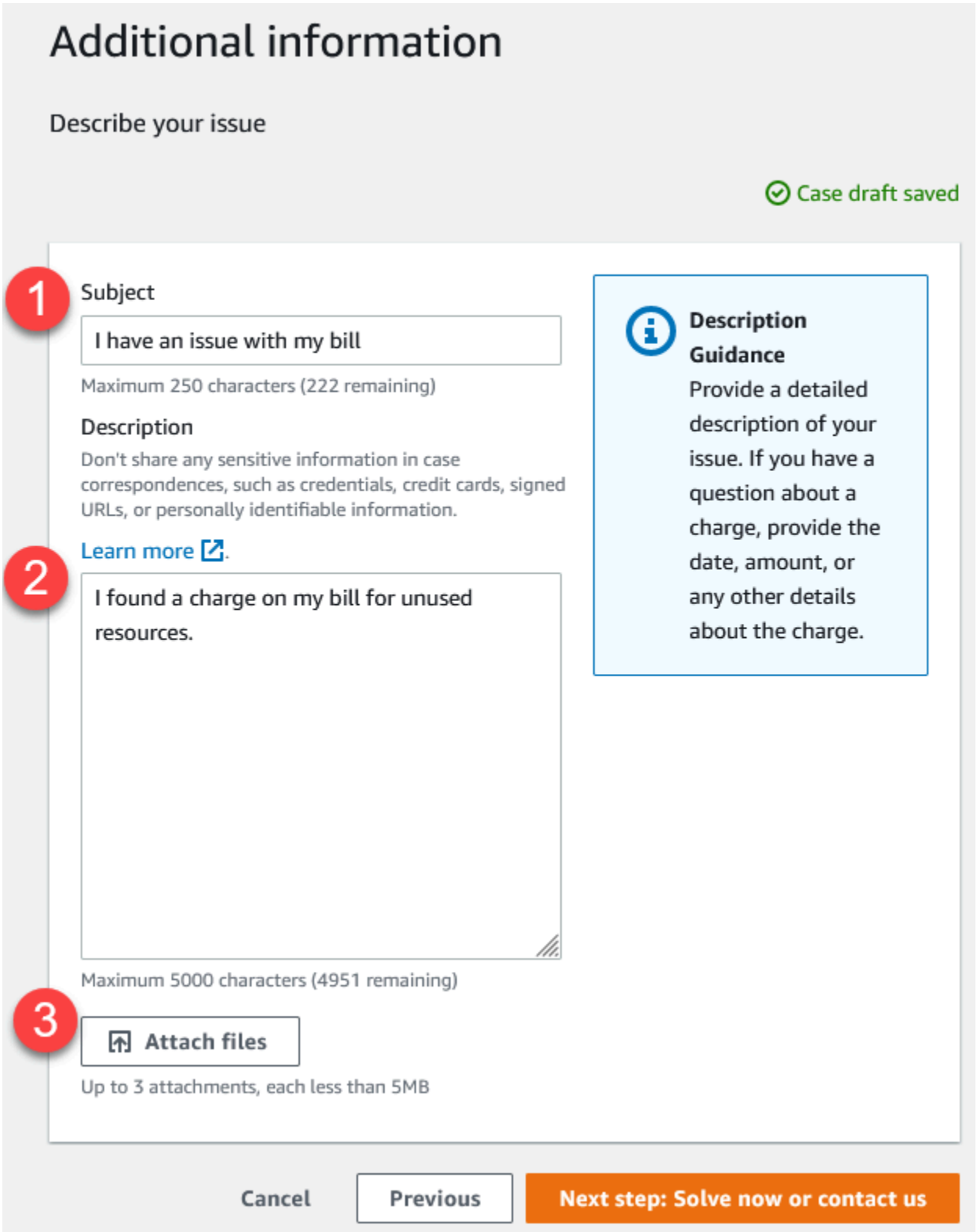
> **Note**
>
> Basic Support プランをご利用の場合は、技術サポートケースを作成できません。

2. [Service] (サービス) – 複数のサービスに関連する質問の場合は、最も該当するサービスを選択します。
3. [Category] (カテゴリ) – ユースケースに最も該当するカテゴリを選択します。カテゴリを選択すると、問題の解決に役立つ可能性がある情報のリンクが下に表示されます。
4. [Severity] (緊急度) – 有料サポートプランをご利用のお客様は、[一般的な質問、または機能要望] (応答時間 1 日) または [問題発生中、または開発中の急ぎの問い合わせ] (応答時間 12 時間) の緊急度レベルを選択できます。Business Support プランをご利用のお客様は [本番環境の重要な機能に障害発生中] (応答時間 4 時間) または [本番環境のシステム停止中] (応答時間 1 時間) も選択できます。Enterprise On-Ramp または Enterprise Support プランをご利用のお客様は、[本番環境のビジネスクリティカルなシステム停止中] (Enterprise Support では応答時間 15 分、Enterprise On-Ramp では応答時間 30 分) を選択できます。

   応答時間は、最初の応答の です AWS サポート。これらの応答時間は、その後の応答には適用されません。サードパーティの問題については、対応可能なスキルを持つ担当者の空き状況によって応答時間が長くなる可能性があります。詳細については、「緊急度の選択」を参照してください。

   > **Note**
   >
   > カテゴリの選択に基づいて、追加情報の入力を求められることがあります。

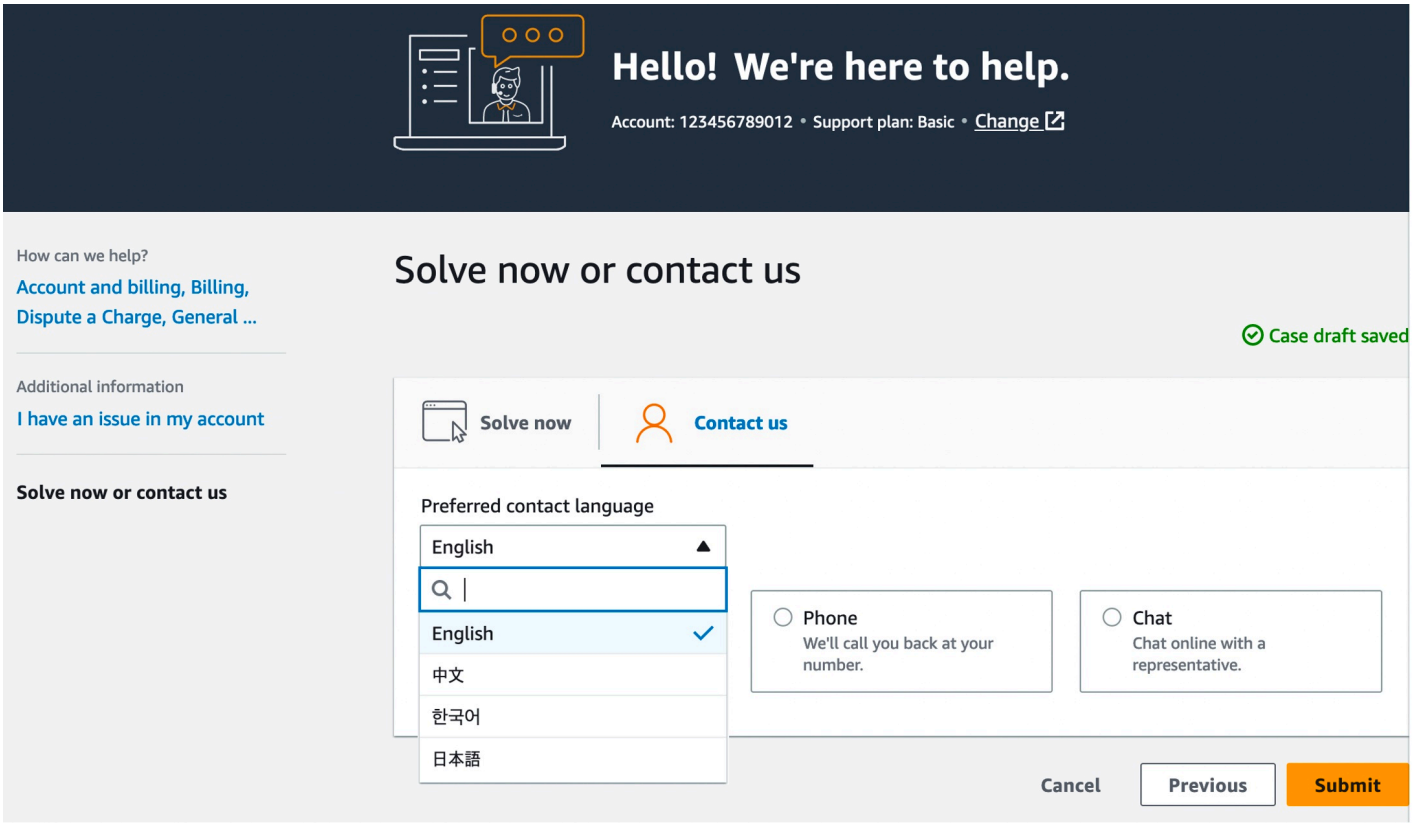
ケースのタイプと分類を指定したら、説明と連絡方法を指定できます。



1. [Subject] (件名) - 問題を簡単に説明するタイトルを入力します。

2. Description – サポートケースについて説明します。これは、提供する最も重要な情報です サポート。一部のサービスとカテゴリの組み合わせでは、関連情報を含むプロンプトが表示されます。これらのリンクを使用して問題を解決してください。詳細については、「問題の説明」を参照してください。
3. [Attachments] (添付) – サポートエージェントがケースを迅速に解決するために役立つスクリーンショットおよびその他のファイルを添付します。最大 3 つまでのファイルをアタッチできます。各ファイルは、最大 5MB まで可能です。

ケースの詳細を追加したら、連絡方法を選択できます。



1. [連絡する際の希望言語] – 使用する言語を選択します。現在、中国語、英語、日本語、韓国語を選択できます。ご希望の言語でカスタマイズされた連絡先オプションがサポートプランに表示されます。
2. 連絡方法を選択します。連絡先オプションは、ケースのタイプとサポートプランによって異なります。
   - [Web] (ウェブ) を選択した場合、サポートセンターでケースの進行状況を確認して返信することができます。

- チャットまたは電話を選択します。[Phone (電話)] を選択した場合、折り返し電話番号の入力が求められます。

3. 入力が完了し、ケースを作成する準備ができたら、[Submit (送信)] ボタンをクリックします。

> **Note**
>
> サポートケースに連絡する際の希望言語として、日本語を選択した場合、以下のサポートを日本語でご利用いただけます。
>
> - テクニカルサポート以外のケースでカスタマーサービスが必要な場合や、デベロッパーサポートプランに加入していてテクニカルサポートが必要な場合は、祝日と週末を除き、日本標準時間の午前 9:00 から午後 6:00 (GMT+9) の営業時間内に、日本語サポートをご利用いただけます。
> - ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートプランをご利用の場合は、年中無休 24 時間体制で日本語のテクニカルサポートにアクセスできます。
>
> サポートケースに連絡する際の希望言語に中国語を選択した場合は、以下のように中国語サポートを受けられます。
>
> - テクニカルサポート以外のサポートケースでのカスタマーサービスが必要な場合は、祝日と週末を除き、午前 9:00から午後 6:00 (GMT+8) まで中国語サポートをご利用いただけます。
> - デベロッパーサポートプランに加入している場合、中国語でのテクニカルサポートは、通常、[アカウント] で設定されているご自身の国での、休日と週末を除く午前 8:00 から午後 6:00 までの営業時間内にご利用いただけます。タイムゾーンが複数ある国/地域では、営業時間が変わる可能性があります。
> - Business、Enterprise On-Ramp、または Enterprise サポートプランをご利用の場合は、年中無休 24 時間体制で中国語のテクニカルサポートが利用できます。
>
> サポートケースで希望言語として韓国語を選択している場合、以下のように韓国語でのサポートをご利用いただけます。
>
> - テクニカルサポート以外のケースでカスタマーサービスが必要な場合、休日と週末を除き、韓国標準時間 (GMT+9) の午前 9:00 から午後 6:00 までの営業時間内に、韓国語でのサポートをご利用いただけます。

- デベロッパーサポートプランに加入している場合、韓国語でのテクニカルサポートは、通常、[アカウント] で設定されているご自身の国での、休日と週末を除く午前 8:00 から午後 6:00 までの営業時間内にご利用いただけます。タイムゾーンが複数ある国/地域では、営業時間が変わる可能性があります。
- Business、Enterprise On-Ramp、または Enterprise サポートプランをご利用の場合は、年中無休 24 時間体制で韓国語語のテクニカルサポートを受けられます。

トラブルシューティング

サポートケースの作成または管理に問題がある場合は、次のトラブルシューティングに関する情報を参照してください。

自分のケースのライブチャットを再開したい

既存のサポートケースに返信して、別のチャットウィンドウを開くことができます。詳細については、「既存のサポートケースの更新」を参照してください。

ライブチャットに接続できない

[Chat] (チャット) オプションを選択したが、チャットウィンドウに接続できない場合は、最初に次のチェックを実行します。

- サポートセンターでポップアップウィンドウを許可するようにブラウザが設定されているようにしてください。

> **Note**
>
> ブラウザの設定を確認します。詳細については、Chrome Help および Firefox Support のウェブサイトを参照してください。

- AWS サポートを使用できるよう、ネットワークが設定されているようにしてください。
  - ネットワークは `*.connect.us-east-1.amazonaws.com` エンドポイントにアクセスできます。

> **Note**
>
> の場合 AWS GovCloud (US)、エンドポイントは です`*.connect-fips.us-east-1.amazonaws.com`。

- ご利用のファイアウォールはウェブソケット接続をサポートしています。

それでもチャットウィンドウに接続できない場合は、E メールまたは電話の連絡先オプション AWS サポート を使用して にお問い合わせください。

Service Quotas の引き上げの作成

サービスのパフォーマンスを向上させるために、Service Quotas (以前は制限と呼ばれていました) の引き上げをリクエストします。

> **Note**
>
> Service Quotas サービスを使用して、サービスの上限緩和を直接リクエストすることもできます。現在、Service Quotas はすべてのサービスの Service Quotas はサポートしていません。詳細については、「Service Quotas ユーザーガイド」の「Service Quotas とは」を参照してください。

Service Quotas の引き上げをリクエストするサポートケースを作成するには

1. AWS Support Center Consoleにサインインします。

   > **Tip**
   >
   > では AWS Management Console、疑問符アイコン
   > ( )
   > を選択してから、サポートセンターを選択することもできます。

2. [ケースを作成] を選択します。
3. サービス制限の増加をお探しですか? を選択する

4. 引き上げをリクエストするには、プロンプトに従います。選択可能なオプションは以下のとおりです。

   - [制限のタイプ]
   - 重要度

   > **Note**
   > カテゴリの選択に基づいて、プロンプトで追加情報の入力を求められることがあります。

5. [Requests] (リクエスト) で、[Region] (リージョン) を選択します。
6. [Limit] (制限) で、サービスの制限のタイプを選択します。
7. [New limit value] (新しい制限値) に、希望する値を入力します。
8. (オプション) 別のの引き上げをリクエストするには、[Add another request] (別のリクエストを追加) を選択します。
9. [Case description] (ケースの説明) で、サポートケースについて説明してください。
10. [Contact options] (連絡先のオプション) ページで、希望する言語と連絡方法を選択します。次のオプションのいずれかを選択します。

    - ウェブ – Support Center で返信を受け取ります。
    - チャット – サポート担当者とライブチャットを開始します。チャットに接続できない場合は、「トラブルシューティング」を参照してください。
    - Phone (電話) — サポートエージェントが電話をかけます。このオプションを選択した場合は、次の情報を入力します。
      - 国/リージョン
      - Phone number (電話番号)
      - (オプション) 拡張
11. [送信] を選択します。ケース ID 番号と概要が表示されます。

ケースの更新、解決、および再開

サポートケースを作成した後、ケースのステータスをサポートセンターでモニタリングできます。新しいケースは、[未割り当て] 状態で開始されます。サポート担当者がケースの対応を開始すると、ステータスは [作業中] に変わります。サポート担当者は、お客様に追加情報を求めるか (お客様による

アクション保留中)、ケースが調査中であることをお客様にお知らせします (保留中の Amazon アクション)。

ケースが更新されると、通知とサポートセンター内のケースへのリンクが記載された E メールがお客様に送信されます。E メールメッセージ内のリンクを使用して、サポートケースに移動します。ケースの通信文にメールで返信することはできません。

> **メモ**
>
> - サポートケースを送信 AWS アカウント した にサインインする必要があります。 AWS Identity and Access Management (IAM) ユーザーとしてサインインする場合は、サポートケースを表示するために必要なアクセス許可が必要です。詳細については、「AWS サポート センターへのアクセスを管理する」を参照してください。
> - 数日以内にケースに応答しない場合、 はケースを自動的に AWS サポート 解決します。
> - 14 日以上解決済みの状態になったサポートケースは、再度開くことができなくなります。解決済みのケースに関連する同様の問題がある場合は、関連するケースを作成できます。詳細については、「関連ケースの作成」を参照してください。

トピック

既存のサポートケースの更新

ケースを更新して、サポートエージェントにより多くの情報を提供できます。例えば、やり取りに返信したり、別のライブチャットを開始したり、メール受信者をさらに追加したりできます。ただし、作成後にケースの重大度を更新することはできません。詳細については、「緊急度の選択」を参照してください。

既存のサポートケースを更新するには

1. AWS Support Center Consoleにサインインします。

> **Tip**
>
> では AWS Management Console、疑問符アイコン
> ()
> を選択してから、サポートセンターを選択することもできます。

2. [Open support cases] (サポートケースを開く) で、サポートケースの [Subject] (件名) を選択します。
3. [Reply] (返信) を選択します。[Correspondence] (コレスポンデンス) セクションでは、次のいずれかの変更を行うこともできます。
   - サポートエージェントがリクエストした情報を提供する
   - 添付ファイルをアップロードする
   - 希望する連絡方法を変更する
   - メールアドレスを追加してケースの更新情報を受け取る
4. [送信] を選択します。

> **Tip**
>
> チャットウィンドウを閉じて、別のライブチャットを開始する場合は、サポートケースに [Reply] (返信) を追加し、[Chat] (チャット)、[Submit] (送信) の順に選択します。新しいポップアップチャットウィンドウが開きます。

サポートケースの解決

対応に満足した場合、または問題が解決した場合は、サポートセンターでケースを解決できます。

サポートケースを解決するには

1. AWS Support Center Consoleにサインインします。

> **Tip**
>
> では AWS Management Console、疑問符アイコン
> ()
> を選択してから、サポートセンターを選択することもできます。

2. [Open support cases] (サポートケースを開く) で、解決するサポートケースの件名 (Subject) を選択します。
3. (オプション) [Reply] (返信) を選択し、[Correspondence] (通信文) セクションでケースを解決する理由を入力して、[Submit] (送信) を選択します。例えば、将来、この情報が必要になった場合に備えて、問題を解決した方法を入力します。
4. [Resolve case] (ケースを解決) を選択します。
5. ダイアログボックスで [OK] を選択してケースを解決します。

> **Note**
>
> ケースが AWS サポート 解決したら、フィードバックリンクを使用して、 エクスペリエンスに関する詳細情報を提供できます AWS サポート。

Example : フィードバックリンク

次のスクリーンショットは、サポートセンターのケースの通信文に関するフィードバックリンクを示しています。

Please let us know if we helped resolve your issue:

If YES, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes

If NO, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No

解決済みのケースを再度開く

同じ問題が再び発生した場合は、元のケースを再度開くことができます。問題が再発した時期と、試行したトラブルシューティング手順の詳細を提供します。サポート担当者が以前の対応情報を参照できるように、関連するケース番号をすべて含めます。

> **メモ**
>
> - 再度開くことができるのは、問題が解決されてから 14 日以内のサポートケースです。ただし、14 日以上非アクティブなケースを再度開くことはできません。新しいケースまたは関連するケースを作成できます。詳細については、「関連ケースの作成」を参照してください。
> - 現在の問題とは異なる情報を持つ既存のケースを再度開いた場合、サポート担当者が新しいケースを作成するよう依頼することがあります。

解決済みのケースを再度開くには

1. AWS Support Center Consoleにサインインします。

   > **Tip**
   >
   > では AWS Management Console、疑問符アイコン
   > ()
   > を選択してから、サポートセンターを選択することもできます。

2. [View all cases] (すべてのケースを表示) を選択して、再度開くサポートケースの件名 (Subject) またはケース ID (Case ID) を選択します。
3. [Reopen case] (ケースを再度開く) を選択します。
4. [Correspondence] (通信文) の [Reply] (返信) にケースの詳細を入力します。
5. (オプション) [Choose files] (ファイルを選択) を選択して、ケースにファイルをアタッチします。最大 3 つのファイルをアタッチできます。
6. [Contact methods] (連絡方法) で次のいずれかのオプションを選択します。
   - Web (ウェブ) — 電子メールとサポートセンターで通知を受け取ります。
   - Chat (チャット) — オンラインでサポート担当者とチャットします。

- Phone (電話) — サポートエージェントが電話をかけます。

7. (オプション) [Additional contacts] (追加の連絡先) にケースの対応情報を受信する他のユーザーのメールアドレスを入力します。
8. ケースの詳細を確認して、[Submit] (送信) を選択します。

関連ケースの作成

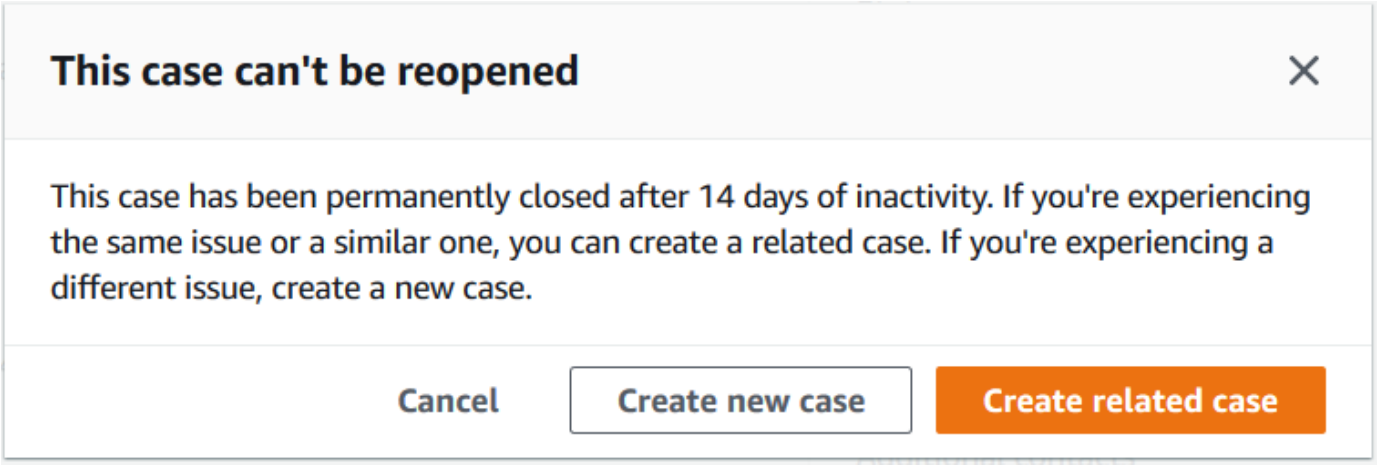
14日間非アクティブな状態の解決済みケースを再度開くことはできません。解決済みのケースに関連する同様の問題がある場合は、関連するケースを作成できます。この関連するケースには、サポート担当者が以前のケースの詳細と対応を確認できるように、以前に解決したケースへのリンクが含まれます。別の問題が発生する場合は、新しいケースを作成することをお勧めします。

関連するケースを作成するには

1. AWS Support Center Consoleにサインインします。

> **Tip**
>
> では AWS Management Console、疑問符アイコン
> ()
> を選択してから、サポートセンターを選択することもできます。

2. [View all cases] (すべてのケースを表示) を選択して、再度開くサポートケースの件名 (Subject) またはケース ID (Case ID) を選択します。
3. [Reopen case] (ケースを再度開く) を選択します。
4. ダイアログボックスで [Create related case] (関連するケースを作成) を選択します。する関連ケースに以前のケース情報が自動的に追加されます。別の問題がある場合は、[Create new case] (新しいケースを作成) を選択します。

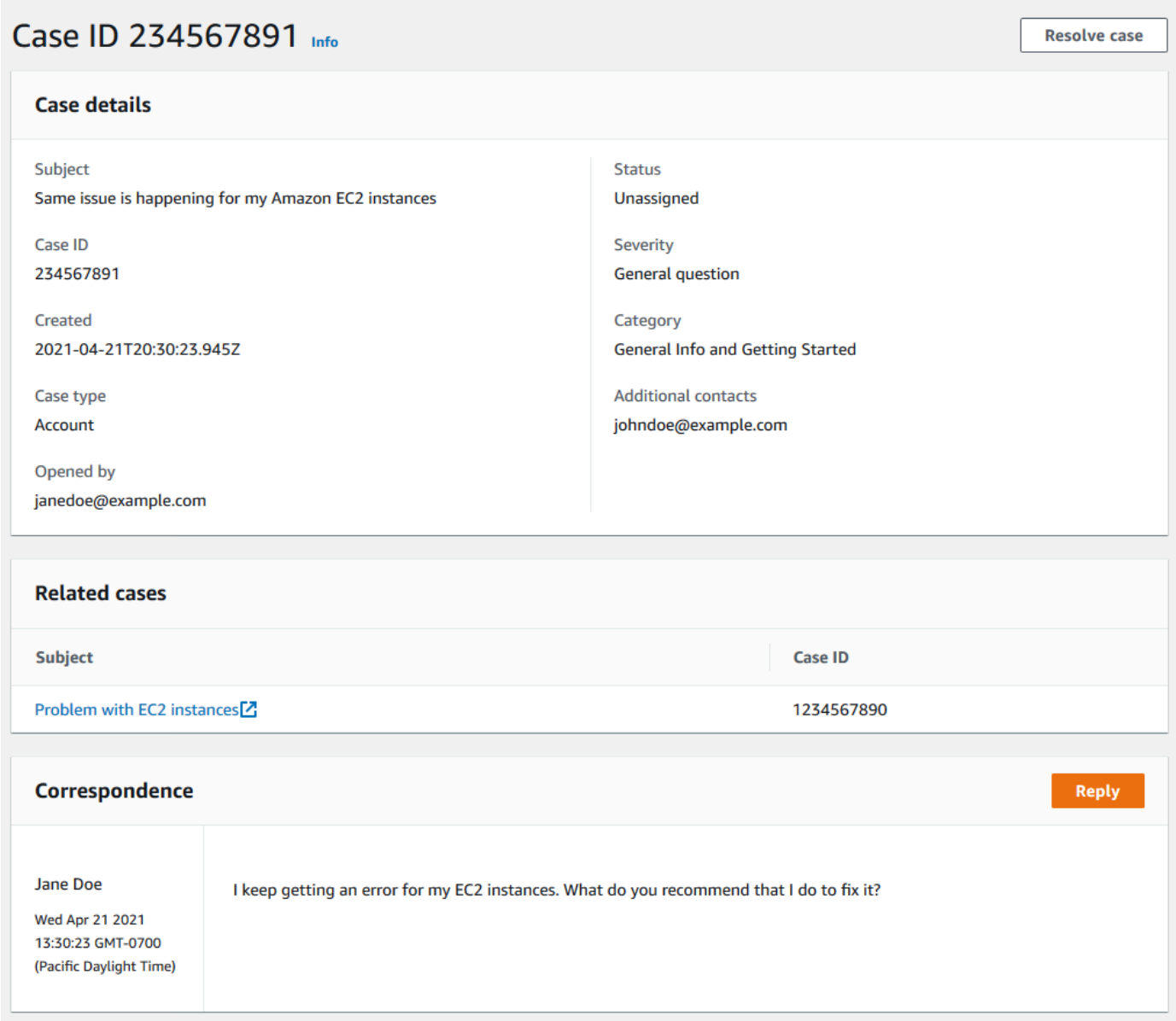


5. ケースを作成するステップに従います。「サポートケースの作成」を参照してください。

> **Note**
>
> デフォルトでは、関連するケースの [Type] (タイプ)、[Category] (カテゴリ)、および [Severity] (重要度) は前のケースと同じになります。必要に応じてケースの詳細を更新できます。

6. ケースの詳細を確認して、[Submit] (送信) を選択します。

   ケースを作成すると、次の例のように前のケースが [Related cases] (関連するケース) セクションに表示されます。



ケース履歴

ケース履歴情報は、ケースを作成した後、最大 24 か月後まで表示できます。

AWS サポート 推奨事項

> **Note**
>
> AWS サポート レコメンデーションは、サービス条件で定義されている「プレビュー AWS サービス」として提供されます。プレビューサービスは変更およびキャンセルされる可能性があります。詳細はこちら。

AWS サポート レコメンデーションでは、 AWS サポート センターコンソールでケース作成フロー中にアカウントと技術的な問題に対するトラブルシューティング支援をパーソナライズできます。AWS サポート レコメンデーションは、ケースの詳細とログインしたアカウントに依存して、問題を解決するためのカスタマイズされたソリューションで応答します。

問題を分析するために、 AWS サポート Recommendations は、承認されたポリシー/ユーザーのアクセス許可の範囲内で、AccountID、 AWS リソース識別子、エラーメッセージなどの情報をクエリします。詳細はこちら。

トピック

- AWS サポート 推奨事項へのアクセスを管理する
- AWS サポート 推奨事項のモニタリングと口グ記録

AWS サポート 推奨事項へのアクセスを管理する

> **Note**
>
> AWS サポート レコメンデーションは、サービス条件で定義されている「プレビュー AWS サービス」として提供されます。プレビューサービスは変更およびキャンセルされる可能性があります。詳細はこちら。

AWS Identity and Access Management (IAM) を使用して、ケース作成フロー中に AWS サポート Center コンソールで AWS サポート Recommendations へのアクセスを管理できます。

トピック

- AWS サポート レコメンデーションアクション
- AWS サポート 推奨事項の IAM ポリシーの例

AWS サポート レコメンデーションアクション

IAM ポリシーで AWS サポート Recommendations アクションを指定して、フルアクセスを提供したり、フルアクセスを拒否したり、特定のアクションへのアクセスを提供/拒否したりできます。

[アクション]	説明
`StartSupportTroubleshooting`	ガイド付きトラブルシューティングセッションを開始して、 AWS サポート センターコンソールでケース作成フロー中にアカウントまたは技術的な問題の診断と解決に役立てます。
`GetSupportTroubleshootingResponse`	StartSupportTroubleshooting で開始されたトラブルシューティングセッションから、現在の状態と出力を取得します。以前のレスポンスに基づいて問題を解決するための詳細情報と推奨事項を求めるインタラクティブなリクエストが含まれています。

AWS サポート 推奨事項の IAM ポリシーの例

次のポリシー例を使用して、 AWS サポート レコメンデーションへのアクセスを管理できます。

AWS サポート 推奨事項へのフルアクセス

次のポリシーでは、ユーザーに AWS サポート Recommendations へのフルアクセスを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportrecommendations:StartSupportTroubleshooting",
                "supportrecommendations:GetSupportTroubleshootingResponse"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS サポート Recommendations へのアクセスを拒否する

次のポリシーでは、ユーザーに AWS サポート Recommendations へのアクセスを許可していません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportrecommendations:*",
            "Resource": "*"
        }
    ]
}
```

AWS サポート 推奨事項のモニタリングとログ記録

> **Note**
>
> AWS サポート レコメンデーションは、サービス条件で定義されている「プレビュー AWS サービス」として提供されます。プレビューサービスは変更およびキャンセルされる可能性があります。詳細はこちら。

モニタリングは、 AWS サポート Recommendations およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 AWS サポート 推奨事項を監視し、問題が発生した場合は報告し、必要に応じて自動アクションを実行するために、次のモニタリングツール AWS を提供します。

- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

- を使用した AWS サポート Recommendations 呼び出しの口グ記録 AWS CloudTrail

を使用した AWS サポート Recommendations 呼び出しのログ記録 AWS CloudTrail

> **Note**
>
> AWS サポート レコメンデーションは、サービス条件で定義されている「プレビュー AWS サービス」として提供されます。プレビューサービスは変更およびキャンセルされる可能性があります。詳細はこちら。

AWS サポート レコメンデーションは、ユーザー AWS CloudTrail、ロール、または サービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、AWS サポート レコメンデーションの API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、 AWS サポート センターコンソールからの呼び出しと、 AWS サポート レコメンデーションへのコード呼び出しが含まれます。

証跡を作成する場合は、レ AWS サポート コメンデーションのイベントなど、Amazon Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。

CloudTrail によって収集された情報を使用して、 AWS サポート Recommendations に対して行われたリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

AWS サポート CloudTrail の推奨事項情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。サポートされるイベントアクティビティが AWS サポート Recommendations で発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「Viewing events with CloudTrail event history」(CloudTrail イベント履歴でのイベントの表示) を参照してください。

AWS サポート レコメンデーションのイベントなど、 AWS アカウント内のイベントの継続的な記録については、証跡を作成します。証跡により、ログファイルを CloudTrail で 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、すべての AWS リージョンに証跡が適用されます。証跡は、 AWS パーティション内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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail ログファイルを複数のリージョンから受け取ると複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS サポート 推奨事項呼び出しは CloudTrail によってログに記録されます。各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- 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 エレメント」を参照してください。

また、複数の AWS リージョンと複数の AWS アカウントからの AWS サポート Recommendations 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。

AWS サポート Recommendations ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail ログファイルには、1 つ以上のログエントリがあります。イベント は、任意の送信元からの単一の要求を表します。これには、リクエストされたオペレーション、オペレーションの日時、リクエストパラメーターなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Example : **`StartSupportTroubleshooting`** のログエントリ

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "StartSupportTroubleshooting",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "message": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : **GetSupportTroubleshootingResponse** のログエントリ

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    },
```

```
    "eventTime": "2023-09-11T16:34:13Z",
    "eventSource": "supportrecommendations.amazonaws.com",
    "eventName": "GetSupportTroubleshootingResponse",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "conversationId": "..."
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


AWS SDK AWS サポート での の使用

AWS Software Development Kit (SDKsは、多くの一般的なプログラミング言語で使用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようにする API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コード例
AWS SDK for C++	AWS SDK for C++ コード例
AWS CLI	AWS CLI コード例
AWS SDK for Go	AWS SDK for Go コード例
AWS SDK for Java	AWS SDK for Java コード例
AWS SDK for JavaScript	AWS SDK for JavaScript コード例
AWS SDK for Kotlin	AWS SDK for Kotlin コード例
AWS SDK for .NET	AWS SDK for .NET コード例

SDK ドキュメント	コード例
AWS SDK for PHP	AWS SDK for PHP コード例
AWS Tools for PowerShell	Tools for PowerShell のコード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コード例
AWS SDK for Ruby	AWS SDK for Ruby コード例
AWS SDK for Rust	AWS SDK for Rust コード例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コード例
AWS SDK for Swift	AWS SDK for Swift コード例

可用性の例

必要なものが見つからなかった場合。このページの下側にある [Provide feedback (フィードバックを送信)] リンクから、コードの例をリクエストしてください。

AWS サポート API について

AWS サポート API は、 AWS サポートセンターの一部の機能へのアクセスを提供します。

API は、オペレーションの 2 つのグループを提供します。

- 作成から解決までの AWS サポートケースのライフサイクル全体を管理する サポートケース管理 オペレーション
- AWS Trusted Advisor チェックにアクセスする AWS Trusted Advisor オペレーション

> **Note**
>
> AWS サポート API を使用するには、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が必要です。詳細については、「サポート」を参照してください。

が提供するオペレーションとデータ型の詳細については サポート、 AWS サポート API リファレンスを参照してください。

トピック

- サポートケース管理
- AWS Trusted Advisor
- エンドポイント
- AWS SDKsでのサポート

サポートケース管理

API を使用して、次のタスクを実行できます。

- サポートケースを開く
- 最近のサポートケースに関する詳細情報と一覧を取得する
- 日付やケース ID でサポートケースをフィルターする (解決積みのケースを含む)。
- ケースに通信文やファイル添付を追加し、ケースの通信にメール受信者を追加する。最大 3 つまでのファイルをアタッチできます。各ファイルは、最大 5MB まで可能

- ケースを解決する

AWS サポート API は、サポートケース管理オペレーションの CloudTrail ログ記録をサポートします。詳細については、「を使用した AWS サポート API コールのログ記録 AWS CloudTrail」を参照してください。

サポートケースのライフサイクル全体を管理する方法を示すコード例については、「SDK サポートを使用するコード例 AWS SDKs」を参照してください。

AWS Trusted Advisor

Trusted Advisor オペレーションを使用して、次のタスクを実行できます。

- Trusted Advisor チェックの名前と識別子を取得する
- AWS アカウントとリソースに対して Trusted Advisor チェックを実行するようにリクエストする
- Trusted Advisor チェック結果の概要と詳細情報を取得する
- Trusted Advisor チェックを更新する
- 各 Trusted Advisor チェックのステータスを取得する

AWS サポート API は、 Trusted Advisor オペレーションの CloudTrail ログ記録をサポートします。詳細については、「AWS Trusted Advisor CloudTrail ログ記録の情報」を参照してください。

Amazon CloudWatch Events を使用して、 Trusted Advisorのチェック結果に対する変更をモニタリングできます。詳細については、「Amazon EventBridge による AWS Trusted Advisor チェック結果のモニタリング」を参照してください。

Trusted Advisor オペレーションの使用方法を示す Java コードの例については、「」を参照してくださいウェブサービス Trusted Advisor としての の使用。

エンドポイント

サポート はグローバルサービスです。これは、使用するすべてのエンドポイントで、サポートセンターコンソールのサポートケースが更新されることを意味します。

例えば、米国東部 (バージニア北部) エンドポイントを使用してケースを作成する場合、米国西部 (オレゴン) または欧州 (アイルランド) エンドポイントを使用して同じケースへのコレスポンデンスを追加できます。

サポート API には次のエンドポイントを使用できます。

- 米国東部 (バージニア北部) – https://support.us-east-1.amazonaws.com
- 米国西部 (オレゴン) – https://support.us-west-2.amazonaws.com
- 欧州 (アイルランド) – https://support.eu-west-1.amazonaws.com

> **Important**
>
> - CreateCase オペレーションを呼び出してテストサポートケースを作成する場合は、TEST CASE- Please ignore などの件名を含めることをお勧めします。テストサポートケースが完了したら、ResolveCase 操作を呼び出してケースを解決します。
> - AWS サポート API で AWS Trusted Advisor オペレーションを呼び出すには、米国東部 (バージニア北部) エンドポイントを使用する必要があります。現在、米国西部 (オレゴン) および欧州 (アイルランド) エンドポイントは Trusted Advisor オペレーションをサポートしていません。

AWS エンドポイントの詳細については、「」のAWS サポート 「 エンドポイントとクォータ」を参照してくださいAmazon Web Services 全般のリファレンス。

AWS SDKsでのサポート

AWS Command Line Interface （ AWS CLI ）、および AWS Software Development Kit (SDKsには、サポート API のサポートが含まれています。

AWS サポート API をサポートする言語のリストについては、CreateCase などのオペレーション名を選択し、https://docs.aws.amazon.com/awssupport/latest/APIReference/API_CreateCase.html#API_CreateCase_SeeAlso「」セクションで任意の言語を選択します。

AWS サポート プラン

ビジネスニーズに基づいて、アカウントの AWS サポート プランを変更できます。

トピック

AWS サポート プランの機能

サポート には、次の 5 つのサポートプランがあります。

- ベーシック
- 開発者
- ビジネス
- Enterprise On-Ramp
- Enterprise

ベーシックプランでは、アカウントと請求に関するご質問、サービスクォータの緩和に関するサポートが提供されます。その他のプランでは、多くの技術サポートケースを利用できます。サポート料金の支払いは月単位で、長期契約は不要です。

すべての AWS お客様は、ベーシックサポートの以下の機能に 24 時間 365 日自動的にアクセスできます。

- アカウントと請求に関するご質問に 1 対 1 で回答
- サポートフォーラム
- サービス状態チェック
- ドキュメント、技術文書、およびベストプラクティスガイド

Developer Support プランのお客様は、以下の追加機能にアクセスできます。

- ベストプラクティスのガイダンス
- クライアント側の診断ツール

- ビルディングブロックアーキテクチャのサポート: AWS 製品、機能、サービスを一緒に使用する方法に関するガイダンス
- アクセス許可を持つ任意のユーザーが開くことができるサポートケースを無制限にサポートします。

Business、Enterprise On-Ramp、または Enterprise Support プランのお客様は、さらにこれらの機能にアクセスできます。

- ユースケースガイダンス – 特定のニーズを最適にサポートするために使用する AWS 製品、機能、サービス。
- AWS Trusted Advisor – の機能。お客様の環境を検査し サポート、コスト削減、セキュリティギャップの解消、システムの信頼性とパフォーマンスの向上の機会を特定します。すべての Trusted Advisor チェックにアクセスできます。
- サポートセンターおよび とやり取りするための AWS サポート API Trusted Advisor。 AWS サポート API を使用して、サポートケースの管理と Trusted Advisor オペレーションを自動化できます。
- サードパーティーのソフトウェアサポート - Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのオペレーティングシステムと設定を支援します。また、最も人気のあるサードパーティー製ソフトウェアコンポーネントのパフォーマンスもサポートします AWS。サードパーティー製ソフトウェアのサポートは、Basic または Developer Support プランのお客様にはご利用いただけません。
- テクニカルサポートケースを開くことができる AWS Identity and Access Management (IAM) ユーザーを無制限にサポートします。

Enterprise On-Ramp または Enterprise Support プランのお客様は、さらにこれらの機能にアクセスできます。

- アプリケーションアーキテクチャガイダンス - 特定のユースケース、ワークロード、またはアプリケーションに適合するサービスの組み合わせに関する助言的なガイダンス。
- インフラストラクチャのイベント管理 - AWS サポート との短期の取り組みでお客様のユースケースの理解を深めます。分析後、イベントに関するアーキテクチャとスケーリングのガイダンスを提供します。
- テクニカルアカウントマネージャー - テクニカルアカウントマネージャー (TAM) と連携して、特定のユースケースやアプリケーションに対応します。
- ホワイトグローブケースルーティング

- 管理ビジネス評価。

各サポートプランの機能と料金の詳細については、AWS サポート「」およびAWS サポート 「プランの比較」を参照してください。24 時間の電話とチャットによるサポートなど、すべての言語で使用できない機能もあります。

> **Note**
>
> AWS パートナーと連携し、パートナー主導のサポートの詳細については、AWS Partner「-Led Support」を参照してください。

AWS サポート プランの変更

AWS サポート プランコンソールを使用して、 のサポートプランを変更できます AWS アカウント。サポートプランを変更するには、 AWS Identity and Access Management (IAM) アクセス許可を持っているか、ルートユーザーとしてアカウントにサインインする必要があります。詳細については、AWS サポート プランへのアクセスを管理するおよびAWSAWS サポート プランの マネージドポリシーを参照してください。

サポートプランを変更するには

1. https://console.aws.amazon.com/support/plans/home の AWS サポート プランコンソールにサインインします。
2. (オプション) [AWS サポート プラン] ページでサポートプランを比較できます。料金の詳細については、料金ページを参照してください。
3. (オプション) [AWS サポート 料金の例] で、[See examples] (例を見る) を選択し、サポートプランのオプションのいずれかを選択すると、推定コストをご覧いただけます。
4. プランを決めたら、希望するプランの [Review downgrade] (ダウングレードを確認する) または [Review upgrade] (アップグレードを確認する) を選択します。

> **メモ**
>
> - 有料のサポートプランにサインアップする場合は、 AWS サポートを 1 か月以上サブスクライブする必要があります。詳細については、「AWS サポート のよくある質問」を参照してください。

- Enterprise On-Ramp またはエンタープライズサポートプランをご利用の場合は、[Change plan confirmation] (変更プランの確認) ダイアログボックスから サポート へ連絡して、サポートプランを変更します。

5. [Change plan confirmation] (変更プランの確認) ダイアログボックスでサポート項目を展開すると、アカウントで追加または削除される機能を確認できます。

   [Pricing] (料金) では、新しいサポートプランの、予定されている 1 回限りの請求を確認できます。

6. [Accept and agree] (承諾して同意する) を選択します。

関連情報

AWS サポート プランの詳細については、AWS サポート FAQsを参照してください。サポートプランのコンソールの [Contact us] (お問い合わせ) もご利用ください。

アカウントを解約するには、AWS Billing ユーザーガイドの「アカウントの解約」を参照してください。

AWS Trusted Advisor

Trusted Advisor は、数十万の AWS お客様にサービスを提供することから学んだベストプラクティスを活用しています。 Trusted Advisor はお客様の AWS 環境を検査し、コスト削減、システムの可用性とパフォーマンスの向上、セキュリティギャップの解消に役立つ機会があれば、レコメンデーションを行います。

ベーシックサポートプランまたはデベロッパーサポートプランをお持ちの場合は、 Trusted Advisor コンソールを使用して、サービス制限カテゴリのすべてのチェックとセキュリティカテゴリの 5 つのチェックにアクセスできます。

Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合は、 Trusted Advisor コンソールと AWS Trusted Advisor API を使用してすべての Trusted Advisor チェックにアクセスできます。Amazon CloudWatch Events を使用して、 Trusted Advisor チェックのステータスをモニタリングすることもできます。詳細については、「Amazon EventBridge による AWS Trusted Advisor チェック結果のモニタリング」を参照してください。

Trusted Advisor で にアクセスできます AWS Management Console。 Trusted Advisor コンソールへのアクセスの制御の詳細については、「」を参照してくださいへのアクセスを管理する AWS Trusted Advisor。

詳細については、「Trusted Advisor」を参照してください。

トピック

- Trusted Advisor Recommendations の開始方法
- Trusted Advisor API の使用を開始する
- ウェブサービス Trusted Advisor としての の使用
- の組織ビュー AWS Trusted Advisor
- による AWS Trusted Advisor チェックの表示 AWS Config
- での AWS Security Hub コントロールの表示 AWS Trusted Advisor
- チェック AWS Compute Optimizer に Trusted Advisor オプトインする
- AWS Trusted Advisor Priority の使用を開始する
- AWS Trusted Advisor Engage の使用を開始する (プレビュー)
- AWS Trusted Advisor チェックリファレンス
- の変更ログ AWS Trusted Advisor

Trusted Advisor Recommendations の開始方法

Trusted Advisor コンソールの Trusted Advisor レコメンデーションページを使用して のチェック結果を確認し AWS アカウント 、推奨される手順に従って問題を解決できます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなどの未使用のリソースを削除して毎月の請求を削減することが Trusted Advisor で推奨されることがあります。

AWS Trusted Advisor API を使用して、 Trusted Advisor チェックに対してオペレーションを実行することもできます。詳細については、「AWS Trusted Advisor API リファレンス」を参照

トピック

Trusted Advisor コンソールにサインインする

Trusted Advisor コンソールで、チェックと各チェックのステータスを表示できます。

> **Note**
>
> Trusted Advisor コンソールにアクセスするには AWS Identity and Access Management 、(IAM) アクセス許可が必要です。詳細については、「へのアクセスを管理する AWS Trusted Advisor」を参照してください。

Trusted Advisor コンソールにサインインするには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。

2. [Trusted Advisor Recommendations] ページに、各チェックカテゴリの概要が表示されます。

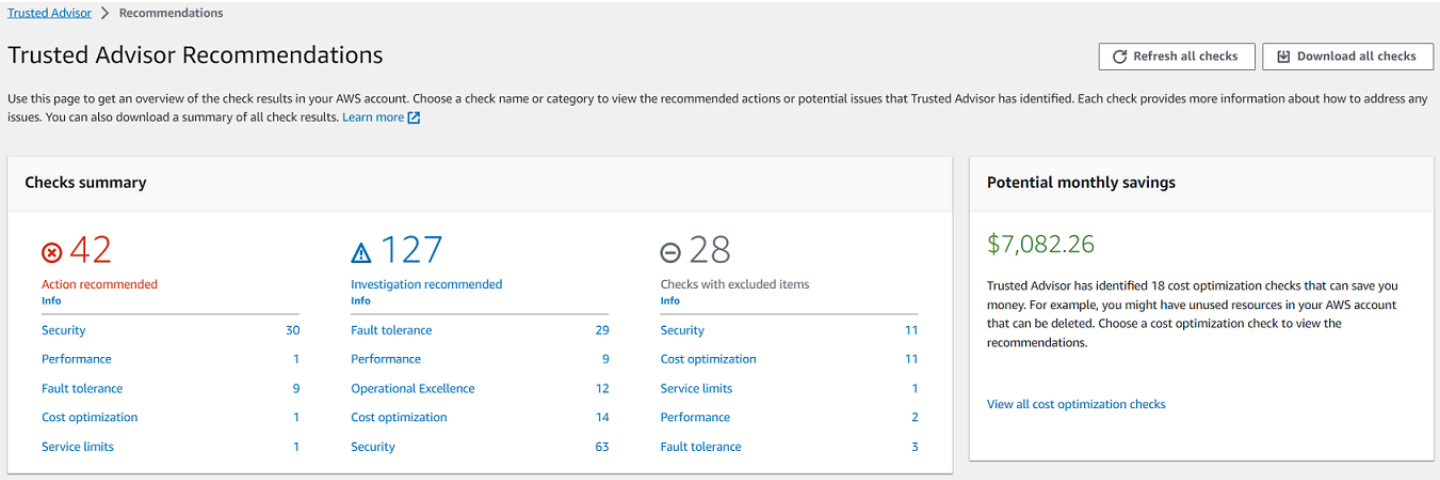
   - 推奨アクション (赤) – Trusted Advisor チェックのアクションを推奨します。例えば、IAM リソースのセキュリティの問題を検出するチェックでは、緊急のステップが推奨されることがあります。
   - [調査が推奨されるチェック項目 (黄色)] – Trusted Advisor は、チェックの潜在的な問題を検出します。例えば、リソースのクォータに達したチェックでは、未使用のリソースを削除する方法が推奨されることがあります。
   - 非表示の項目のチェック (グレー) - チェックで無視するリソースなどの除外する項目があるチェックの数。例えば、チェックで評価しない Amazon EC2 インスタンスなどです。

3. [Trusted Advisor Recommendations] ページでは、以下の操作を行えます。

   - アカウントのすべてのチェックを更新するには、[すべてのチェックを更新] を選択します。
   - すべてのチェック結果を含む .xls ファイルを作成するには、[すべてのチェックをダウンロード] を選択します。
   - [Checks summary] (チェックの概要) でチェックカテゴリ ([Security] (セキュリティ) など) を選択して結果を表示します。
   - [月額料金節約の可能性] には、アカウントで節約できる金額とレコメンデーションのコスト最適化チェックが表示されます。
   - [Recent changes] (最近の変化) では、過去 30 日以内のチェックステータスの変化を表示できます。チェック名を選択してそのチェックの最新の結果を表示するか、矢印アイコンを選択して次のページを表示します。

Example : Trusted Advisor 推奨事項

次の例は、 AWS アカウントのチェック結果のサマリーを示しています。



チェックカテゴリの表示

次のチェックカテゴリのチェックの説明と結果を表示できます。

- Cost optimization (コスト最適化) — 節約可能な金額のレコメンデーション。これらのチェックでは、未使用のリソースと請求を削減する機会がハイライトされます。
- パフォーマンス — アプリケーションのスピードと応答性を向上させるためのレコメンデーション。
- セキュリティ — AWS ソリューションのセキュリティを強化するセキュリティ設定に関する推奨事項。
- 耐障害性 – AWS ソリューションの耐障害性を高めるのに役立つ推奨事項。これらのチェックでは、冗長性の欠落や過度に使用されたリソースがハイライトされます。
- Service limits (サービスの制限) — アカウントの使用状況、およびアカウントが AWS のサービスとリソースの制限 (クォータとも呼ばれます) に近づいているか制限を超えているかをチェックします。
- 運用上の優秀性 – AWS 環境を効果的かつ大規模に運用するための推奨事項。

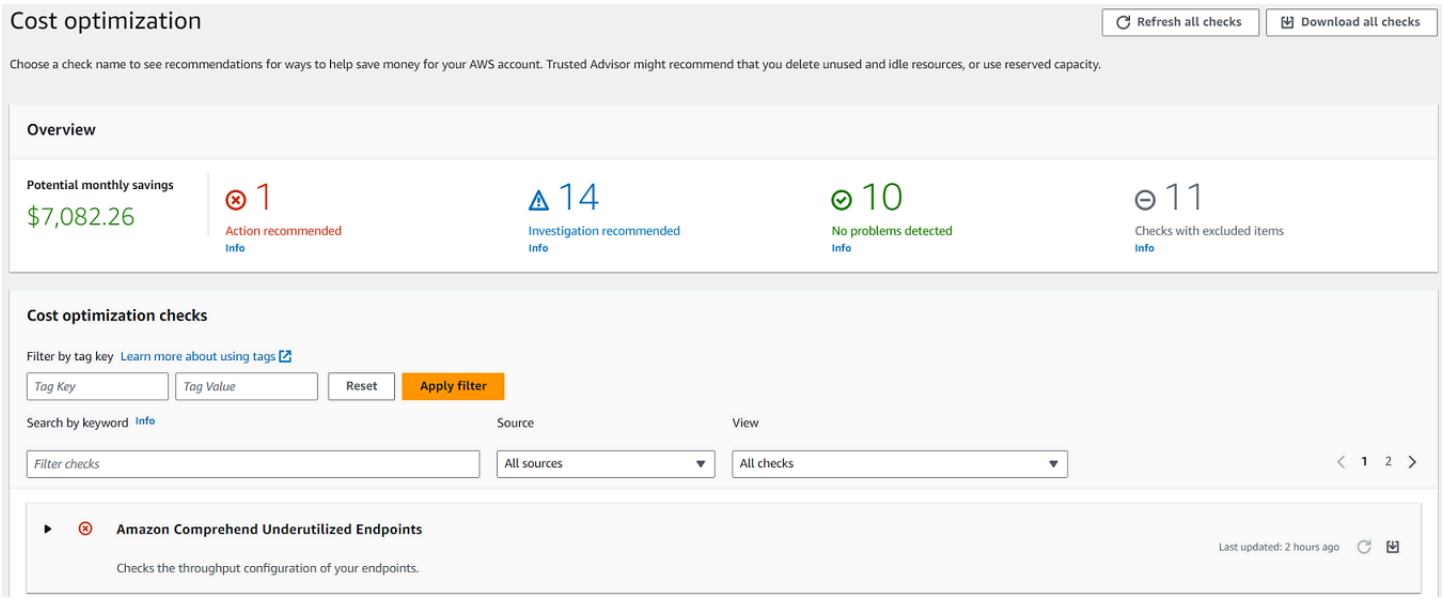
チェックカテゴリを表示するには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインで目的のチェックカテゴリを選択します。
3. カテゴリページには、各チェックカテゴリの概要が表示されます。
   - 推奨アクション (赤) – Trusted Advisor チェックのアクションを推奨します。
   - [調査が推奨されるチェック項目 (黄色)] – Trusted Advisor は、チェックの潜在的な問題を検出します。
   - 問題が検出されない (緑) – チェックの問題は検出されません。 Trusted Advisor
   - [非表示の項目 (グレー)] — チェックで無視するリソースなど、除外項目があるチェックの数。
4. 各チェックで、更新アイコン
   ()
   をクリックして、そのチェックを更新します。

5. ダウンロードアイコン
   ( )
   を使用して、そのチェックの結果を含む .xls ファイルを作成します。

Example : コスト最適化カテゴリ

次の例は、問題のない 10 (グリーン) チェックを示しています。



特定のチェックの表示

チェックを展開すると、チェックの完全な説明、影響を受けるリソース、推奨されるステップ、および詳細情報へのリンクが表示されます。

特定のチェックを表示するには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインで目的のチェックカテゴリを選択します。
3. チェック名を選択して、説明と次の詳細を表示します。

   - アラート基準 — チェックのステータスが変更されるときのしきい値を示します。
   - 推奨されるアクション — そのチェックの推奨アクションを示します。
   - 追加のリソース — 関連 AWS ドキュメントを一覧表示します。

- アカウント内の影響を受ける項目の表。チェック結果にこれらの項目を含めるか、除外することができます。

4. (オプション) チェック結果に表示されないように項目を除外するには:

   a. 項目を選択し、[非表示 & 更新] を選択します。

   b. 除外されたすべての項目を表示するには、[非表示の項目] を選択します。

5. (オプション) チェックで再度評価されるように項目を含めるには:

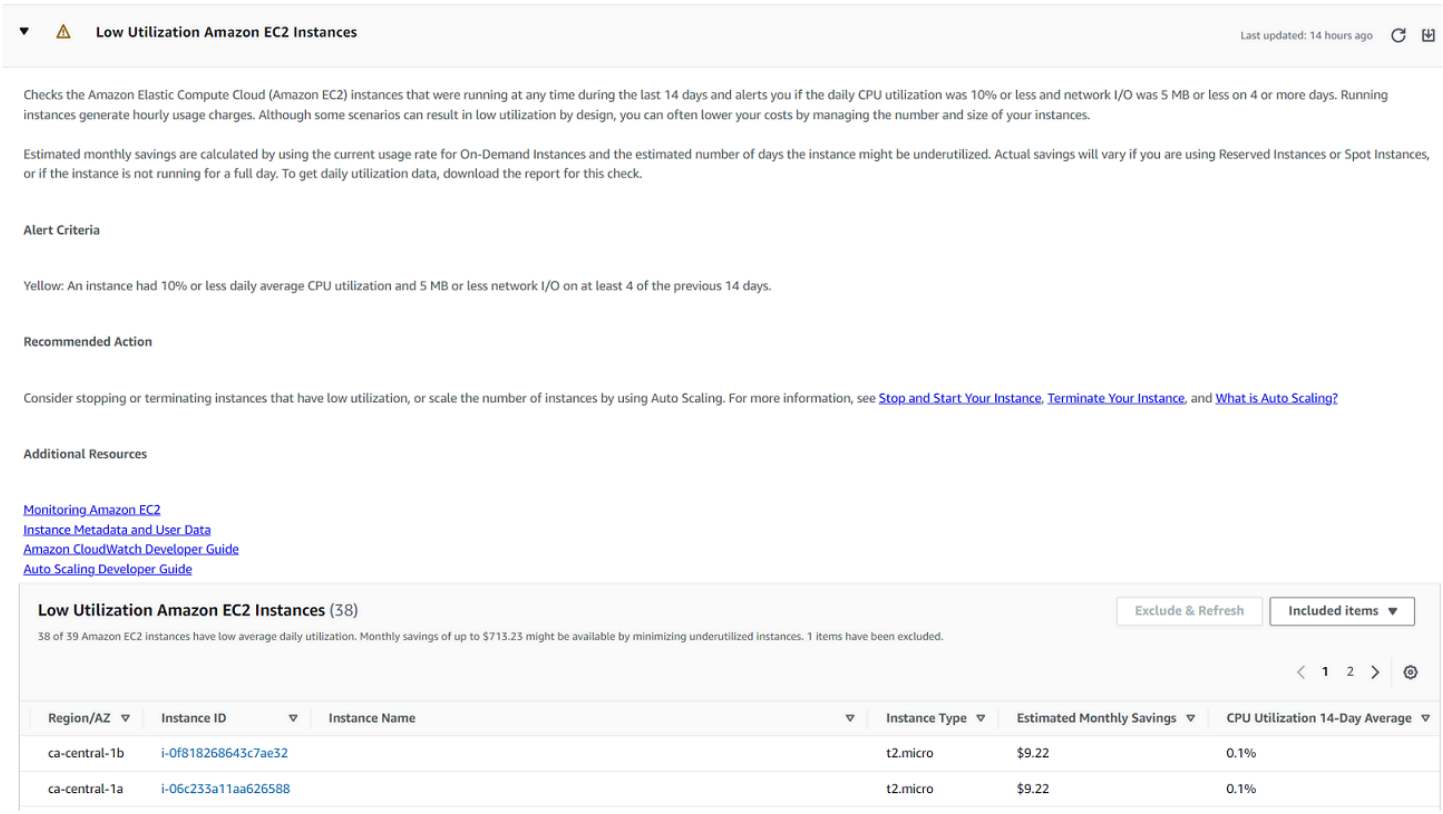
   a. [非表示の項目] を選択し、項目を選択して [表示 & 更新] を選択します。

   b. すべての含まれる項目を表示するには、[表示可能な項目] を選択します。

6. 設定アイコン
   ()
   を選択します。[Preferences] (通知設定) ダイアログボックスでは、表示する項目の数またはプロパティを指定し、[Confirm] (確認) を選択します。

Example : コスト最適化チェック

次の [使用率の低い Amazon EC2 Instances] チェックは、アカウント内の影響を受けるインスタンスを一覧表示します。このチェックでは、使用率が低い 38 の Amazon EC2 インスタンスが識別され、リソースを停止または終了することが推奨されています。



チェックのフィルター

チェックカテゴリページでは、表示するチェック結果を指定できます。例えば、アカウントのエラーを検出したチェックをフィルターして、緊急の問題を最初に調査することができます。

AWS リソースなど、アカウント内の項目を評価するチェックがある場合は、タグフィルターを使用して、指定されたタグを持つ項目のみを表示できます。

チェックをフィルターするには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインまたは [Trusted Advisor Recommendations] ページで、チェックカテゴリを選択します。
3. [Search by keyword] (キーワードによる検索) 場合は、チェック名や説明文からキーワードを入力し、検索結果をフィルターします。
4. [表示] リストで、表示するチェックを指定します。

   - [All checks] (全てのチェック項目) - このカテゴリのすべてのチェックが一覧表示されます。

- 推奨されるアクション — アクションの実行が推奨されるチェックが一覧表示されます。これらのチェックは赤色でハイライトされます。
- 調査が推奨されるチェック項目 — 可能なアクションの実行が推奨されるチェックが一覧表示されます。これらのチェックは黄色でハイライトされます。
- 問題は検出されませんでした — 問題のないチェックが一覧表示されます。これらのチェックは緑色でハイライトされます。
- 非表示の項目を含むチェック — チェック結果から項目を除外するよう指定したチェックが一覧表示されます。

5. Amazon EC2 インスタンスや AWS CloudTrail 証跡などの AWS リソースにタグを追加した場合は、指定したタグを持つ項目のみをチェックに表示するように結果をフィルタリングできます。

   [タグでフィルター] にタグキーと値を入力して [フィルターを適用] を選択します。
6. チェックのテーブルでは、チェック結果には、指定されたキーと値を持つ項目のみが表示されます。
7. タグによるフィルターをクリアするには、[リセット] を選択します。

関連情報

のタグ付けの詳細については Trusted Advisor、以下のトピックを参照してください。

- AWS サポート でタグ付け機能を有効にする Trusted Advisor
- 「AWS 全般のリファレンス」の「AWS リソースのタグ付け」

チェック結果の更新

チェックを更新して、アカウントの最新の結果を取得できます。デベロッパーまたはベーシックサポートプランをお持ちの場合は、 Trusted Advisor コンソールにサインインしてチェックを更新できます。Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合、 はアカウント内のチェックを毎週 Trusted Advisor 自動的に更新します。

Trusted Advisor チェックを更新するには

1. https://console.aws.amazon.com/trustedadvisor で AWS Trusted Advisor コンソールに移動します。
2. Trusted Advisor レコメンデーションまたはチェックカテゴリページで、すべてのチェックの更新を選択します。

次の方法で特定のチェックを更新することもできます。

- 目的のチェックの更新アイコン
  ()
  を選択します。
- RefreshTrustedAdvisorCheck API オペレーションを使用します。

> **メモ**
>
> - Trusted Advisor は、AWS Well-Architected信頼性チェックの高リスクの問題など、1 日に数回、一部のチェックを自動的に更新します。アカウントに変更が表示されるまでに数時間かかる場合があります。自動更新されるチェックについては、最新表示アイコン
>   ()
>   を選択して結果を手動で更新することはできません。
> - アカウント AWS Security Hub で を有効にした場合、 Trusted Advisor コンソールを使用して Security Hub コントロールを更新することはできません。詳細については、「Security Hub の調査結果を更新する」を参照してください。

結果のダウンロード

チェック結果をダウンロードして、アカウント Trusted Advisor 内の の概要を取得できます。すべてのチェックまたは特定のチェックの結果をダウンロードできます。

Trusted Advisor Recommendations からチェック結果をダウンロードするには

1. https://console.aws.amazon.com/trustedadvisor で AWS Trusted Advisor コンソールに移動します。
   - すべてのチェック結果をダウンロードするには、[Trusted Advisor Recommendations] または [Check category] (チェックカテゴリー) ページで、[Download all checks] (すべてのチェックをダウンロード) を選択します。
   - 特定のチェックのチェック結果をダウンロードするには、チェック名を選択し、ダウンロードアイコン
     ()
     を選択します。

2. .xls ファイルを保存するか、開きます。このファイルには、 Trusted Advisor コンソールと同じサマリー情報 (チェック名、説明、ステータス、影響を受けるリソースなど) が含まれます。

組織ビュー

組織ビュー機能を設定して、 AWS 組織内のすべてのメンバーアカウントのレポートを作成できます。詳細については、「の組織ビュー AWS Trusted Advisor」を参照してください。

詳細設定

[Trusted Advisorの管理] ページで、Trusted Advisorを無効化できます。

Notifications ページで、チェックサマリーの毎週の E メールメッセージを設定できます。「通知設定の設定」を参照してください。

組織ページで、信頼されたアクセスを有効または無効にできます AWS Organizations。これは「の組織ビュー AWS Trusted Advisor」の機能、Trusted Advisor Priority、および Trusted Advisor Engage のために必須です。

通知設定の設定

チェック結果の毎週の Trusted Advisor E メールメッセージを受信できるユーザーと言語を指定します。 Trusted Advisor 推奨事項のチェック概要に関する E メール通知が週に 1 回届きます。

Trusted Advisor レコメンデーションの E メール通知には、 Trusted Advisor Priority の結果は含まれません。詳細については、「Trusted Advisor Priority 通知の管理」を参照してください。

通知設定をセットアップするには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインの [Preferences] (設定) で、[Notifications] (通知) を選択します。
3. [Recommendations] (レコメンデーション) で、チェック結果の通知先を選択します。 AWS Billing and Cost Management コンソールのアカウント設定ページから連絡先を追加または削除できます。
4. [言語] で E メールメッセージの言語を選択します。
5. [Save your preferences] (詳細設定を保存) を選択します。

組織ビューのセットアップ

アカウントを でセットアップすると AWS Organizations、組織内のすべてのメンバーアカウントのレポートを作成できます。詳細については、「の組織ビュー AWS Trusted Advisor」を参照してください。

無効 Trusted Advisor

このサービスを無効にすると、 はアカウントでチェックを実行 Trusted Advisor しません。 Trusted Advisor コンソールにアクセスしようとしたり、 API オペレーションを使用したりしようとすると、アクセス拒否のエラーメッセージが表示されます。

を無効にするには Trusted Advisor

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインの [設定]で [Trusted Advisorを管理]を選択します。
3. [Trusted Advisor] で、[Enabled] (有効) をオフにします。このアクションにより、アカウント内のすべてのチェック Trusted Advisor が無効になります。
4. その後、アカウントから AWSServiceRoleForTrustedAdvisor を手動で削除できます。詳細については、「Trusted Advisorのサービスリンクロールの削除」を参照してください。

関連情報

詳細については Trusted Advisor、以下のトピックを参照してください。

- の使用を開始するにはどうすればよいですか Trusted Advisor？
- AWS Trusted Advisor チェックリファレンス

Trusted Advisor API の使用を開始する

AWS Trusted Advisor API リファレンスは、API オペレーションとデータ型に関する詳細情報を必要とするプログラマーを対象としています Trusted Advisor 。この API は、 アカウントまたは AWS Organization 内のすべてのアカウントの Trusted Advisor レコメンデーションへのアクセスを提供します。 Trusted Advisor API は、結果を JSON 形式で返す HTTP メソッドを使用します。

> **Note**
>
> - Trusted Advisor API を使用するには、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 Trusted Advisor API を呼び出すと、アクセス拒否例外が発生します。サポートプランの変更の詳細については、AWS 「 サポート」を参照してください。

AWS Trusted Advisor API を使用して、チェックのリストとその説明、レコメンデーション、およびレコメンデーションのリソースを取得できます。また、推奨事項のライフサイクルを更新することもできます。推奨事項を管理するには、以下の API オペレーションを使用します。

- ListChecks、LestRecommendations、GetRecommendation、ListRecommendationResources API オペレーションを使用して、推奨事項とそれに対応するアカウントやリソースを表示します。
- UpdateRecommendationLifecycle API オペレーションを使用して、 Trusted Advisor Priority によって管理されるレコメンデーションのライフサイクルを更新します。
- BatchUpdateRecommendationResourceExclusion API オペレーションを使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外します。
- ListOrganizationRecommendations、GetOrganizationRecommendation、ListOrganizationRecommendatio および UpdateOrganizationRecommendationLifecycle API コールは、 Trusted Advisor Priority によって管理されるレコメンデーションのみをサポートします。これらの推奨事項は優先推奨事項とも呼ばれます。Trusted Advisor Priority を有効にしている場合は、管理者アカウントまたは委任管理者アカウントから、優先順位を付けた推奨事項を表示および管理できます。Priority が有効になっていない場合、リクエストを行うとアクセス拒否の例外が表示されます。

詳細については、AWS 「 サポートユーザーガイド AWS Trusted Advisor 」の「」を参照してください。

リクエストの認証については、「署名バージョン 4 の署名プロセス」を参照してください。

ウェブサービス Trusted Advisor としての の使用

この AWS サポート サービスを使用すると、 とやり取りするアプリケーションを作成できますAWS Trusted Advisor。このトピックでは、 Trusted Advisor チェックのリストを取得して更新し、チェッ

クから詳細な結果を取得する方法を示します。これには、Java を使用します。他の言語のサポートに関する情報については、アマゾン ウェブ サービスのツールを参照してください。

トピック

- 利用可能な Trusted Advisor チェックのリストを取得する
- 利用可能な Trusted Advisor チェックのリストを更新する
- ステータス変更の Trusted Advisor チェックをポーリングする
- Trusted Advisor チェック結果をリクエストする
- Trusted Advisor チェックの詳細を表示する

利用可能な Trusted Advisor チェックのリストを取得する

次の Java コードスニペットは、すべての Trusted Advisor API オペレーションを呼び出すために使用できる サポート クライアントのインスタンスを作成します。次に、DescribeTrustedAdvisorChecks API オペレーションを呼び出して、コードは Trusted Advisor チェックのリストとそれに対応するCheckId値を取得します。この情報を使って、チェックを実行するか更新するかをユーザーが選択できるユーザーインターフェイスを構築できます。

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

利用可能な Trusted Advisor チェックのリストを更新する

次の Java コードスニペットは、 Trusted Advisor データの更新に使用できる サポート クライアントのインスタンスを作成します。

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

ステータス変更の Trusted Advisor チェックをポーリングする

Trusted Advisor チェックを実行して最新のステータスデータを生成するリクエストを送信したら、DescribeTrustedAdvisorCheckRefreshStatuses API オペレーションを使用して、チェックの実行の進行状況と、新しいデータでチェックの準備ができたタイミングをリクエストします。

次の Java コードスニペットは、`CheckId` 変数内の対応する値を使用して、次のセクションで要求したチェックのステータスを取得します。さらに、このコードは、 Trusted Advisor サービスの他のいくつかの使用方法を示しています。

1. `getMillisUntilNextRefreshable` の呼び出しは、`DescribeTrustedAdvisorCheckRefreshStatusesResult` インスタンス内に含まれるオブジェクトをトラバースすることによって実行できます。返された値を使用して、チェックの更新を続けるのにコードが必要かどうかをテストできます。
2. `timeUntilRefreshable` が 0 の場合、チェックの更新を要求できます。
3. 返されたステータスを使って、ステータスの変更のポーリングを続けることができます。このコードスニペットは、ポーリング間隔を推奨値の 10 秒に設定しています。ステータスが `enqueued` または `in_progress` のいずれかの場合、ループは回帰し、他のステータスを要求します。呼び出しによって `successful` が返ってきた場合は、ループは終了します。

4. 最後に、コードは、チェックによって生成された情報をトラバースするために使用できる、DescribeTrustedAdvisorCheckResultResult データ型のインスタンスを返します。

注: リクエストのステータスをポーリングする前に、単一の更新リクエストを使用します。

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new
 DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") ||
 status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh
 status for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId)
 throws InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
```

```
// is only functional for checks that can be refreshed using the
 RefreshTrustedAdvisorCheck operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus()))
 {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may
 not be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

Trusted Advisor チェック結果をリクエストする

目的の詳細結果のチェックを選択したら、DescribeTrustedAdvisorCheckResult API オペレーションを使ってリクエストを送信します。

> **Tip**
>
> Trusted Advisor チェックの名前と説明は変更される可能性があります。チェックを一意に識別するために、コードでチェック ID を指定することをお勧めします。チェック ID を取得するには、DescribeTrustedAdvisorChecks API オペレーションを使用します。

次の Java コードスニペットでは、前のコードスニペットで取得された `result` 変数によって参照される、`DescribeTrustedAdvisorChecksResult` インスタンスを使用します。ユーザーインターフェイスを通じてインタラクティブにチェックを定義する代わりに、このスニペットを実行する要求を送信した後で、`result.getChecks().get(0)` 呼び出しごとに 0 のインデックス値を指定することによってリスト内の最初のチェックを実行する要求を送信します。次に、コードで

は、checkResult と呼ばれる DescribeTrustedAdvisorCheckResultResult のインスタンスに渡す DescribeTrustedAdvisorCheckResultRequest のインスタンスを定義します。チェックの結果を見るには、このデータ型のメンバー構造体を使用します。

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

注： Trusted Advisor チェック結果をリクエストしても、更新された結果データは生成されません。

Trusted Advisor チェックの詳細を表示する

次の Java コードスニペットは、前のセクションで返されたDescribeTrustedAdvisorCheckResultResultインスタンスを反復処理して、 Trusted Advisor チェックによってフラグが付けられたリソースのリストを取得します。

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

の組織ビュー AWS Trusted Advisor

組織ビューでは、 内のすべてのアカウントの Trusted Advisor チェックを表示できますAWS Organizations。この機能を有効にすると、組織内のすべてのメンバーアカウントのチェック結果を集計するレポートを作成できます。このレポートには、チェック結果のサマリー、および各アカウントの影響を受けるリソースに関する情報が含まれます。例えば、レポートを使用して、IAM 使

用チェックで組織内のどのアカウントが AWS Identity and Access Management (IAM) を使用しているか、または Amazon S3 バケットのアクセス許可チェックで Amazon Simple Storage Service (Amazon S3) バケットに推奨アクションがあるかどうかを特定できます。

トピック

前提条件

組織ビューを有効にするには、次の要件を満たす必要があります。

- アカウントは、AWS 組織のメンバーである必要があります。
- 組織で Organizations のすべての機能が有効になっている必要があります。詳細については、AWS Organizations ユーザーガイドの「組織内のすべての機能の有効化」を参照してください。。
- 組織の管理アカウントには、Business、Enterprise On-Ramp、または Enterprise Support プランが必要です。サポートプランは、 AWS サポート センターまたはサポートプランページから確認できます。「AWS サポート サポートのプラン比較」を参照してください。
- 管理アカウント (または同等の継承されたロール) のユーザーとしてサインインする必要があります。IAM ユーザーとしてサインインする場合でも IAM ロールとしてサインインする場合でも、必要なアクセス許可のあるポリシーが必要です。「IAM ポリシーを使用して組織ビューへのアクセスを許可する」を参照してください。

組織ビューを有効にする

前提要件を満たした後、次の手順に従って組織ビューを有効にします。この機能を有効にすると、次の処理が実行されます。

- Trusted Advisor は、組織内で信頼されたサービスとして有効になっています。詳細については、「AWS Organizations ユーザーガイド」の「AWS の他のサービスで信頼されたアクセスを有効にする」 を参照してください。
- `AWSServiceRoleForTrustedAdvisorReporting` サービスリンクロールが組織の管理アカウントに作成されます。このロールには、 がユーザーに代わって Organizations を呼び出す Trusted Advisor ために必要なアクセス許可が含まれています。このサービスリンクロールはロックされているため、手動で削除することはできません。詳細については、「Trusted Advisor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。

Trusted Advisor コンソールから組織ビューを有効にします。

組織ビューを有効にするには

1. 組織の管理アカウントで管理者としてサインインし、https://console.aws.amazon.com/trustedadvisor で AWS Trusted Advisor コンソールを開きます。
2. ナビゲーションペインの [Preferences] (設定) で、[Your organization] (お客様の組織) を選択します。
3. で信頼されたアクセスを有効にする AWS Organizationsで、有効をオンにします。

> **Note**
>
> 管理アカウントの組織ビューを有効にしても、すべてのメンバーアカウントに同じチェックが提供されるわけではありません。例えば、メンバーアカウントすべてにベーシックサポートがついている場合、それらのアカウントは管理アカウントと同じチェックを受けることはできません。 AWS サポート プランは、アカウントで使用できる Trusted Advisor チェック項目を決定します。

Trusted Advisor チェックの更新

組織のレポートを作成する前に、 Trusted Advisor チェックのステータスを更新することをお勧めします。 Trusted Advisor を更新せずにレポートをダウンロードすることができますが、レポートに最新情報が含まれない可能性があります。

Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合、 はアカウント内のチェックを毎週 Trusted Advisor 自動的に更新します。

> **Note**
>
> デベロッパーサポートプランまたはベーシックサポートプランを持つアカウントが組織にある場合、それらのアカウントのユーザーは Trusted Advisor コンソールにサインインしてチェックを更新する必要があります。組織の管理アカウントからすべてのアカウントのチェックを更新することはできません。

Trusted Advisor チェックを更新するには

1. https://console.aws.amazon.com/trustedadvisor で AWS Trusted Advisor コンソールに移動します。
2. [Trusted Advisor Recommendations] ページで、[Refresh all checks] (すべてのチェックを更新) を選択します。アカウントのすべてのチェックが更新されます。

次の方法で特定のチェックを更新することもできます。

- RefreshTrustedAdvisorCheck API オペレーションを使用します。
- 目的のチェックの更新アイコン () を選択します。

組織ビューレポートを作成する

組織ビューを有効にした後、レポートを作成して組織の Trusted Advisor チェック結果を表示できます。

最大 50 のレポートを作成できます。このクォータを超えるレポートを作成した場合、以前のレポートが Trusted Advisor によって削除されます。削除されたレポートを復元することはできません。

組織ビューレポートを作成するには

1. 組織の管理アカウントにサインインし、 AWS Trusted Advisor コンソール (https://console.aws.amazon.com/trustedadvisor) を開きます。
2. ナビゲーションペインの [Organizational View] (組織ビュー) を選択します。
3. [レポートを作成] を選択します。

4. デフォルトでは、レポートにはすべての AWS リージョン、チェックカテゴリ、チェック、リソースステータスが含まれます。リポジトリの [Create report] (レポートの作成) ページでは、フィルターオプションを使用してレポートをカスタマイズできます。例えば、[Region] (リージョン) の [All] (すべて) をクリアして、レポートに含める個々のリージョンを指定できます。

   a. レポートの [Name](名前) を入力します。

   b. [Format] で、[JSON] または [CSV] を選択します。

   c. リージョンで、 AWS リージョンを指定するか、すべてを選択します。

   d. [Check category] (チェックカテゴリ) でチェックカテゴリを選択するか、[All] (すべて) を選択します。

   e. [Check] で、そのカテゴリの特定のチェックを選択するか、[All] (すべて) を選択します。

   > **Note**
   >
   > [Check category] (チェックカテゴリ) フィルターは [Check] (チェック) フィルターを上書きします。例えば、[Security] (セキュリティ) カテゴリを選択し、特定のチェック名を選択した場合、レポートには、そのカテゴリのすべてのチェック結果が含まれます。特定のチェックのみのレポートを作成するには、[Check category] (チェックカテゴリ) のデフォルトの [All] (すべて) を選択し、目的のチェック名を選択します。

   f. [Resource status] (リソースのステータス) で、フィルターするステータス ([Warning] など) または [All] (すべて) を選択します。

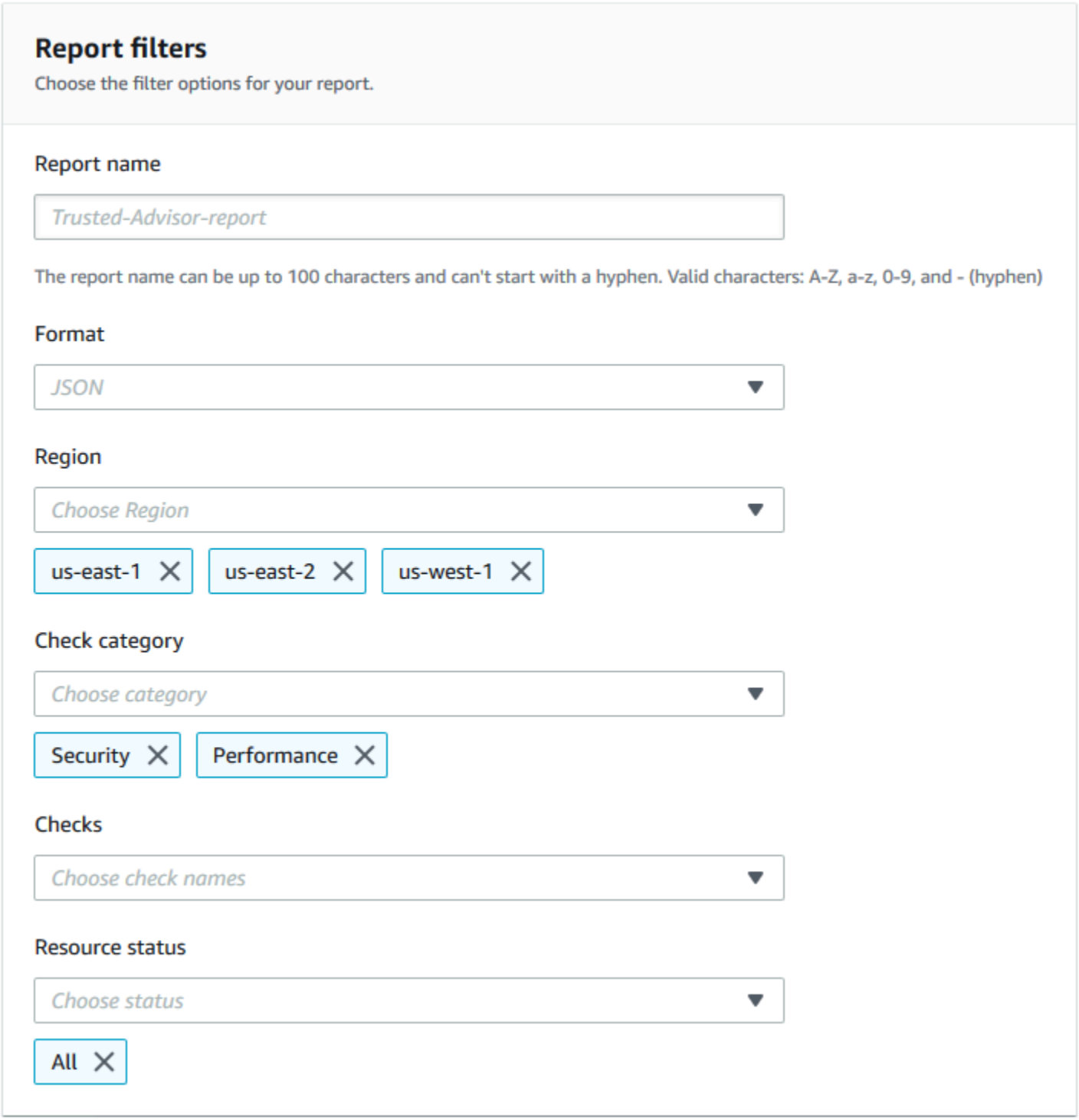
5. [AWS Organization] で、レポートに含める組織単位 (OU) を選択します。OU の詳細については、AWS Organizations ユーザーガイドの「組織単位 (OU) の管理」を参照してください。

6. [レポートを作成] を選択します。

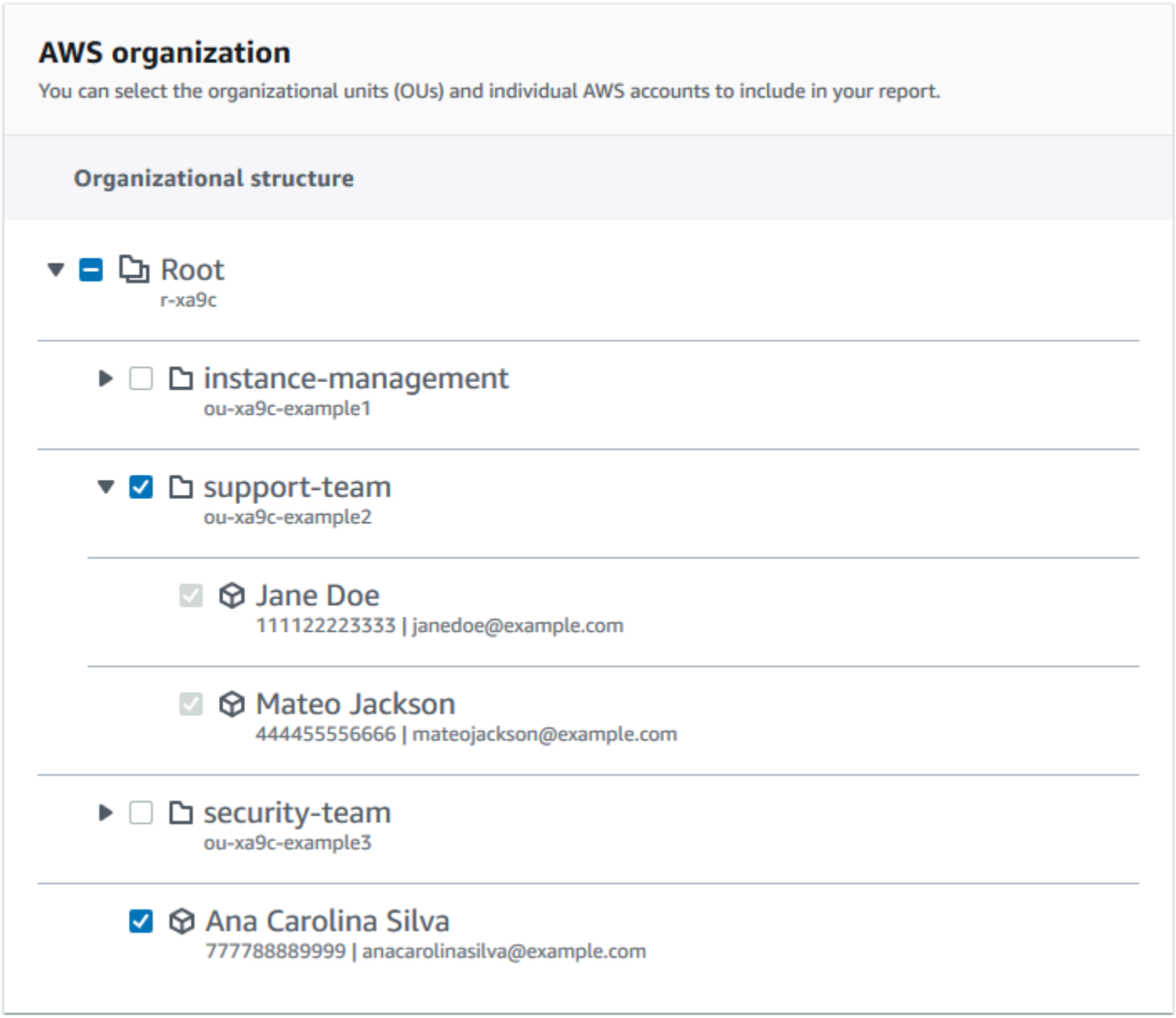
Example : レポートフィルターオプションの作成

次の例は、以下の JSON レポートを作成します。

- 3 つの AWS リージョン
- すべてのセキュリティおよびパフォーマンスチェック



次の例では、レポートに support-team OU と、組織の一部である 1 つの AWS アカウントが含まれています。



メモ

- レポートの作成に要する時間は、組織内のアカウントの数と各アカウントのリソースの数によって異なります。
- 現在のレポートが 6 時間以上実行している場合を除き、複数のレポートを同時に生成することはできません。
- レポートがページに表示されない場合は、ページを更新します。

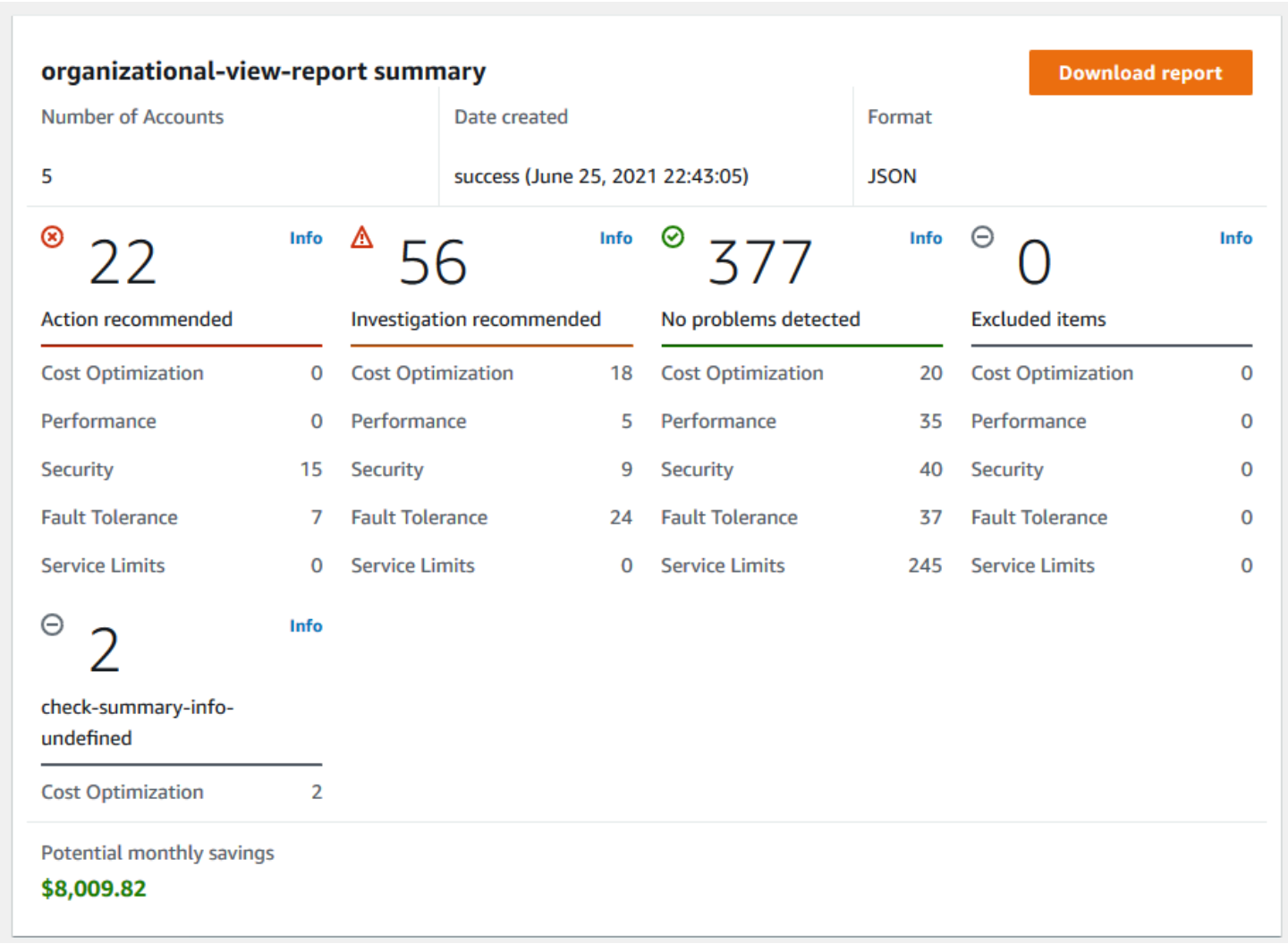
レポートのサマリーの表示

レポートの準備ができたら、 Trusted Advisor コンソールからレポートの概要を表示できます。この機能を使用して、組織全体のチェック結果のサマリーをすばやく表示できます。

レポートのサマリーを表示するには

1. 組織の管理アカウントにサインインし、 AWS Trusted Advisor コンソール (https://console.aws.amazon.com/trustedadvisor) を開きます。
2. ナビゲーションペインの [Organizational View] (組織ビュー) を選択します。
3. レポート名を選択します。
4. [Summary] (サマリー) ページには、各カテゴリのチェックのステータスが表示されます。[Download report] (レポートをダウンロード) を選択することもできます。

Example : 組織のレポートのサマリー



組織ビューレポートをダウンロードする

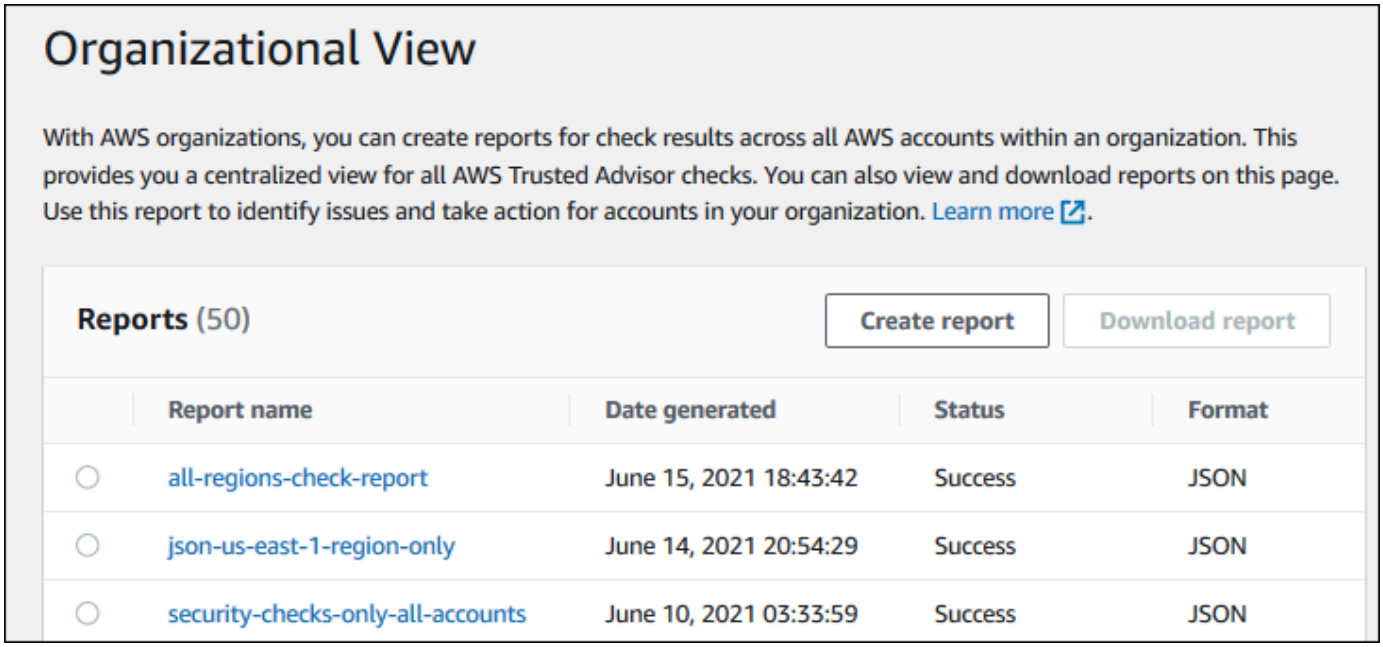
レポートの準備ができたら、 Trusted Advisor コンソールからダウンロードします。レポートは、次の 3 つのファイルを含む .zip ファイルです。

- `summary.json` — 各チェックカテゴリのチェック結果のサマリーが含まれます。
- `schema.json` — レポート内の指定されたチェックのスキーマが含まれます。
- リソースファイル (.json または .csv) — 組織内のリソースのチェックステータスに関する詳細情報が含まれます。

組織ビューレポートをダウンロードするには

1. 組織の管理アカウントにサインインし、 AWS Trusted Advisor コンソール (https://console.aws.amazon.com/trustedadvisor) を開きます。
2. ナビゲーションペインの [Organizational View] (組織ビュー) を選択します。

   組織ビューページに、ダウンロードできるレポートが表示されます。
3. レポートを選択し、[Download report] (レポートをダウンロード) を選択してファイルを保存します。一度にダウンロードできるレポートは 1 つだけです。



4. ファイル を解凍します。
5. テキストエディタを使用して `.json` ファイルを開くか、スプレッドシートアプリケーションを使用して `.csv` ファイルを開きます。

> **Note**
>
> レポートが 5 MB 以上の場合、複数のファイルがダウンロードされることがあります。

Example : summary.json ファイル

`summary.json` ファイルには、組織内のアカウントの数、および各カテゴリのチェックのステータスが表示されます。

Trusted Advisor は、チェック結果に次のカラーコードを使用します。

- Green - Trusted Advisor チェックの問題を検出しません。
- Yellow - チェックで発生する可能性のある問題 Trusted Advisor を検出します。
- Red – エラー Trusted Advisor を検出し、チェックのアクションを推奨します。
- Blue – Trusted Advisor チェックのステータスを判断できません。

次の例では、2 つのチェックが Red で、1 つチェックが Green、そして 1 つのチェックが Yellow です。


```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
```

```
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example : schema.json ファイル

schema.json ファイルには、レポート内のチェックのスキーマが含まれます。次の例には、IAM パスワードポリシー (Yw2K9puPzl) チェックと IAM キーローテーション (DqdJqYeRm5) チェックの ID とプロパティが含まれます。

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
```

```
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example : resources.csv ファイル

resources.csv ファイルには、組織内のリソースに関する情報が含まれます。この例は、次のようなレポートに表示されるデータ列の一部を示します。

- 影響を受けるアカウントのアカウント ID
- Trusted Advisor チェック ID
- リソース ID。
- レポートのタイムスタンプ
- Trusted Advisor チェックのフルネーム
- Trusted Advisor チェックカテゴリ
- 親組織単位 (OU) またはルートのアカウント ID

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5(	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxIBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J(	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

チェック結果がリソースレベルに存在する場合、リソースファイルにはエントリのみが含まれます。次のような理由から、レポートにチェックが表示されない場合があります。

- いくつかのチェック ([ルートアカウントの MFA] など) にはリソースがないので、レポートに表示されません。リソースのないチェックは、summary.json ファイルに含まれます。
- 一部のチェックでは、Red または Yellow の場合にリソースのみが表示されます。すべてのリソースが Green の場合、リソースがレポートに表示されないことがあります。
- チェックが必要なサービスに対してアカウントが有効になっていない場合、チェックがレポートに表示されないことがあります。例えば、組織で Amazon Elastic Compute Cloud リザーブドインスタンスを使用していない場合、[Amazon EC2 リザーブドインスタンスリースの有効期限切れ] チェックはレポートに表示されません。
- アカウントでチェック結果が更新されていません。これは、ベーシックサポートプランまたはデベロッパーサポートプランのユーザーが Trusted Advisor コンソールに初めてサインインした場合に発生する可能性があります。Business、Enterprise On-Ramp、または Enterprise Support プランをご利用の場合は、チェック結果が表示されるまでにアカウントのサインアップから最大で 1 週間かかることがあります。詳細については、「Trusted Advisor チェックの更新」を参照してください。
- 組織の管理アカウントのみでチェックのレコメンデーションが有効な場合、レポートには組織内の他のアカウントのリソースは含まれません。

リソースファイルでは、Microsoft Excel などの一般的なソフトウェアを使用して、.csv ファイル形式を開くことができます。.csv ファイルは、組織内のすべてのアカウントにわたるチェックの 1 回だけの分析に使用できます。レポートをアプリケーションで使用する場合は、.json ファイルとしてレポートをダウンロードできます。

.json ファイル形式は、集約や複数のデータセットを使用した高度な分析などの高度なユースケースで .csv ファイル形式よりも高い柔軟性を提供します。例えば、Amazon Athena などの AWS サービスで SQL インターフェイスを使用して、レポートに対してクエリを実行できます。Amazon QuickSight を使用してダッシュボードを作成し、データを視覚化することもできます。詳細については、「他の AWS サービスを使用した Trusted Advisor レポートの表示」を参照してください。

組織ビューを無効にする

組織ビューを無効にするには、次の手順に従います。この機能を無効にするには、組織の管理アカウントにサインインするか、必要なアクセス許可を持つロールを継承する必要があります。この機能を組織内の別のアカウントから無効にすることはできません。

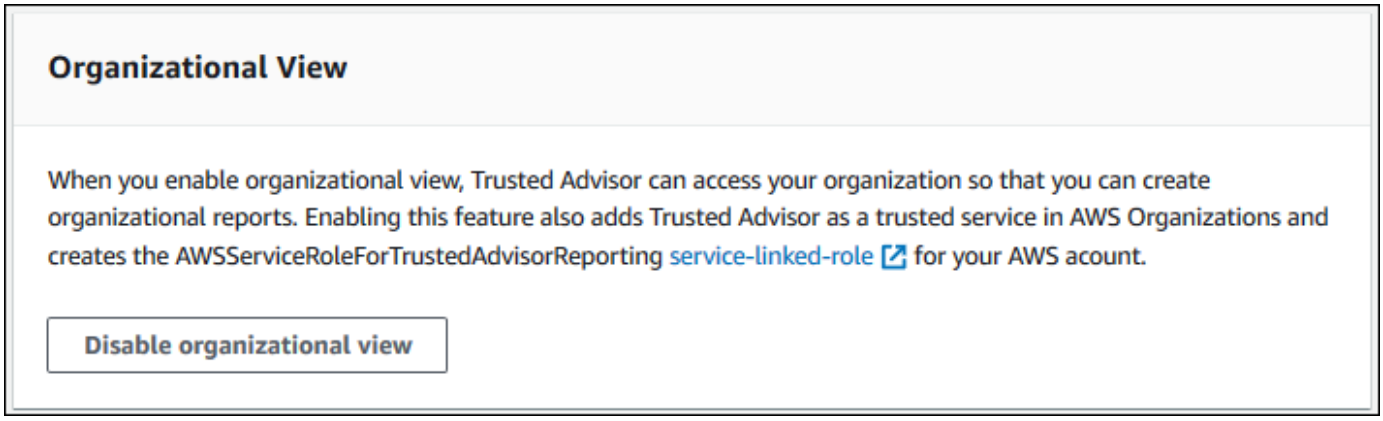
この機能を無効にすると、次の処理が実行されます。

- Trusted Advisor は Organizations で信頼されたサービスとして削除されます。

- AWSServiceRoleForTrustedAdvisorReporting サービスリンクロールのロックが組織の管理アカウントで解除されます。その結果、必要に応じて手動で削除できるようになります。
- 組織のレポートを作成、表示、およびダウンロードすることはできません。以前に作成したレポートにアクセスするには、 Trusted Advisor コンソールから組織ビューを再度有効にする必要があります。「組織ビューを有効にする」を参照してください。

の組織ビューを無効にするには Trusted Advisor

1. 組織の管理アカウントにサインインし、 AWS Trusted Advisor コンソール (https://console.aws.amazon.com/trustedadvisor) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [Organizational View] (組織ビュー) で [Disable organizational view] (組織ビューを無効化) を選択します。



組織ビューを無効にすると、 は組織内の他の AWS アカウントからのチェックを集約 Trusted Advisor しなくなります。ただし、AWSServiceRoleForTrustedAdvisorReportingサービスにリンクされたロールは、IAM コンソール、IAM API、または AWS Command Line Interface () を使用して削除するまで、組織の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。

> **Note**
>
> 他の AWS サービスを使用して、組織ビューレポートのデータをクエリおよび視覚化できます。詳細については、以下のリソースを参照してください。
>
> - AWS Management & Governance ブログ の「View AWS Trusted Advisor recommendations at scale with AWS Organizations」

- 他の AWS サービスを使用した Trusted Advisor レポートの表示

IAM ポリシーを使用して組織ビューへのアクセスを許可する

次の AWS Identity and Access Management (IAM) ポリシーを使用して、アカウントのユーザーまたはロールに の組織ビューへのアクセスを許可できます AWS Trusted Advisor。

Example : 組織ビューへのフルアクセス

次のポリシーは、組織ビュー機能へのフルアクセスを許可します。これらのアクセス許可が付与されているユーザーは、次のことを行うことができます。

- 組織ビューを有効または無効にする
- レポートを作成、表示、およびダウンロードする。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example : 組織ビューへの読み取りアクセス

次のポリシーでは、 の組織ビューへの読み取り専用アクセスを許可します Trusted Advisor。これらのアクセス許可を持つユーザーは、既存のレポートを表示およびダウンロードできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
```

```
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

独自の IAM ポリシーを作成することもできます。詳細については、IAM ユーザーガイド の「IAM ポリシーの作成」を参照してください。

> **Note**
>
> アカウント AWS CloudTrail で を有効にした場合、ログエントリに次のロールが表示されます。
>
> - `AWSServiceRoleForTrustedAdvisorReporting` – が組織内のアカウントにアクセス Trusted Advisor するために使用するサービスにリンクされたロール。
> - `AWSServiceRoleForTrustedAdvisor` – が組織内のサービスにアクセス Trusted Advisor するために使用する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の詳細については、「Trusted Advisor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。

他の AWS サービスを使用した Trusted Advisor レポートの表示

このチュートリアルに従って、他の AWS サービスを使用してデータをアップロードおよび表示します。このトピックでは、レポートを保存する Amazon Simple Storage Service (Amazon S3) バケットと、アカウントにリソースを作成するための AWS CloudFormation テンプレートを作成します。次に、Amazon Athena を使用してレポートに対して分析またはクエリを実行するか、Amazon QuickSight を使用して、そのデータをダッシュボードで視覚化できます。

レポートデータの視覚化の詳細と例については、AWS Management & Governance ブログの「View AWS Trusted Advisor recommendations at scale with AWS Organizations」を参照してください。

前提条件

このチュートリアルを開始する前に、以下の要件を満たす必要があります。

- 管理者権限を持つ AWS Identity and Access Management (IAM) ユーザーとしてサインインします。
- 米国東部 (バージニア北部) AWS リージョンを使用して、 AWS サービスとリソースをすばやくセットアップします。
- Amazon QuickSight アカウントを作成します。詳細については、Amazon QuickSight ユーザーガイド「Amazon QuickSight でのデータ分析の開始方法」を参照してください。

レポートを Amazon S3 にアップロードする

`resources.json` レポートをダウンロードした後、ファイルを Amazon S3 にアップロードします。米国東部 (バージニア北部) リージョンのバケットを使用する必要があります。

Amazon S3 バケットにレポートをアップロードするには

1. https://console.aws.amazon.com/ AWS Management Console で にサインインします。
2. リージョンの選択ツールを使用して [米国東部 (バージニア北部] リージョンを選択します。
3. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
4. バケットの一覧から S3 バケットを選択し、名前をコピーします。この名前は次の手順で使用します。
5. #####のページで、[フォルダの作成] を選択して フォルダ名に「**`folder1`**」と入力して [保存] を選択します。
6. [folder1] を選択します。

7. folder1 で [アップロード] を選択し、`resources.json` ファイルを選択します。
8. [次へ] を選択し、デフォルトのオプションを変更せずに、[アップロード] を選択します。

> **Note**
>
> このバケットに新しいレポートをアップロードする場合は、既存のレポートが上書きされないように `.json` ファイルをアップロードするたびに名前を変更します。例えば、各ファイルにタイムスタンプ (`resources-timestamp.json`、`resources-timestamp2.json` など) を追加できます。

AWS CloudFormationを使用してリソースを作成する

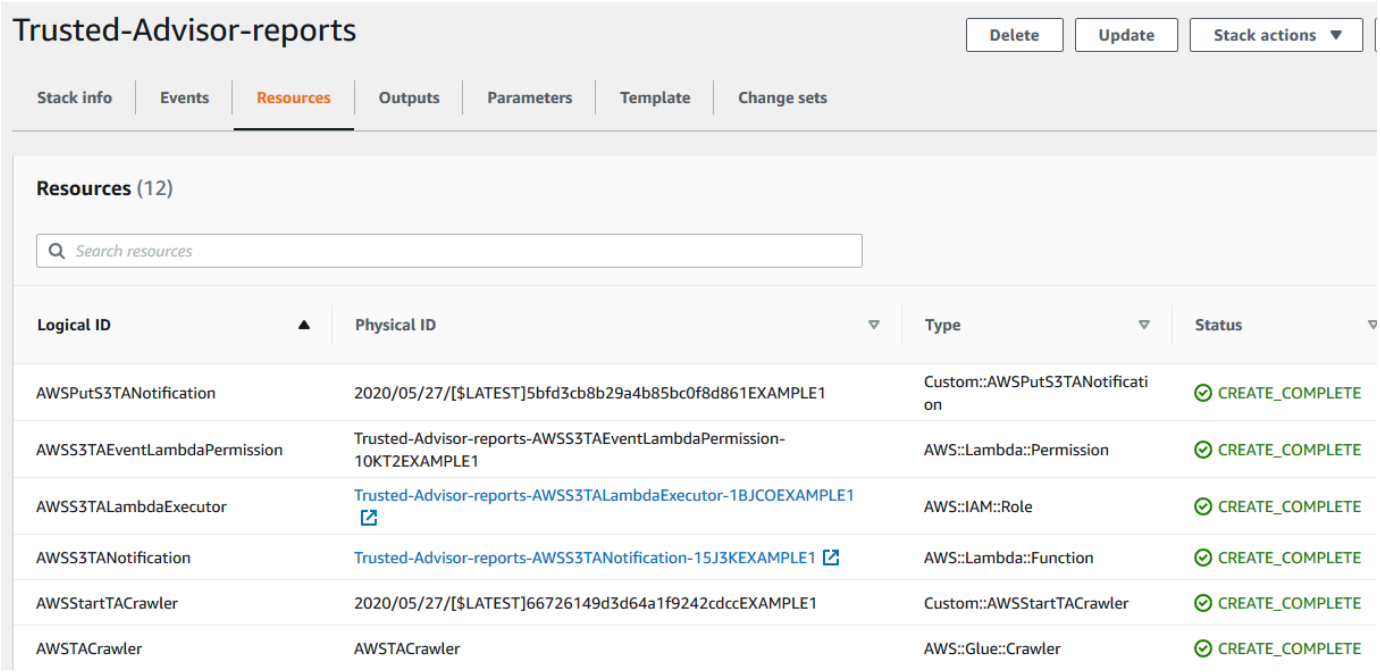
レポートを Amazon S3 にアップロードしたら、次の YAML テンプレートを AWS CloudFormation にアップロードします。このテンプレートは、他のサービスが S3 バケット内のレポートデータを使用できるように、アカウント用に作成する AWS CloudFormation リソースを に指示します。テンプレートは、IAM、 AWS Lambda、および のリソースを作成します AWS Glue。

を使用して リソースを作成するには AWS CloudFormation

1. trusted-advisor-reports-template.zip ファイルをダウンロードします。
2. ファイル を解凍します。
3. テキストエディタでテンプレートファイルを開きます。
4. `BucketName` および `FolderName` パラメーターで、*`your-bucket-name-here`* および *`folder1`* の値をアカウントのバケット名とフォルダ名で置き換えます。
5. ファイルを保存します。
6. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
7. リージョンの選択ツールで [米国東部 (バージニア北部)] リージョンを選択します (まだ選択していない場合)。
8. ナビゲーションペインで、[Stacks] を選択します。
9. [スタックの作成] を選択し、[新しいリソースを使用 (標準)] を選択します。
10. [スタックの作成] ページの [テンプレートの指定] で、テンプレートファイルのアップロード]、[ファイルの選択] の順に選択します。
11. YAML ファイルを選択し、[次へ] を選択します。

12. [スタックの詳細を指定] ページで、スタック名 (**Organizational-view-Trusted-Advisor-reports** など) を入力して [次へ] を選択します。
13. [スタックオプションを設定] ページでデフォルトオプションを受け入れ、[次へ] を選択します。
14. [**Organizational-view-Trusted-Advisor-reports** の確認] ページでオプションを確認します。ページの下部にある「 が IAM リソースを作成する AWS CloudFormation 可能性があることを承認します」のチェックボックスをオンにします。
15. [スタックの作成] を選択してください。

    スタックの作成には約 5 分かかります。
16. スタックが正常に作成されると、[リソース] タブは、次の例のようになります。



Amazon Athena でデータをクエリする

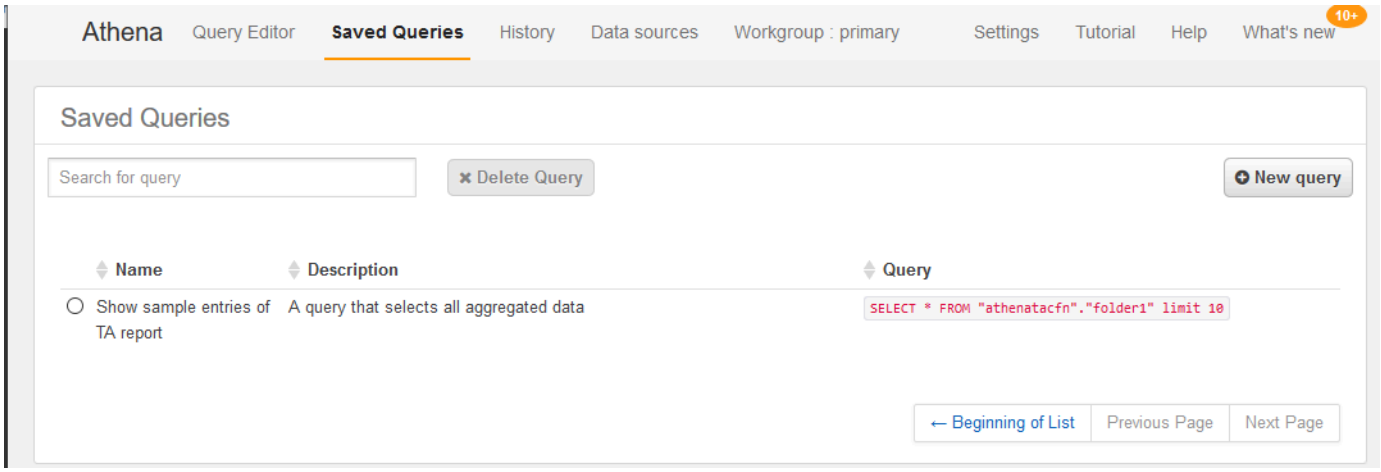
リソースを取得したら、Athena でデータを表示できます。Athena を使用してクエリを作成し、レポートの結果を分析します (組織内のアカウントの特定のチェック結果の検索など)。

> **メモ**
>
> - 米国東部 (バージニア北部) リージョンを使用します。
> - Athena を初めて使用する場合は、レポートに対してクエリを実行する前にクエリ結果の場所を指定する必要があります。この場所には別の S3 バケットを指定することをお勧めし

ます。詳細については、Amazon Athena ユーザーガイドの「クエリ結果の場所の指定」を参照してください。

Amazon Athena でデータをクエリするには

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. リージョンの選択ツールで [米国東部 (バージニア北部)] リージョンを選択します (まだ選択していない場合)。
3. [保存したクエリ] を選択し、検索フィールドに「**`Show sample`**」と入力します。
4. 表示されたクエリを選択します ([Show sample entries of TA report] など)。



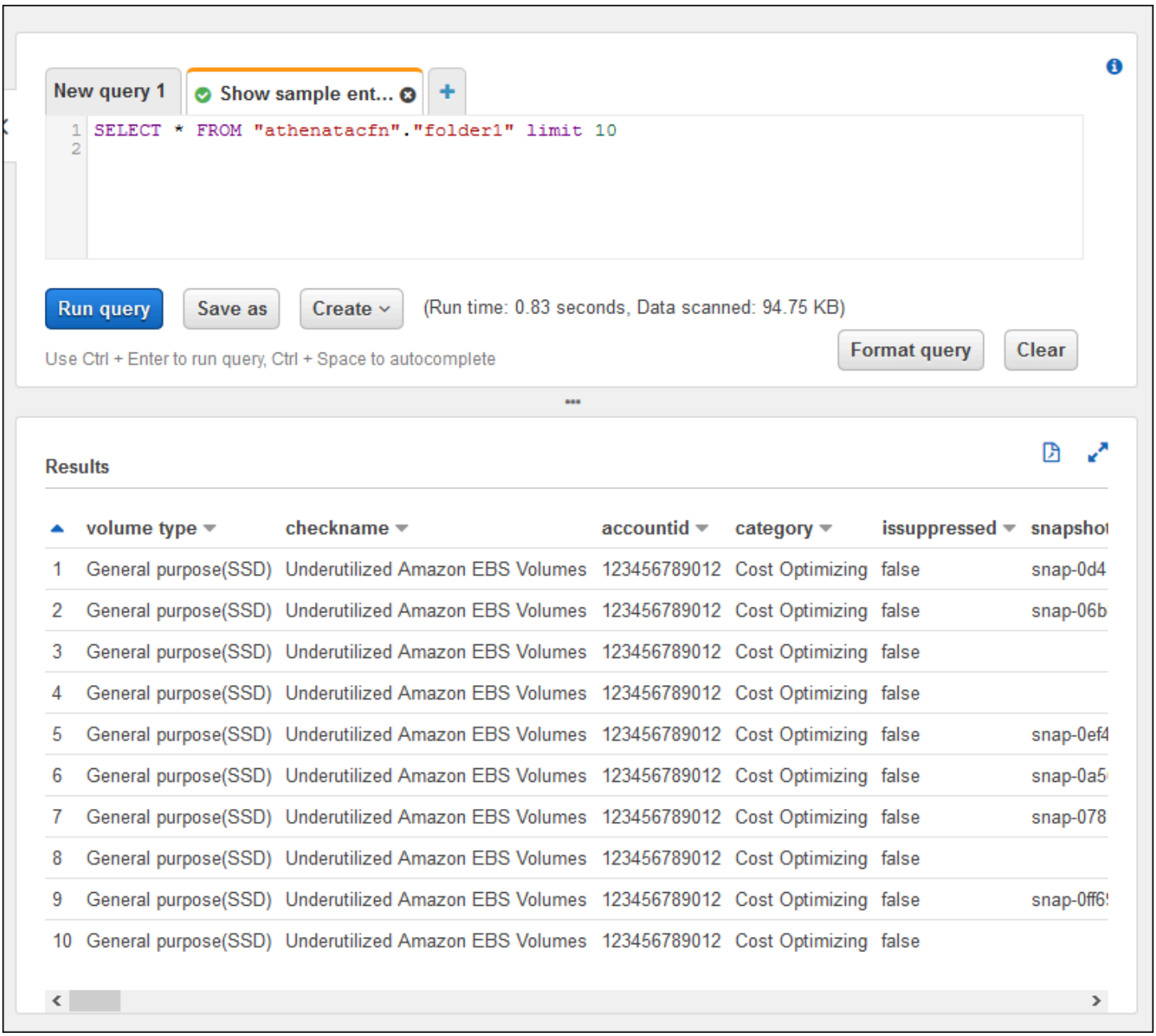
クエリは以下のようになります。

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. [Run query] (クエリの実行) を選択します。クエリの結果が表示されます。

Example : Athena クエリ

次の例は、レポートの 10 件のサンプルエントリを示しています。



詳細については、Amazon Athena ユーザーガイドの「Amazon Athena を使用した SQL クエリの実行」を参照してください。

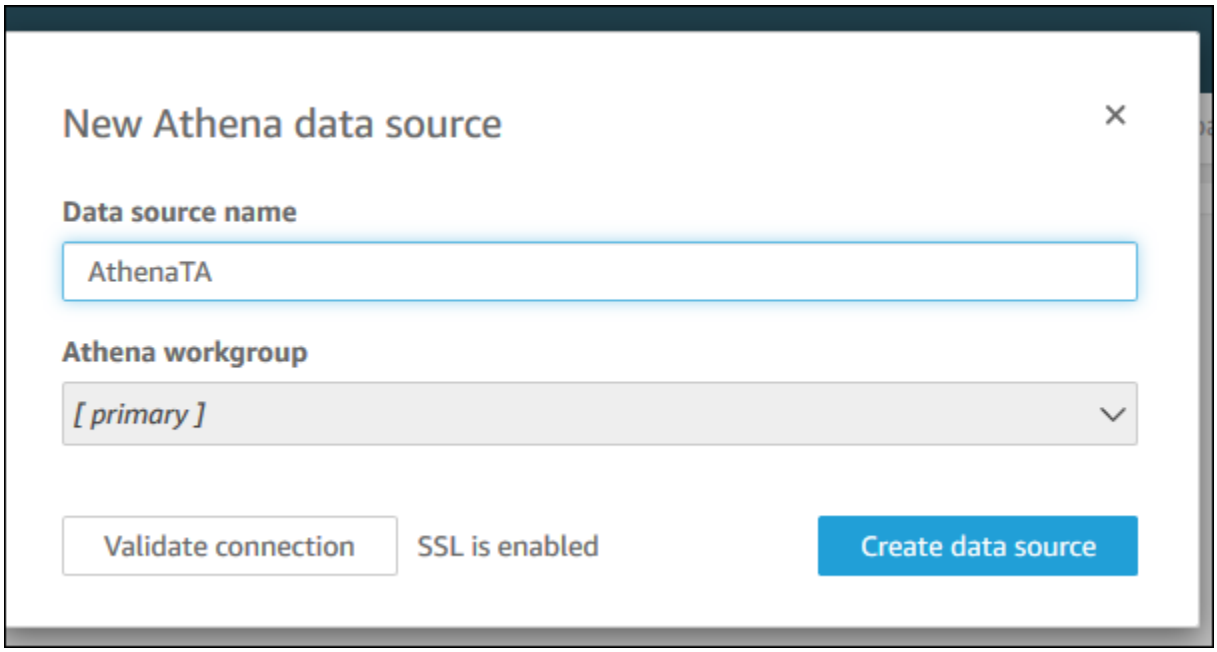
これで Amazon QuickSight でダッシュボードを作成できるようになりました。

Amazon QuickSight をセットアップして、ダッシュボードでデータを表示し、レポート情報を視覚化することもできます。

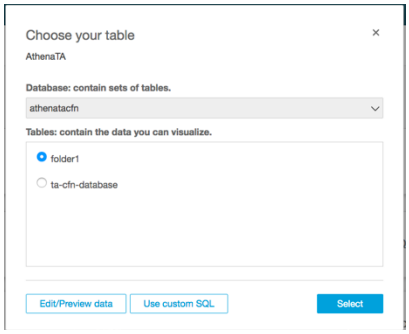
> **Note**
>
> 米国東部 (バージニア北部) リージョンを使用する必要があります。

Amazon QuickSight でダッシュボードを作成するには

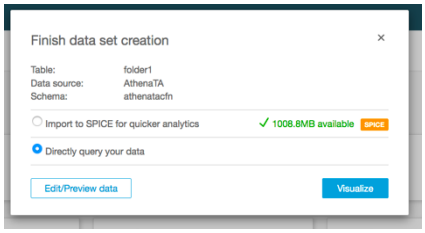
1. Amazon QuickSight コンソールに移動し、アカウントにサインインします。
2. [新しい分析]、[新しいデータセット] の順に選択し、[Athena] を選択します。
3. [新しい Athena データソース] ダイアログボックスで、データソース名 (「AthenaTA」など) を入力して [データソースを作成] を選択します。



4. [テーブルを選択] ダイアログボックスで、[athenatacfn] テーブル、[folder1] の順に選択し、[選択] を選択します。



5. [データセットの作成を完了] ダイアログボックスで [データを直接クエリする] を選択し、[視覚化] を選択します。



これで Amazon QuickSight でダッシュボードを作成できるようになりました。詳細については、Amazon QuickSight ユーザーガイドの「ダッシュボードの使用」を参照してください。

Example : Amazon QuickSight ダッシュボード

次のダッシュボードの例は、次のような Trusted Advisor チェックに関する情報を示しています。

- 影響を受けるアカウント ID
- AWS リージョン別の概要
- チェックカテゴリ
- チェックのステータス
- 各アカウントのレポート内のエントリの数

> **Note**
>
> ダッシュボードの作成中にアクセス許可エラーが発生した場合は、Amazon QuickSight が Athena を使用できることを確認してください。詳細については、Amazon QuickSight ユーザーガイドの「Amazon Athena に接続できない」を参照してください。

レポートデータの視覚化の詳細と例については、AWS Management & Governance ブログの「View AWS Trusted Advisor recommendations at scale with AWS Organizations」を参照してください。

トラブルシューティング

このチュートリアルで問題が発生した場合は、次のトラブルシューティングのヒントを参照してください。

レポートに最新のデータが表示されない

レポートを作成すると、組織ビュー機能は組織内の Trusted Advisor チェックを自動的に更新しません。最新のチェック結果を取得するには、組織内の管理アカウントと各メンバーアカウントのチェックを更新します。詳細については、「Trusted Advisor チェックの更新」を参照してください。

レポートに重複する列がある

レポートに重複する列がある場合、Athena コンソールのテーブルに次のエラーが表示されることがあります。

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table descriptor contains duplicate columns
```

例えば、すでに存在する列をレポートに追加した場合、Athena コンソールでレポートデータを表示しようとすると問題が発生する可能性があります。この問題を解決するには、次のステップに従います。

重複した列を検索する

AWS Glue コンソールを使用してスキーマを表示し、レポートに重複する列があるかどうかをすばやく特定できます。

重複した列を検索するには

1. https://console.aws.amazon.com/glue/ で AWS Glue コンソールを開きます。

2. リージョンの選択ツールで [米国東部 (バージニア北部)] リージョンを選択します (まだ選択していない場合)。
3. ナビゲーションペインで、[Tables (テーブル)] を選択します。
4. フォルダ名 (***folder1*** など) を選択し、[スキーマ] で [列名] の値を表示します。

   列が重複する場合は、新しいレポートを Amazon S3 バケットにアップロードする必要があります。次の「新しいレポートをアップロードする」セクションを参照してください。

新しいレポートをアップロードする

重複する列を識別したら、既存のレポートを新しいレポートで置き換えることをお勧めします。これにより、このチュートリアルで作成されたリソースは、組織の最新のレポートデータを使用するようになります。

新しいレポートをアップロードするには

1. まだ更新していない場合は、組織内のアカウントの Trusted Advisor チェックを更新します。「Trusted Advisor チェックの更新」を参照してください。
2. Trusted Advisor コンソールで別の JSON レポートを作成してダウンロードします。「組織ビューレポートを作成する」を参照してください。このチュートリアルでは、JSON ファイルを使用する必要があります。
3. にサインイン AWS Management Console し、https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
4. Amazon S3 バケットを選択し、*folder1* フォルダを選択します。
5. 以前の *resources*.json レポートを選択し、[削除] を選択します。
6. [オブジェクトの削除] ページの [オブジェクトを完全に削除しますか?] に「**permanently delete**」と入力し、[オブジェクトを削除] を選択します。
7. S3 バケットで [アップロード] を選択し、新しいレポートを指定します。この操作により Athena テーブルと AWS Glue クローラリソースが最新のレポートデータで更新されます。リソースの更新には数分かかることがあります。
8. Athena コンソールで新しいクエリを入力します。「Amazon Athena でデータをクエリする」を参照してください。

> **Note**
>
> このチュートリアルの問題が解決しない場合は、AWS サポート センターで技術サポートを作成できます。

による AWS Trusted Advisor チェックの表示 AWS Config

AWS Config は、必要な設定のリソース設定を継続的に評価、監査、評価するサービスです。 は、マネージドルール AWS Config を提供します。マネージドルールは、 が AWS リソースが一般的なベストプラクティスに準拠しているかどうかを評価するために AWS Config 使用する、事前定義されたカスタマイズ可能なコンプライアンスチェックです。

AWS Config コンソールでは、 マネージドルールの設定とアクティブ化について説明します。 AWS Command Line Interface （ AWS CLI) または AWS Config API を使用して、マネージドルールの設定を定義する JSON コードを渡すこともできます。マネージドルールの動作は、ニーズに合わせてカスタマイズできます。ルールのパラメータをカスタマイズして、ルールに準拠するためにリソースに必要とされる属性を定義できます。の有効化の詳細については AWS Config、「 AWS Config デベロッパーガイド」を参照してください。

AWS Config マネージドルールは、すべてのカテゴリにわたって一連の Trusted Advisor チェックを強化します。特定のマネージドルールを有効にすると、対応する Trusted Advisor チェックが自動的に有効になります。特定の AWS Config マネージドルールによって実行される Trusted Advisor チェックを確認するには、「」を参照してくださいAWS Trusted Advisor チェックリファレンス。

AWS Config パワードチェックは、AWS ビジネスサポート、AWS エンタープライズオンランプ、AWS エンタープライズサポートプランをご利用のお客様が利用できます。を有効に AWS Config し、これらの AWS サポートプランのいずれかがある場合、対応するデプロイされた AWS Config マネージドルールに基づくレコメンデーションが自動的に表示されます。

> **Note**
>
> これらのチェックの結果は、 AWS Config マネージドルールの変更によってトリガーされる更新に基づいて自動的に更新されます。更新要求は許可されません。現時点では、これらのチェックからリソースを除外することはできません。

トラブルシューティング

この統合に問題がある場合は、次のトラブルシューティング情報を参照してください。

目次

の記録とマネージドルールを有効にしたが AWS Config、対応する Trusted Advisor チェックが表示されない。

AWS Config ルールが評価結果を生成すると、ほぼリアルタイムで Trusted Advisor に結果が表示されます。この機能に問題がある場合は、AWS サポート センターで技術サポートケースを作成してください。

同じ AWS Config マネージドルールを 2 回デプロイしましたが、何が表示されます Trusted Advisorか？

インストールするマネージドルールごとに、 Trusted Advisor チェック結果に個別のエントリが表示されます。

AWS リージョン AWS Config で の記録をオフにしました。では何が表示されます Trusted Advisorか？

AWS リージョン AWS Config で のリソース記録をオフにした場合、 は対応するマネージドルールのデータを受信 Trusted Advisor しなくなり、そのリージョンで をチェックします。既存のマネージドルールの結果は、レコーダー保持ポリシーに基づいて、 AWS Config の有効期限が切れ Trusted Advisor るまで AWS Config と に残ります。マネージドルールを削除すると、 Trusted Advisor チェックデータは通常ほぼリアルタイムで削除されます。

での AWS Security Hub コントロールの表示 AWS Trusted Advisor

AWS Security Hub で を有効にすると AWS アカウント、 Trusted Advisor コンソールでセキュリティコントロールとその検出結果を表示できます。Security Hub コントロールを使用すると、

Trusted Advisor チェックを使用するのと同じ方法で、アカウントのセキュリティの脆弱性を特定できます。チェック状況や影響を受けるリソースのリストを表示し、Security Hub のレコメンデーションに従ってセキュリティ問題を対処します。この機能を使用すると、 Trusted Advisor と Security Hub から 1 つの便利な場所でセキュリティレコメンデーションを見つけることができます。

> **メモ**
>
> - から Trusted Advisor、カテゴリ: 復旧 > 回復力を持つコントロールを除き、 AWS Foundational Security Best Practices セキュリティ標準でコントロールを表示できます。サポートされるコントロールのリストについては、AWS Security Hub ユーザーガイドの「AWS Foundational Security Best Practices controls」を参照してください。
>
> Security Hub のカテゴリの詳細については、「Control categories」を参照してください。
> - Trusted Advisor は、2024 年 9 月 26 日までの Security Hub コントロールをオンボードしました。2024 年 9 月 26 日以降にリリースされたコントロールはまだオンボーディングされていません Trusted Advisor。その日付以降にリリースされたコントロールは、Security Hub ログにあります。

トピック

前提条件

Security Hub と Trusted Advisorの統合を有効にするには、次の要件を満たす必要があります。

- この機能を使用するには、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必要です。サポートプランは、AWS サポート センターまたはサポートプランページで確認できます。詳細については、AWS サポート 「計画の比較」を参照してください。
- Security Hub コントロール AWS リージョン に必要な AWS Config のリソース記録を で有効にする必要があります。詳細については、「 AWS Configの有効化と設定」を参照してください。

- Security Hub を有効にして、[AWS Foundational Security Best Practices v1.0.0] (基礎セキュリティのベストプラクティス v1.0.0) セキュリティスタンダードを選択する必要があります。まだ設定していない場合は、AWS Security Hub ユーザーガイドの「 AWS Security Hubのセットアップ」を参照してください。

> **Note**
>
> 前提条件をすでに満たしている場合は、Security Hub の調査結果を表示する に進んでください。

AWS Organizations アカウントについて

管理者アカウントの前提条件をすでに満たしている場合、この統合は組織内すべてのメンバーアカウントに対して自動的に有効になります。個々のメンバーアカウントは、この機能を有効にする サポート ために に問い合わせる必要はありません。ただし、組織のメンバーアカウントは、 Trusted Advisorで調査結果を確認したい場合は、Security Hub を有効にする必要があります。

特定のメンバーアカウントに対してこの統合を無効にする場合は、AWS Organizations アカウントのこの機能を無効にする を参照してください。

Security Hub の調査結果を表示する

アカウントの Security Hub を有効にした後、 Trusted Advisor コンソールの[Security] (セキュリティ) ページに、Security Hub の調査結果が表示されるまで最大 24 時間かかる場合があります。

で Security Hub の検出結果を表示するには Trusted Advisor

1. Trusted Advisor コンソールに移動し、[Security] (セキュリティ) カテゴリを選択します。
2. [Search by keyword] (キーワードによる検索) フィールドに、コントロール名または説明をに入力します。

   > **Tip**
   >
   > [Source] (ソース) は、[AWS Security Hub] を選択して、Security Hub のコントロールをフィルターできます。

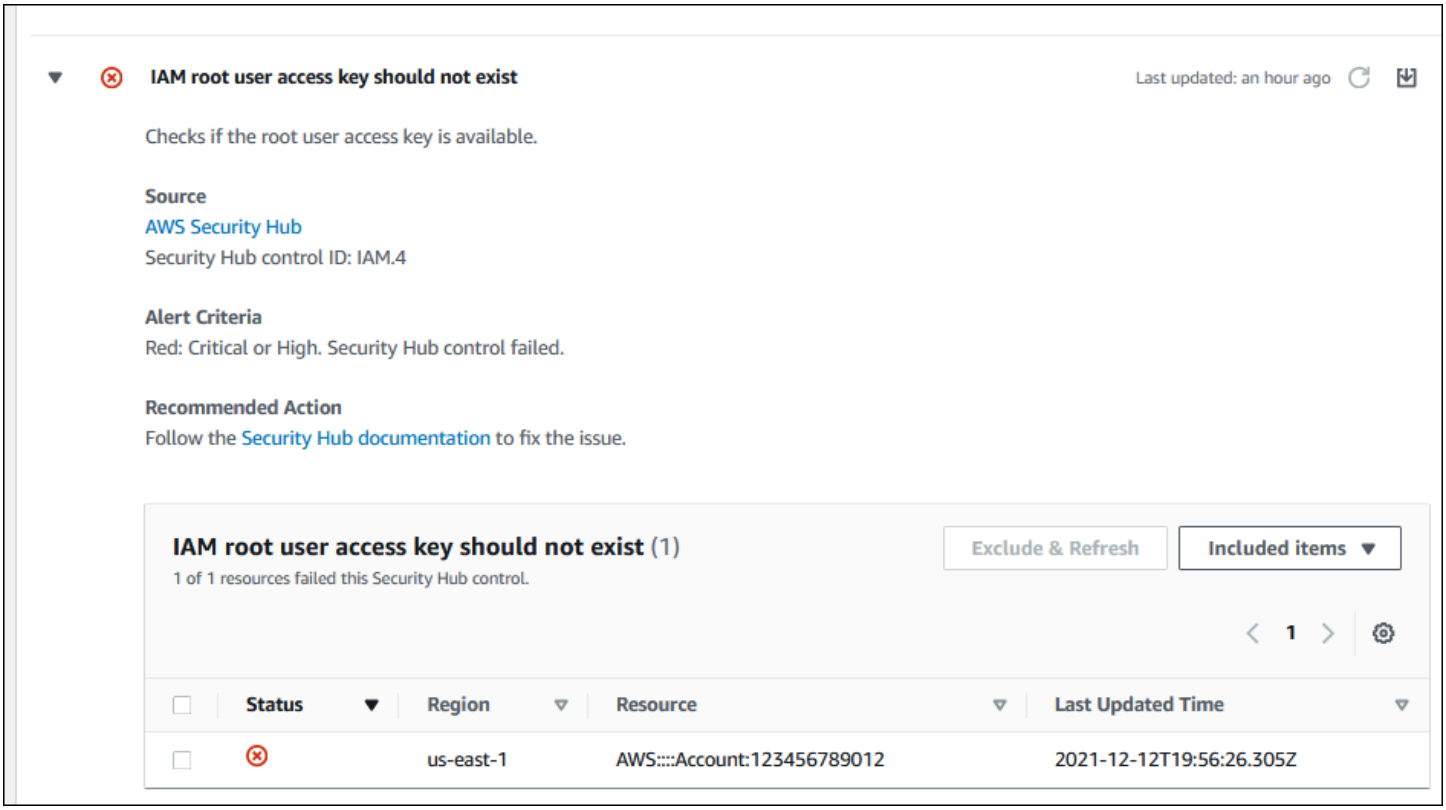
3. Security Hub コントロール名を選択すると、次の情報が表示されます。

- [Description] (説明) — コントロールがアカウントに対してセキュリティの脆弱性をチェックする方法を説明します。
- [Source] (ソース) — AWS Trusted Advisor または AWS Security Hubからのチェックか確認します。Security Hub コントロールの場合、コントロール ID を確認できます。
- [Alert Criteria] (アラート基準) — コントロールのステータスを確認します。例えば、Security Hub が重要な問題を検出した場合、ステータスは赤: [Critical] (重大) または [High] (高) と表示される場合があります。
- [Recommended Action] (推奨されるアクション) — Security Hub のドキュメントリンクを活用して、問題解決の推奨手順を確認します。
- [Security Hub resources] (Security Hub リソース) — Security Hub が問題を検出したリソースは、アカウントで確認できます。

> **メモ**
>
> - 調査結果からリソースを除外するには、Security Hub を使用する必要があります。現在、Trusted Advisor コンソールを使用して Security Hub コントロールから項目を除外することはできません。詳細については、「Setting the workflow status for findings」を参照してください。
> - 組織ビュー機能は、Security Hub との統合をサポートします。組織全体の Security Hub コントロールの調査結果を表示した後、レポートを作成しダウンロードできます。詳細については、「の組織ビュー AWS Trusted Advisor」を参照してください。

Example 例:IAM ユーザーアクセスキーの Security Hub コントロールは存在してはいけない

次の例は、 Trusted Advisor コンソールの Security Hub コントロールの調査結果です。



Security Hub の調査結果を更新する

セキュリティスタンダードを有効にした後、Security Hub がリソースの調査結果を取得するまでに最大 2 時間かかる場合があります。その後、そのデータが Trusted Advisor コンソールに表示されるまでに最大 24 時間かかることがあります。AWS Foundational Security Best Practices v1.0.0 セキュリティ標準を最近有効にした場合は、後で Trusted Advisor コンソールを再度確認してください。

> **Note**
>
> - 各 Security Hub の更新スケジュールは、定期的または変更がトリガーとなり設定されます。現在、 Trusted Advisor コンソールまたは AWS サポート API を使用して Security Hub コントロールを更新することはできません。詳細については、「Schedule for running security checks」を参照してください。
> - 調査結果からリソースを除外するには、Security Hub を使用する必要があります。現在、Trusted Advisor コンソールを使用して Security Hub コントロールから項目を除外することはできません。詳細については、「Setting the workflow status for findings」を参照してください。

から Security Hub を無効にする Trusted Advisor

Security Hub 情報を Trusted Advisor コンソールに表示したくない場合は、この手順を実行してください。この手順では、Security Hub と の統合のみが無効になります Trusted Advisor。Security Hub の設定には影響しません。引き続き、Security Hub のコンソールを使用して、セキュリティコントロール、リソース、およびレコメンデーションを表示できます。

Security Hub の統合を無効にするには

1. に連絡してAWS サポート、Security Hub と の統合を無効にするようにリクエストします Trusted Advisor。

   がこの機能 AWS サポート を無効にすると、Security Hub はデータを に送信しなくなります Trusted Advisor。Security Hub データは削除されます Trusted Advisor。
2. この統合を再度有効にするには、AWS サポート にお問い合わせください。

AWS Organizations アカウントのこの機能を無効にする

管理アカウントに対して既に前述の手順を完了している場合、組織内のすべてのメンバーアカウントから Security Hub の統合が自動的に削除されます。組織内の個々のメンバーアカウントは、個別に AWS サポート へお問い合わせ必要はありません。

組織のメンバーアカウントの場合は、 サポート に連絡して、アカウントからのみこの機能を削除できます。

トラブルシューティング

この統合に問題がある場合は、次のトラブルシューティング情報を参照してください。

目次

- コントロールは Security Hub にアーカイブされていますが、 に結果が表示されます Trusted Advisor
- Security Hub の調査結果がまだ表示されない。

Trusted Advisor コンソールに Security Hub の検出結果が表示されない

次のステップを完了していることを確認します。

- ビジネスプラン、エンタープライズ On-Ramp、エンタープライズサポートプランを利用している。
- Security Hub と同じリージョン AWS Config 内の でリソース記録を有効にしました。
- Security Hub を有効にして、[AWS Foundational Security Best Practices v1.0.0] (基礎セキュリティのベストプラクティス v1.0.0) セキュリティスタンダードを選択した。
- Security Hub の新しいコントロールは、 Trusted Advisor 2～4 週間以内にチェックインとして追加されます。注釈を参照してください。

詳細については、「前提条件」を参照してください。

Security Hub と AWS Config を正しく設定したが、検出結果がまだ確認できない。

Security Hub がリソースの結果を取得するまでに、最大 2 時間かかることがあります。その後、そのデータが Trusted Advisor コンソールに表示されるまでに最大 24 時間かかることがあります。後で Trusted Advisor コンソールをもう一度チェックしてください。

> **メモ**
>
> - カテゴリ: 復旧 > 回復力を持つコントロールを除き、 AWS Foundational Security Best Practices セキュリティ標準のコントロールの結果のみが Trusted Advisor に表示されます。
> - Security Hub または Security Hub にサービス上の問題がある場合、調査結果が Trusted Advisorに表示されるまでに最大 24 時間かかる場合があります。後で Trusted Advisor コンソールをもう一度チェックしてください。

特定の Security Hub コントロールを無効にしたい

Security Hub はデータを Trusted Advisor に自動的に送信します。Security Hub コントロールを無効にするか、そのコントロールのリソースが存在しなくなった場合、調査結果は Trusted Advisorに表示されません。

Security Hub のコンソールにサインインして、コントロールが有効か無効か確認できます。

Security Hub コントロールを無効にするか、 AWS Foundational Security Best Practices セキュリティ標準のすべてのコントロールを無効にすると、結果は今後 5 日以内にアーカイブされます。この 5 日間のアーカイブ期間は概算かつベストエフォートにとどまるものであり、保証されるものではありません。結果がアーカイブされると、 から削除されます Trusted Advisor。

詳細については、以下の各トピックを参照してください。

- 個々のコントロールの無効化と有効化
- セキュリティ標準の無効化または有効化

除外された Security Hub リソースを検索したい

Trusted Advisor コンソールから、Security Hub コントロール名を選択し、除外された項目オプションを選択できます。このオプションは、Security Hub で抑制されているすべてのリソースを表示します。

リソースのワークフローステータスが SUPPRESSED に設定されている場合、そのリソースは Trusted Advisorでは除外項目となります。 Trusted Advisor コンソールから Security Hub リソースを抑制することはできません。抑制する場合は、Security Hub コンソールを使用します。詳細については、「Setting the workflow status for findings」を参照してください。

AWS 組織に属するメンバーアカウントに対してこの機能を有効または無効にしたい

デフォルトでは、メンバーアカウントは AWS Organizationsの管理アカウントから機能を引き継ぎます。管理アカウントでこの機能を有効にした場合、組織内のすべてのアカウントにもこの機能が備わります。メンバーアカウントに対して特定の変更を加えたい場合は、AWS サポート にお問い合わせ必要があります。

Security Hub チェック AWS リージョン で同じ影響を受けるリソースに複数の が表示される

一部の AWS のサービス はグローバルであり、IAM や Amazon CloudFront など、リージョンに固有ではありません。デフォルトでは、Amazon S3 バケットなどのグローバルリソースは、米国東部 (バージニア北部) リージョンに表示されます。

グローバルサービスのリソースを評価する Security Hub チェックでは、影響を受けるリソースに関して複数の項目が表示される場合があります。例えば、アカウントでこの機能がアクティブ化されていないことが `Hardware MFA should be enabled for the root user` チェックで確認された場合、同じリソースのテーブルに複数のリージョンが表示されます。

Security Hub と を設定 AWS Config して、同じリソースに対して複数のリージョンが表示されないようにすることができます。詳細については、「AWS Foundational Best Practices controls that you might want to disable」(無効にする可能性のある の基本的なベストプラクティスのコントロール) を参照してください。

Security Hub またはリージョン AWS Config で をオフにした

で Security Hub を使用してリソースの記録を停止 AWS Config するか、無効にすると AWS リージョン、 はそのリージョンのコントロールのデータを受信 Trusted Advisor しなくなります。 は 7～9 日以内に Security Hub の検出結果 Trusted Advisor を削除します。この期間は、ベストエフォートであり、保証されません。詳細については、「Security Hub を無効にする」を参照してください。

アカウントでこの機能を無効にするには、「から Security Hub を無効にする Trusted Advisor」を参照してください。

コントロールは Security Hub にアーカイブされていますが、 に結果が表示されます Trusted Advisor

検出結果`RecordState`のステータスが に変わる`ARCHIVED`と、 はその Security Hub コントロール Trusted Advisor の検出結果をアカウントから削除します。削除されるまで、 Trusted Advisor 最大 7～9 日間、 に結果が表示されることがあります。この期間は、ベストエフォートであり、保証されません。

Security Hub の調査結果がまだ表示されない。

この機能の問題が解決しない場合は、AWS サポート センターで技術サポートを作成できます。

チェック AWS Compute Optimizer に Trusted Advisor オプトインする

Compute Optimizer は、 AWS リソースの設定と使用率のメトリクスを分析するサービスです。このサービスは、リソースが効率性と信頼性のために正しく設定されているかどうかを報告します。また、ワークロードのパフォーマンスを向上させるために実装できる改善も示唆しています。Compute Optimizer では、 Trusted Advisor チェックで同じレコメンデーションを表示します。

AWS アカウント のみ、または組織の一部であるすべてのメンバーアカウントをオプトインできます AWS Organizations。詳細については、AWS Compute Optimizer ユーザーガイド の「使用開始」を参照してください。

Compute Optimizer をオプトインすると、以下のチェックは Lambda 関数と Amazon EBS ボリュームからデータを受け取ります。検出結果と最適化のレコメンデーションの生成には、最大 12 時間かかることがあります。その後、次のチェック Trusted Advisor のために で結果が表示されるまでに最大 48 時間かかることがあります。

コスト最適化

- Amazon EBS の過剰プロビジョニングボリューム
- AWS Lambda メモリサイズの過剰プロビジョニングされた関数

パフォーマンス

- Amazon EBS のプロビジョニング不足ボリューム
- AWS Lambda メモリサイズのプロビジョニング不足関数

> **メモ**
>
> - これらのチェックの結果は、毎日数回自動的に更新されます。更新要求は許可されません。変更が表示されるまでに数時間かかる場合があります。現時点では、これらのチェックからリソースを除外することはできません。
> - Trusted Advisor には、使用率の低い Amazon EBS ボリュームと使用率の高い Amazon EBS マグネティックボリュームチェックが既にあります。

Compute Optimizer でオプトインしたら、新しい Amazon EBS 過剰プロビジョニングボリュームと Amazon EBS プロビジョニング不足ボリュームのチェックを代わりに使用することをお勧めします。

関連情報

詳細については、以下の各トピックを参照してください。

- AWS Compute Optimizer ユーザーガイドの Amazon EBS ボリュームに関するレコメンデーションの表示
- AWS Compute Optimizer ユーザーガイドの Lambda 関数に関するレコメンデーションの表示
- 詳細については、「AWS Lambda デベロッパーガイド」の「Lambda 関数メモリの設定」を参照してください。
- 「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリュームの変更をリクエストするAmazon EC2」

AWS Trusted Advisor Priority の使用を開始する

Trusted Advisor Priority は、 AWS がベストプラクティスに従う AWS アカウント ように保護および最適化するのに役立ちます。 Trusted Advisor Priority を使用すると、 AWS アカウント チームはアカウントをプロアクティブにモニタリングし、機会を特定したときに優先順位の高いレコメンデーションを作成できます。

例えば、アカウントチームは、 AWS アカウントのルートユーザーに多要素認証 (MFA) がないかどうかを特定できます。アカウントチームは、レコメンデーションを作成することで、`MFA on Root Account` などのチェックにすぐに対応できます。レコメンデーションは、 Trusted Advisor コンソールの Trusted Advisor Priority ページにアクティブな優先順位付きレコメンデーションとして表示されます。次に、このレコメンデーションに従って解決します。

Trusted Advisor 優先度の推奨事項は、次の 2 つのソースから取得されます。

- AWS のサービス – Trusted Advisorや Well-Architected などのサービスによって AWS Security Hub、 AWS 自動的にレコメンデーションが作成されます。アカウントチームがこれらのレコメンデーションを共有し、それらのレコメンデーションが Trusted Advisor Priority に表示されるようにします。

- アカウントチーム — アカウントチームは手動レコメンデーションを作成できます。

Trusted Advisor Priority は、最も重要なレコメンデーションに集中するのに役立ちます。お客様とアカウントチームは、アカウントチームがレコメンデーションを共有したときからお客様がレコメンデーションを確認、解決、却下するまでのレコメンデーションライフサイクルをモニタリングできます。 Trusted Advisor Priority を使用して、組織内のすべてのメンバーアカウントのレコメンデーションを検索できます。

トピック

前提条件

Trusted Advisor Priority を使用するには、次の要件を満たす必要があります。

- エンタープライズサポートプランが必要です。
- アカウントは、 AWS Organizationsのすべての機能が有効化された組織に属している必要があります。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。
- 組織で への信頼されたアクセスが有効になっている必要があります Trusted Advisor。信頼されたアクセスを有効にするには、管理アカウントとしてログインします。 Trusted Advisor コンソールで組織ページを開きます。

- AWS アカウントの Trusted Advisor Priority レコメンデーションを表示するには、アカウントにサインインする必要があります。
- 組織全体で集約されたレコメンデーションを表示するには、組織の管理アカウントまたは委任された管理者アカウントにサインインする必要があります。委任された管理者アカウントの登録方法については、「委任管理者を登録する」を参照してください。
- Trusted Advisor Priority にアクセスするには AWS Identity and Access Management 、(IAM) アクセス許可が必要です。 Trusted Advisor Priority へのアクセスを制御する方法については、へのアクセスを管理する AWS Trusted Advisor「」および「」を参照してくださいAWS の マネージドポリシー AWS Trusted Advisor。

Priority を有効にする Trusted Advisor

この機能を有効にするようアカウントチームに依頼してください。エンタープライズサポートプランがあり、組織の管理アカウントの所有者である必要があります。コンソールの Trusted Advisor Priority ページに信頼されたアクセスが必要であると表示された場合は AWS Organizations、信頼されたアクセスを有効にする AWS Organizationsを選択します。詳細については「前提条件」セクションを参照してください。

優先レコメンデーションを表示

アカウントチームが Trusted Advisor Priority を有効にしたら、 AWS アカウントの最新のレコメンデーションを表示できます。

優先レコメンデーションを表示するには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Priority] ページで、次を表示することができます。

   AWS Organizations 管理アカウントまたは委任管理者アカウントを使用している場合は、マイアカウントタブに切り替えます。

   - [必要なアクション] — 応答を保留中または処理中のレコメンデーションの数。
   - [Overview] (概要) - 次の情報が表示されます。
     - 過去 90 日間に却下されたレコメンデーション
     - 過去 90 日間に解決されたレコメンデーション
     - 30 日以上更新されていないレコメンデーション

- レコメンデーションの解決に要する平均時間

3. [アクティブ] タブの [優先順位付けされたアクティブなレコメンデーション] に、アカウントチームが優先順位付けしたレコメンデーションが表示されます。[クローズ] タブには、解決済みまたは却下されたレコメンデーションが表示されます。

   - 結果を絞り込むには、次のオプションを使用します。

     - [Recommendation] (レコメンデーション) – 名前で検索するためのキーワードを入力します。チェック名、またはアカウントチームが作成したカスタム名などです。
     - ステータス – レコメンデーションが応答を保留中、進行中、却下、または解決済みのいずれか。
     - 送信元 – 優先レコメンデーションの起源。レコメンデーションは AWS のサービス、、AWS アカウント チーム、または計画されたサービスイベントから取得できます。
     - カテゴリ – セキュリティやコストの最適化などのレコメンデーションカテゴリ。
     - [Age] (経過時間) – アカウントチームがお客様にレコメンデーションを共有した時期です。

4. レコメンデーションを選択すると、その詳細、影響を受けるリソース、推奨されるアクションの詳細を確認できます。その後、レコメンデーションを確認または却下できます。

AWS 組織内のすべてのアカウントで優先レコメンデーションを表示するには

管理アカウントと Trusted Advisor Priority の委任された管理者の両方が、組織全体に集約されたレコメンデーションを表示できます。

> **Note**
>
> メンバーアカウントは、集約されたレコメンデーションにアクセスできません。

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Priority] ページで、[自分の組織] タブが表示されていることを確認します。
3. 1 つのアカウントのレコメンデーションを表示するには、[組織からアカウントを選択] のドロップダウンリストからアカウントを選択します。または、すべてのアカウントのレコメンデーションを表示することもできます。

[自分の組織] タブでは、次の項目を表示できます。

- [必要なアクション]: 応答を保留中または処理中の、組織全体のレコメンデーションの数。
- [概要]: 次の項目を表示します。

  - 過去 90 日間に却下されたレコメンデーション。

  - 過去 90 日間に解決されたレコメンデーション。

  - 30 日間を超える期間にわたって更新されていないレコメンデーション。

  - レコメンデーションを解決するのにかかる平均時間。

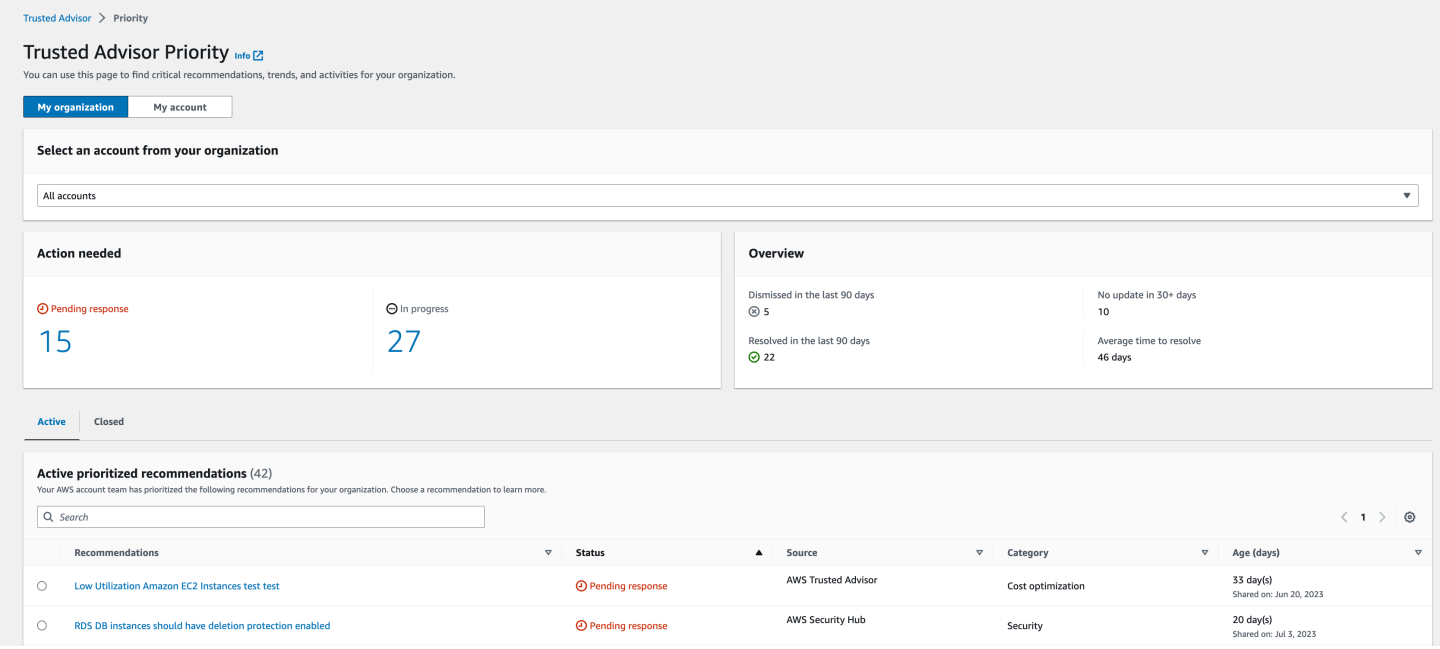
4. [アクティブ] タブの [優先順位付けされたアクティブなレコメンデーション] セクションに、アカウントチームが優先順位付けしたレコメンデーションが表示されます。[クローズ] タブには、解決済みまたは却下されたレコメンデーションが表示されます。

   結果を絞り込むには、次のオプションを使用します。

   - [Recommendation] (レコメンデーション) – 名前で検索するためのキーワードを入力します。これは、チェック名、またはアカウントチームが作成したカスタム名のいずれかです。
   - ステータス – レコメンデーションが応答を保留中、進行中、却下、または解決済みのいずれか。
   - 送信元 – 優先レコメンデーションの起源。レコメンデーションは AWS のサービス、、 AWS アカウント チーム、または計画されたサービスイベントから取得できます。
   - カテゴリ – セキュリティやコストの最適化などのレコメンデーションカテゴリ。
   - [Age] (経過時間) – アカウントチームがお客様にレコメンデーションを共有した時期です。
5. レコメンデーションを選択すると、追加の詳細、影響を受けるアカウントとリソース、推奨されるアクションが表示されます。その後、レコメンデーションを確認または却下できます。

Example ： Trusted Advisor 優先順位の推奨事項

次の例は、[必要なアクション] セクションに表示されている応答を保留中の 15 のレコメンデーションと進行中の 27 のレコメンデーションを示しています。次の画像は、[アクティブな優先レコメンデーション] タブに表示されている応答を保留中の 2 つのレコメンデーションを示しています。



レコメンデーションを確認するには

[アクティブ] タブでは、レコメンデーションの詳細を確認し、それを確認するかどうか決定できます。

レコメンデーションを確認するには

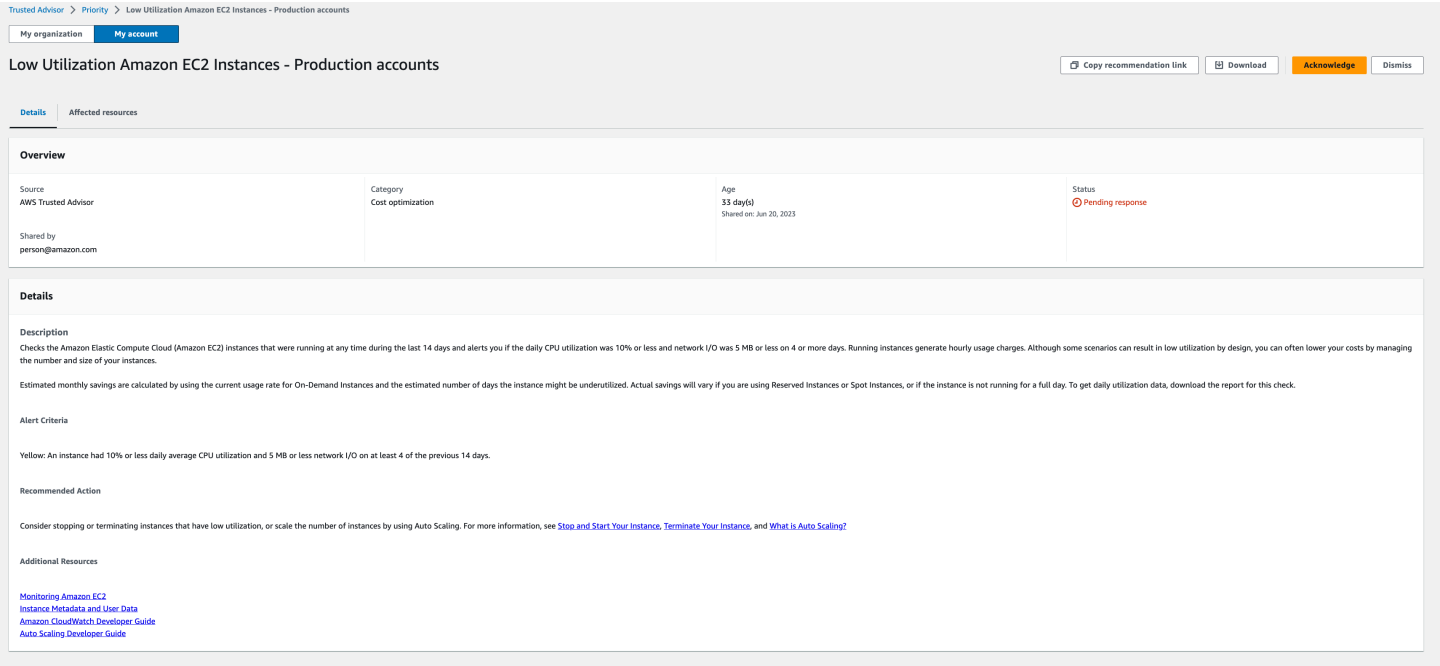
1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. AWS Organizations 管理アカウントまたは委任管理者アカウントを使用している場合は、マイアカウントタブに切り替えます。
3. [Trusted Advisor Priority] ページの [Active] (アクティブ) タブで、レコメンデーション名を選択します。
4. [詳細] セクションでは、レコメンデーションを解決するために推奨されるアクションを確認できます。
5. [影響を受けるリソース] セクションでは、影響を受けるリソースを確認し、[ステータス] でフィルタリングできます。
6. [承認] を選択します。
7. [レコメンデーションを確認] ダイアログボックスで [確認] を選択します。

   レコメンデーションステータスが [In progress] に変わります。進行中のレコメンデーションまたは保留中のレスポンスは、 Trusted Advisor 優先度ページのアクティブタブに表示されます。

8. レコメンデーションを解決するには、レコメンデーションに従います。詳細については、「レコメンデーションを解決する」を参照してください。

Example : Trusted Advisor Priority からの手動レコメンデーション

次の図は、応答を保留している [使用率が低い EC2 インスタンス] のレコメンデーションを示しています。



AWS 組織内のすべてのアカウントのレコメンデーションを承認するには

管理アカウントまたは Trusted Advisor の委任された管理者は、影響を受けるすべてのアカウントのためにレコメンデーションを承認できます。

> **Note**
>
> メンバーアカウントは、集約されたレコメンデーションにアクセスできません。

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Priority] ページで、[自分の組織] タブが表示されていることを確認します。
3. [アクティブ] タブで、推奨される名前を選択します。
4. [承認] を選択します。

5. [レコメンデーションを確認] ダイアログボックスで [確認] を選択します。

   レコメンデーションステータスが [In progress] に変わります。

6. レコメンデーションを解決するには、レコメンデーションに従います。詳細については、「レコメンデーションを解決する」を参照してください。

7. レコメンデーションの詳細を表示するには、レコメンデーションの名前を選択します。

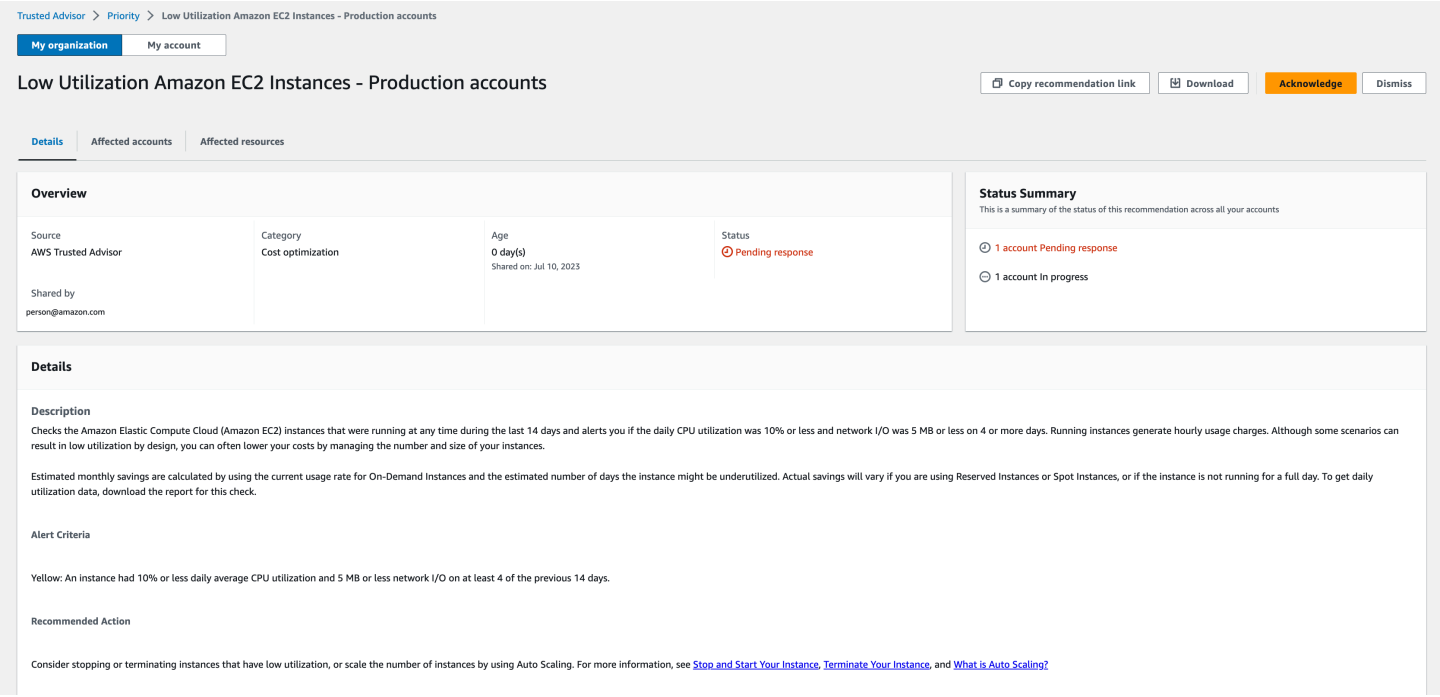
   [詳細] セクションで、レコメンデーションに関する次の情報を確認できます。

   - レコメンデーションの [概要] と、完了するレコメンデーションアクションを説明する [詳細] セクション。

     影響を受けるすべてのアカウントのレコメンデーションを示す [ステータスの概要]。
   - [影響を受けるアカウント] セクションでは、すべてのアカウントにおける影響を受けるリソースを確認できます。[アカウント番号] と [ステータス] でフィルタリングできます。
   - [影響を受けるリソース] セクションでは、すべてのアカウントにおける影響を受けるリソースを確認できます。[アカウント番号] と [ステータス] でフィルタリングできます。

Example : Trusted Advisor Priority からの手動レコメンデーション

次の図は、応答を保留している [使用率が低い Amazon EC2 インスタンス] のレコメンデーションを示しています。影響を受けるアカウントの 1 つがこのレコメンデーションを承認しました。別のアカウントが応答を保留しているため、レコメンデーションステータスが [応答待ち] になっています。



レコメンデーションを却下する

レコメンデーションは却下することもできます。これは、レコメンデーションを承認しても対処しないことを意味します。アカウントに関係ないレコメンデーションは却下できます。例えば、 AWS アカウント 削除する予定のテストがある場合、推奨されるアクションに従う必要はありません。

レコメンデーションを却下するには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. AWS Organizations 管理アカウントまたは委任管理者アカウントを使用している場合は、マイアカウントタブに切り替えます。
3. [Trusted Advisor Priority] ページの [Active] (アクティブ) タブで、レコメンデーション名を選択します。
4. レコメンデーションの詳細ページで、影響が及ぶアカウントの情報を確認します。
5. このレコメンデーションがアカウントに該当しない場合は、[却下] を選択します。
6. [レコメンデーションを却下] ダイアログでレコメンデーションに対処しない理由を選択します。
7. (オプション) レコメンデーションを却下する詳細な理由を入力します。[その他] を選択した場合は、[メモ] セクションに説明を入力する必要があります。

8. [却下] を選択します。レコメンデーションのステータスが「Dismissed」に変わり、 Trusted Advisor 「優先度」ページの「クローズド」タブに表示されます。

AWS 組織内のすべてのアカウントのレコメンデーションを却下するには

Trusted Advisor Priority の管理アカウントまたは委任された管理者は、すべてのアカウントのレコメンデーションを却下できます。

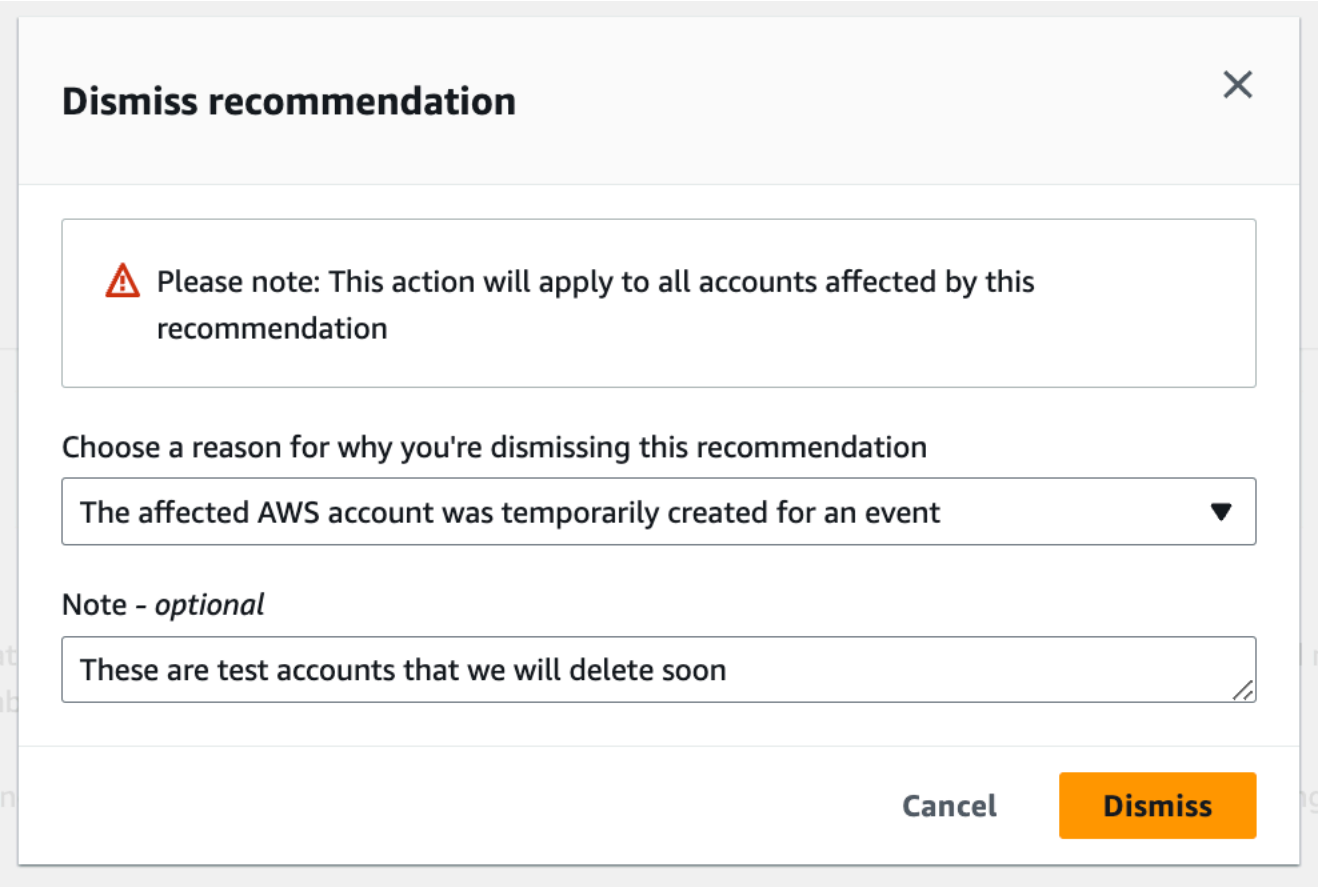
1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. Priority Trusted Advisor ページで、My Organization タブが表示されていることを確認します。
3. [アクティブ] タブで、推奨される名前を選択します。
4. このレコメンデーションがアカウントに該当しない場合は、[却下] を選択します。
5. [レコメンデーションを却下] ダイアログでレコメンデーションに対処しない理由を選択します。
6. (オプション) レコメンデーションを却下する詳細な理由を入力します。[その他] を選択した場合は、[メモ] セクションに説明を入力する必要があります。
7. [却下] を選択します。レコメンデーションステータスが [却下済み] に変わります。レコメンデーションは、 Trusted Advisor 優先度ページのクローズタブに表示されます。

> **Note**
>
> レコメンデーションの名前を選択し、[メモを表示] を選択すると却下の理由を確認できます。アカウントチームがお客様に代わってレコメンデーションを却下した場合、メモの横にチームの E メールアドレスが表示されます。

Trusted Advisor Priority は、レコメンデーションを却下したことをアカウントチームにも通知します。

Example : Trusted Advisor Priority からのレコメンデーションを却下する

次の例は、レコメンデーションを却下する方法を示します。



レコメンデーションを解決する

レコメンデーションを確認して推奨されるアクションを完了したら、レコメンデーションを解決できます。

> **Tip**
>
> 解決したレコメンデーションは再度開くことはできません。後でもう一度レコメンデーション確認する場合は、「レコメンデーションを却下する」を参照してください。

レコメンデーションを解決するには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. Priority Trusted Advisor ページで、My Organization タブが表示されていることを確認します。
3. [Trusted Advisor Priority] ページで、レコメンデーションを選択してから、[Resolve] を選択します。

4. [レコメンデーションの解決] ダイアログで [解決] を選択します。解決されたレコメンデーションは、 Trusted Advisor 優先度ページのクローズタブの下に表示されます。 Trusted Advisor 優先度は、レコメンデーションを解決したことをアカウントチームに通知します。

AWS 組織内のすべてのアカウントのレコメンデーションを解決するには

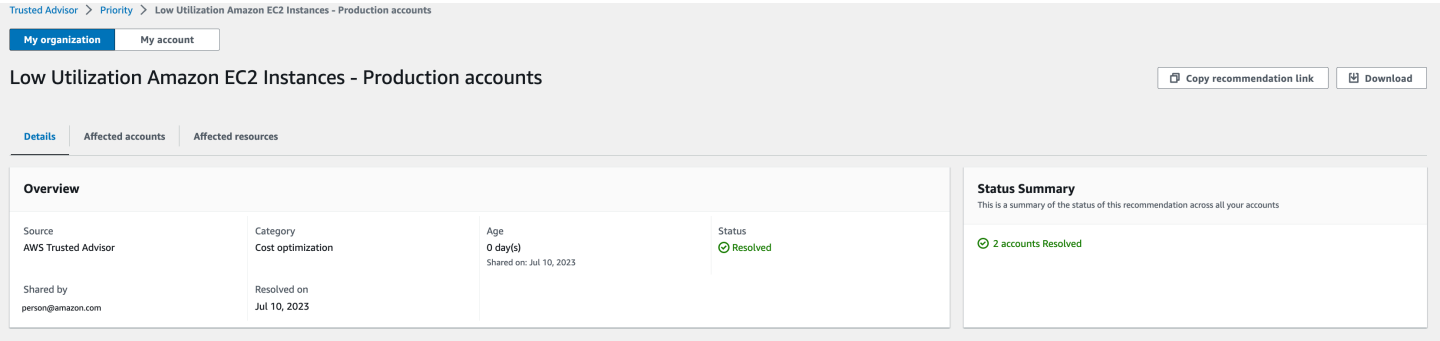
管理アカウントまたは Trusted Advisor Priority の委任管理者は、すべてのアカウントのレコメンデーションを解決できます。

> **Note**
>
> メンバーアカウントは、集約されたレコメンデーションにアクセスできません。

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. AWS Organizations 管理アカウントまたは委任管理者アカウントを使用している場合は、マイアカウントタブに切り替えます。
3. [アクティブ] タブで、推奨される名前を選択します。
4. レコメンデーションがアカウントに適用されない場合は、[解決] を選択します。
5. [レコメンデーションの解決] ダイアログで [解決] を選択します。解決されたレコメンデーションは、 Trusted Advisor 優先度ページのクローズタブの下に表示されます。 Trusted Advisor 優先度は、レコメンデーションを解決したことをアカウントチームに通知します。

Example : Trusted Advisor Priority からの手動レコメンデーション

次の例は、[使用率の低い Amazon EC2 インスタンス] の解決済みのレコメンデーションを示しています。



レコメンデーションを再オープンする

却下したレコメンデーションはお客様またはアカウントチームが再度開くことができます。

レコメンデーションを再オープンするには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. AWS Organizations 管理アカウントまたは委任管理者アカウントを使用している場合は、マイアカウントタブに切り替えます。
3. [Trusted Advisor Priority] ページで、[Closed] (クローズ) タブを選択します。
4. [クローズしたレコメンデーション] で、[却下済み] のレコメンデーションを選択して [再度開く] を選択します。
5. [レコメンデーションを再度開く] ダイアログボックスで、レコメンデーションを再度開く理由を入力します。
6. [Reopen] (再オープン) を選択します。レコメンデーションステータスが [In progress] (進行中) に変わって、[Active] (アクティブ) タブに表示されます。

   > **Tip**
   >
   > レコメンデーションの名前を選択し、[メモを表示] を選択すると再度開く理由が表示されます。アカウントチームがお客様に代わってレコメンデーションを再度開いた場合、メモの横にチームの名前が表示されます。

7. レコメンデーションの詳細に表示される手順に従います。

AWS 組織内のすべてのアカウントのレコメンデーションを再開するには

管理アカウントまたは Trusted Advisor Priority の委任管理者は、すべてのアカウントのレコメンデーションを再開できます。

> **Note**
>
> メンバーアカウントは、集約されたレコメンデーションにアクセスできません。

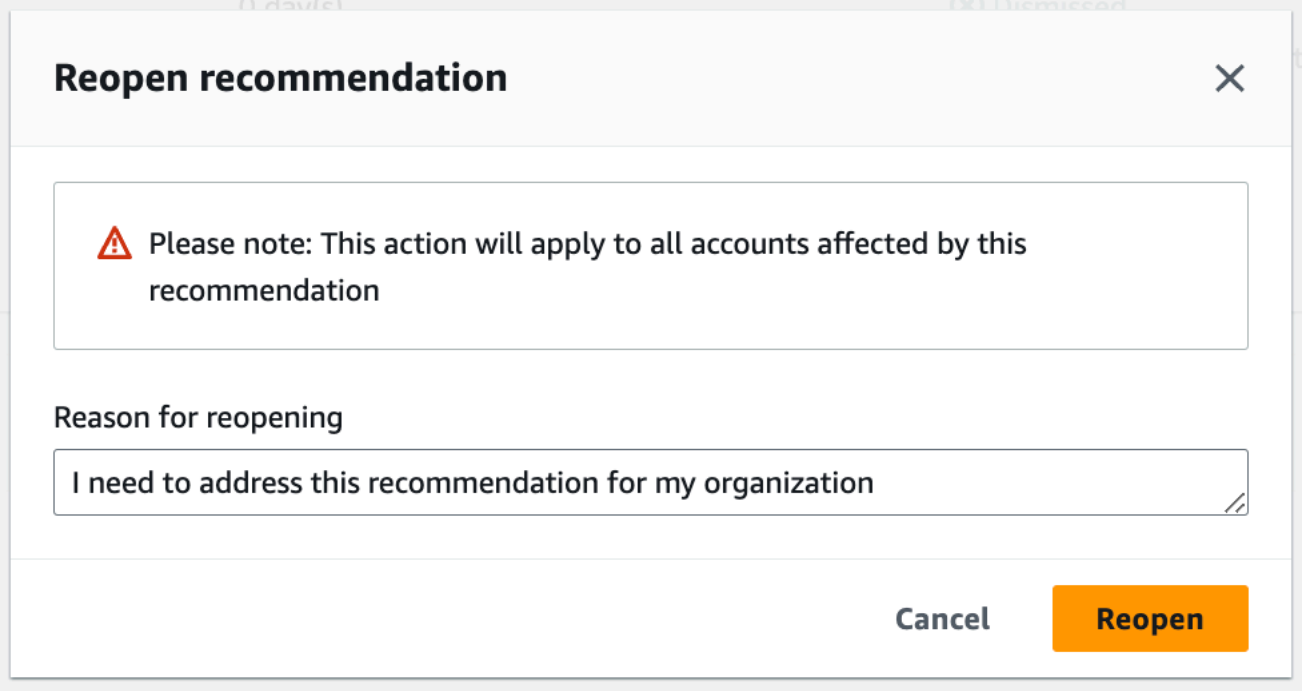
1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. Priority Trusted Advisor ページで、My Organization タブが表示されていることを確認します。
3. [クローズしたレコメンデーション] で、[却下済み] のレコメンデーションを選択して [再度開く] を選択します。
4. [レコメンデーションを再度開く] ダイアログボックスで、レコメンデーションを再度開く理由を入力します。
5. [Reopen] (再オープン) を選択します。レコメンデーションステータスが [In progress] (進行中) に変わって、[Active] (アクティブ) タブに表示されます。

> **Tip**
>
> レコメンデーションの名前を選択し、[メモを表示] を選択すると再度開く理由が表示されます。アカウントチームがお客様に代わってレコメンデーションを再度開いた場合、メモの横にチームの名前が表示されます。

6. レコメンデーションの詳細に表示される手順に従います。

Example : Trusted Advisor Priority からレコメンデーションを再開する

以下は、レコメンデーションの再オープンの例です。



レコメンデーションの詳細をダウンロード

また、 Trusted Advisor Priority から優先レコメンデーションの結果をダウンロードすることもできます。

> **Note**
>
> 現在、レコメンデーションをダウンロードできるのは、一度に 1 回のみです。

レコメンデーションをダウンロードするには

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Priority] ページで、レコメンデーションを選択してから、[Download] を選択します。
3. ファイルを開いてレコメンデーションの詳細を表示します。

委任管理者を登録する

組織に属するメンバーアカウントを委任管理者として追加できます。委任された管理者アカウントは、 Trusted Advisor Priority でレコメンデーションを確認、承認、解決、却下、再開できます。

アカウントを登録したら、 Trusted Advisor Priority にアクセスするために必要なアクセス AWS Identity and Access Management 許可を委任管理者に付与する必要があります。詳細については、へのアクセスを管理する AWS Trusted AdvisorおよびAWS の マネージドポリシー AWS Trusted Advisorを参照してください。

メンバーアカウントは 5 つまで登録できます。組織の委任管理者を追加できるのは、管理アカウントのみです。委任された管理者を登録または登録解除するには、組織の管理アカウントにサインインする必要があります。

の委任管理者を登録する手順

1. 管理アカウントとして https://console.aws.amazon.com/trustedadvisor/home の Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインの [Preferences] (設定) で、[Your organization] (お客様の組織) を選択します。

3. [Delegated administrator] (委任管理者) で、[Register new account] (新しいアカウントを登録) を選択します。
4. ダイアログボックスでメンバーアカウント ID を入力し、[Register] (登録) を選択します。
5. (オプション) アカウントの登録を解除するには、アカウントを選択して [Deregister] (登録解除) を選択します。ダイアログボックスで、再度 [Deregister] (登録解除) を選択します。

委任管理者を登録解除する

メンバーアカウントの登録を解除すると、そのアカウントは、管理アカウントと同じように Trusted Advisor Priority にアクセスすることができなくなります。委任管理者でなくなったアカウントは、Trusted Advisor Priority から E メール通知を受信しません。

の委任管理者を登録解除する手順

1. 管理アカウントとして https://console.aws.amazon.com/trustedadvisor/home の Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインの [Preferences] (設定) で、[Your organization] (お客様の組織) を選択します。
3. [委任された管理者] で、アカウントを選択し、[登録解除] を選択します。
4. ダイアログボックスで、[Deregister] (登録解除) を選択します。

Trusted Advisor Priority 通知の管理

Trusted Advisor Priority は、E メールで通知を送信します。このメール通知には、アカウントチームが優先順位付けしているレコメンデーションの概要が記されています。 Trusted Advisor Priority から更新を受け取る頻度を指定できます。

メンバーアカウントを委任管理者として登録した場合、メンバーアカウントが Trusted Advisor Priority の E メール通知を受信するように設定することもできます。

Trusted Advisor 優先度 E メール通知には、個々のアカウントのチェック結果は含まれません。レ Trusted Advisor コメンデーションの週次通知とは別のものです。詳細については、「通知設定の設定」を参照してください。

> **Note**
>
> Trusted Advisor Priority E メール通知は、管理アカウントまたは委任された管理者のみが設定できます。

Trusted Advisor Priority 通知を管理するには

1. 管理アカウントまたは委任された管理者アカウントとして、https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. ナビゲーションペインの [Preferences] (設定) で、[Notifications] (通知) を選択します。
3. [Priority] で、以下のオプションを選択できます。
   a. [Daily] (日次) — メール通知を毎日受け取ります。
   b. [Weekly] (週次) — メール通知を週 1 回受け取ります。
   c. 受信する通知を選択してください。
      - 優先順位付けされたレコメンデーションの概要
      - 解決した日
4. [受信者] で、メール通知を受け取るその他の連絡先を選択します。 AWS Billing and Cost Management コンソールのアカウント設定ページから連絡先を追加または削除できます。
5. [Language] (言語) で、メール通知の使用言語を選択します。
6. [Save your preferences] (詳細設定を保存) を選択します。

> **Note**
>
> Trusted Advisor Priority は、noreply@notifications.trustedadvisor.us-west-2.amazonaws.com アドレスから E メール通知を送信します。メールクライアントがこれらのメールをスパムとして認識していないかどうか、確認することをお勧めします。

Priority を無効にする Trusted Advisor

アカウントチームに連絡し、この機能を無効にするように依頼してください。この機能を無効にすると、優先レコメンデーションは Trusted Advisor コンソールに表示されなくなります。

Trusted Advisor Priority を無効にしてから後で再度有効にしても、 Trusted Advisor Priority を無効にする前にアカウントチームが送信したレコメンデーションは引き続き表示できます。

AWS Trusted Advisor Engage の使用を開始する (プレビュー)

> **Note**
>
> AWS Trusted Advisor Engage はプレビューリリースであり、変更される可能性があります。プレビューサービス条件については、https://aws.amazon.com/service-terms/ を参照してください。

AWS Trusted Advisor Engage を使用すると、すべてのプロアクティブなエンゲージメントを簡単に確認、リクエスト、追跡し、進行中のエンゲージメントについて AWS アカウント チームと通信できるため、 AWS サポート プランを最大限に活用できます。

例えば、 AWS Trusted Advisor コンソール内の Engage ページに移動して、 AWS アカウント チームに「Management Business Review」をリクエストできます。その後、 AWS 専門家がリクエストの担当になり、エンゲージメント全体をフォローします。

トピック

前提条件

Trusted Advisor Engage を使用するには、次の要件を満たすために必要なアクションを実行する必要があります。

- Enterprise On-Ramp サポートプランが必要です。
- アカウントは、 AWS Organizationsのすべての機能が有効化された組織に属している必要があります。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。
- 組織で への信頼されたアクセスが有効になっている必要があります Trusted Advisor。信頼されたアクセスを有効にするには、管理アカウントとしてログインし、 Trusted Advisor コンソールの組織ページに移動します。
- Trusted Advisor Engage にアクセスするには AWS Identity and Access Management 、(IAM) アクセス許可が必要です。 Trusted Advisor Engage へのアクセスを制御する方法については、「」を参照してくださいへのアクセスを管理する AWS Trusted Advisor。

> **Note**
>
> AWS Organization 内の任意のアカウントでエンゲージメントリクエストを作成できます。エンゲージメント所有アカウントが別の AWS 組織に移動した場合、エンゲージメントにはアカウントのみがアクセスできます。コントロールを制限するには、「AWS Trusted Advisor のサービスコントロールポリシーの例」を参照してください。

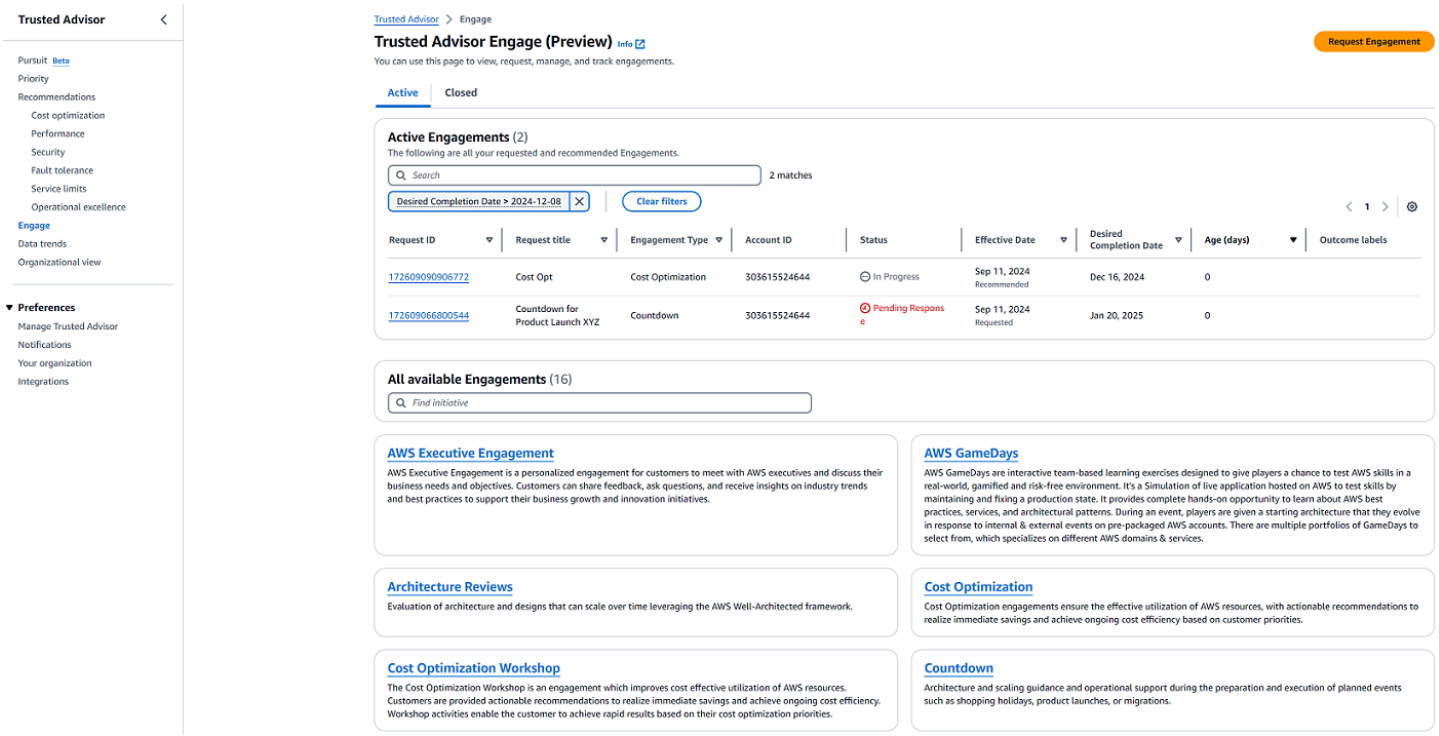
エンゲージメントダッシュボードを表示する

アクセス権を取得したら、コンソール内の Trusted Advisor Trusted Advisor Engage ページにアクセスしてダッシュボードを表示し、 AWS アカウント チームとのエンゲージメントを管理できます。

エンゲージメントを管理するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページでは、以下を表示できます。
   - [エンゲージメントをリクエスト] ボタン
   - [アクティブなエンゲージメント] テーブル
   - [クローズしたエンゲージメント] テーブル
   - [利用可能なすべてのエンゲージメント] カタログ

Example : エンゲージメントダッシュボード



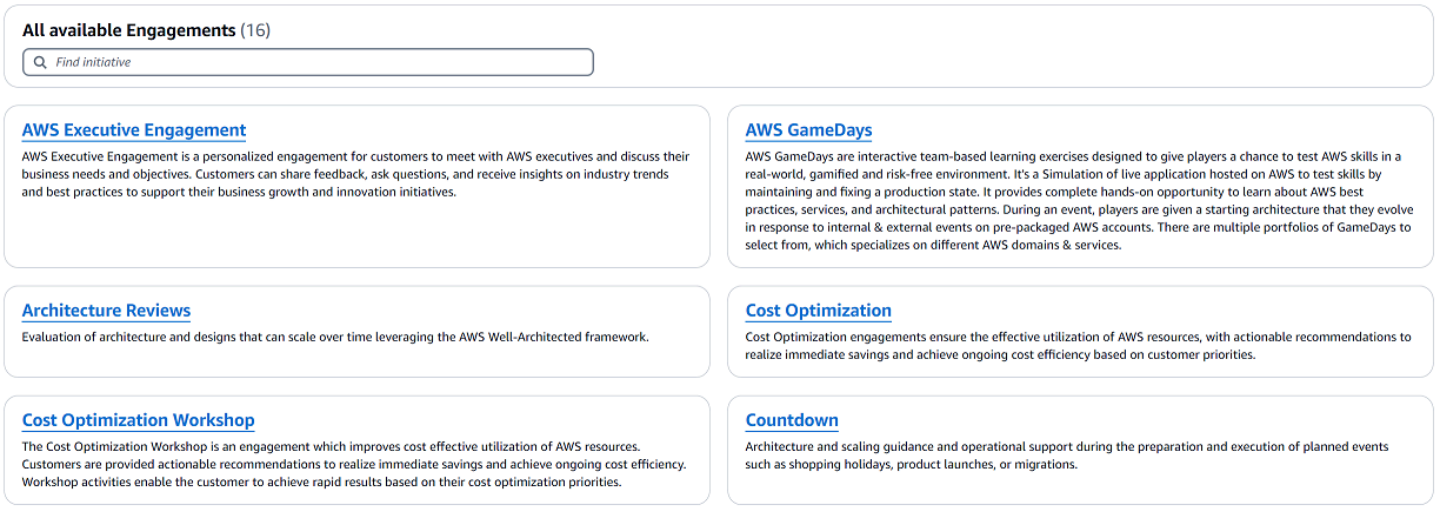
エンゲージメントタイプのカタログを表示する

エンゲージメントタイプのカタログを表示して、 AWS アカウント チームに対してリクエストできる最新のタイプのエンゲージメントを見つけることができます。

エンゲージメントタイプのカタログを表示するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページには、エンゲージメントタイプのカタログがあります。

Example : エンゲージメントタイプカタログ



エンゲージメントをリクエストする

AWS サポートプランに含まれているエンゲージメントタイプに従って、 AWS アカウント チームにエンゲージメントをリクエストできます。

エンゲージメントをリクエストするには:

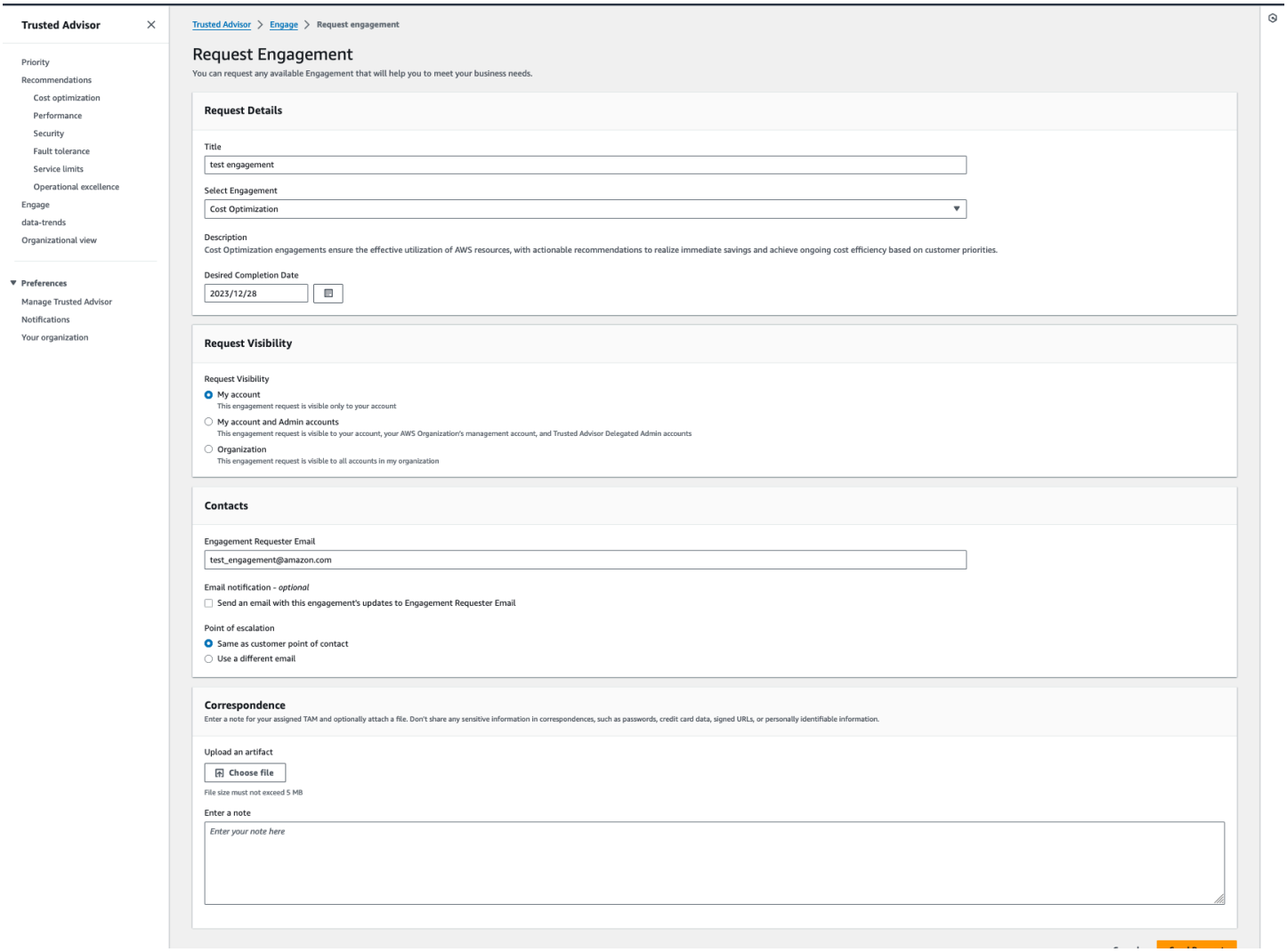
1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページで、[エンゲージメントをリクエスト] を選択します。
3. 以下の項目に入力します。

   - タイトル
   - [エンゲージメントを選択]: リクエストしたいエンゲージメントのタイプ。
   - [希望完了日]: エンゲージメントの希望完了日。各エンゲージメントタイプには異なるリードタイムがあり、最短完了希望日で計算されます。
   - リクエストの可視性:
     - [自分のアカウント]: このエンゲージメントリクエストはユーザーのアカウントでのみ表示されます。
     - マイアカウントと管理者アカウント: このエンゲージメントリクエストは、アカウント、組織の管理アカウント、およびすべての委任管理者アカウントに表示されます AWS 。
     - 組織: このエンゲージメントリクエストは、 AWS 組織内のすべてのアカウントに表示されます。

- エンゲージメントリクエスタ E メール: このエンゲージメントの主要連絡先 AWS として使用する E メールアドレス。
- E メール通知設定: エンゲージメントのリクエスターが、エンゲージメントに関する E メール通知を受け取るかどうかを選択します。
- エスカレーションポイント: このエンゲージメントにエスカレーションが必要な場合 AWS にが使用する E メールアドレス。
- [コレスポンデンス]: このエンゲージメントに関する詳細を知らせるメモと (必要に応じて) 添付ファイル。

4. [リクエストを送信] を選択します。

Example : エンゲージメントをリクエスト



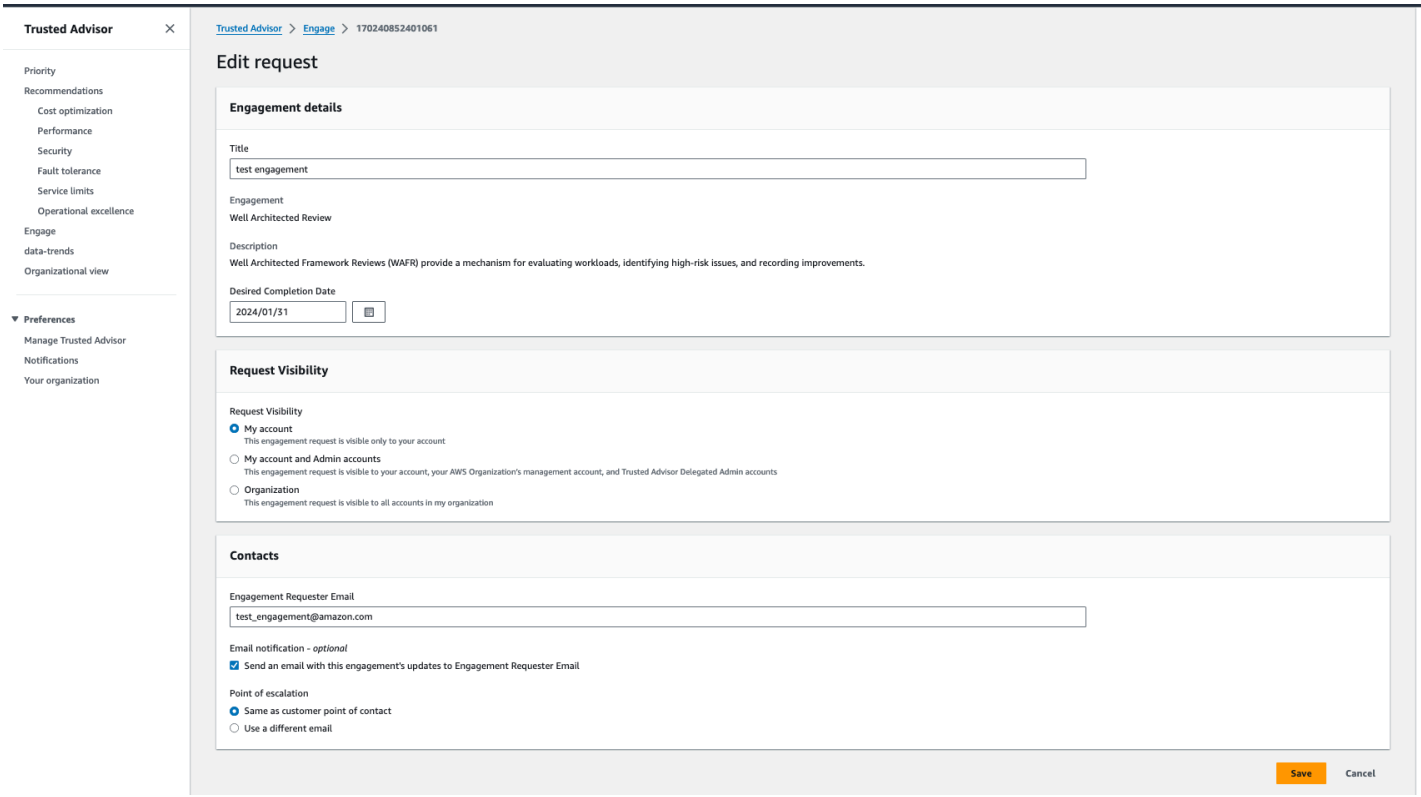
エンゲージメントを編集する

エンゲージメントリクエストの詳細を編集できます。

エンゲージメントを編集するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページで、既存のエンゲージメントを選択します。
3. [Edit] (編集) を選択します。
4. 次を編集できます。
   - タイトル
   - [希望完了日]: エンゲージメントの希望完了日。各エンゲージメントタイプには異なるリードタイムがあり、最短完了希望日で計算されます。
   - リクエストの可視性:
     - [自分のアカウント]: このエンゲージメントリクエストはユーザーのアカウントでのみ表示されます。
     - マイアカウントと管理者アカウント: このエンゲージメントリクエストは、アカウント、組織の管理アカウント、およびすべての委任管理者アカウントに表示されます AWS 。
     - 組織: このエンゲージメントリクエストは、 AWS 組織内のすべてのアカウントに表示されます。
   - エンゲージメントリクエスタ E メール: このエンゲージメントの主要連絡先 AWS として使用する E メールアドレス。
   - E メール通知設定: エンゲージメントのリクエスターが、エンゲージメントに関する E メール通知を受け取るかどうかを選択します。
   - エスカレーションポイント: このエンゲージメントにエスカレーションが必要な場合 AWS にが使用する E メールアドレス。
5. [Save] を選択します。

Example : エンゲージメントを編集する



添付ファイルとメモを送信する

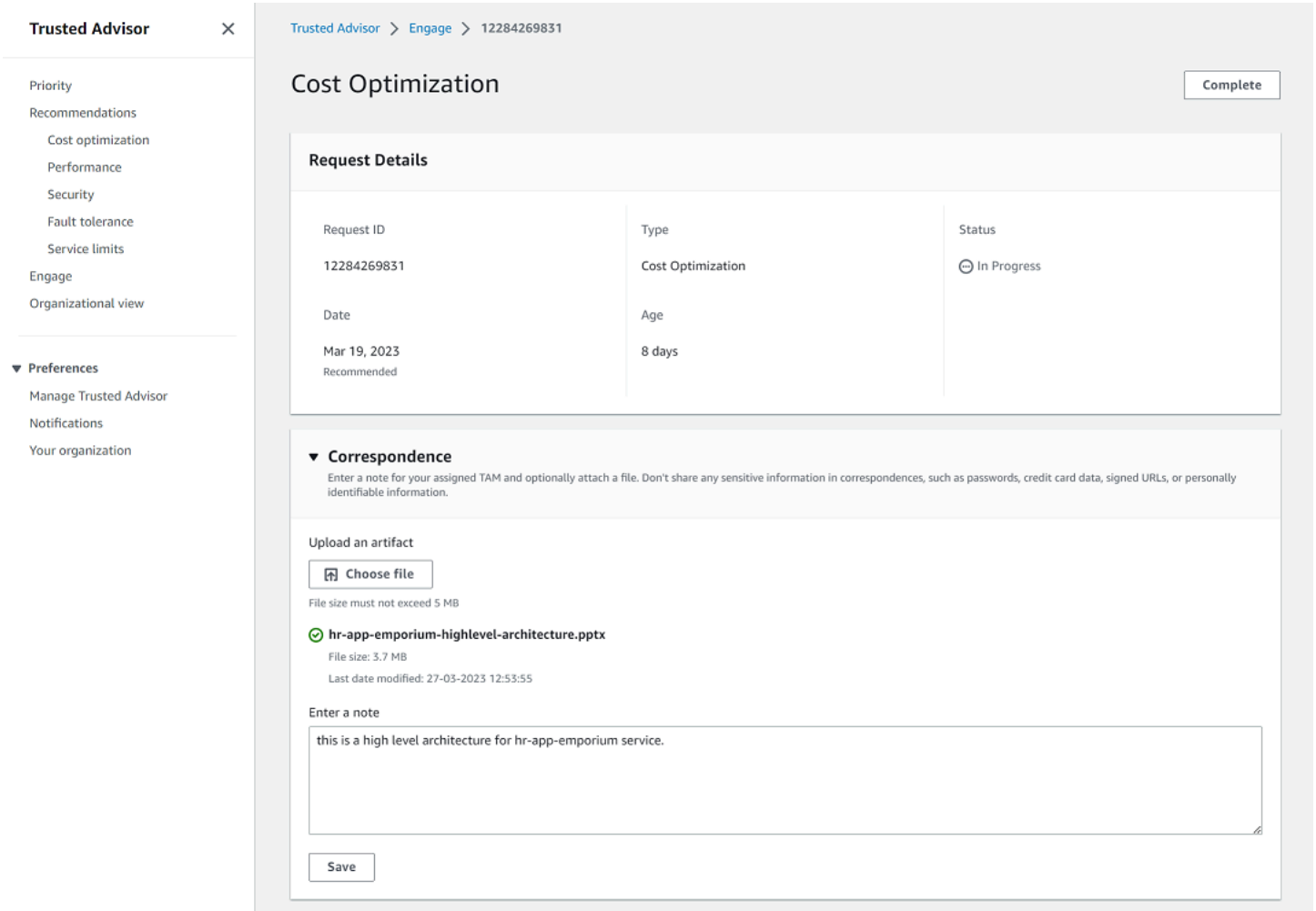
エンゲージメントリクエストをサポートするメモと添付ファイルを送信することで、個々のエンゲージメントについて AWS アカウント チームと通信できます。コミュニケーションごとに 1 つの添付ファイルとメモを含めることができ、エンゲージメントをリクエスト AWS アカウント したのと同じ のエンゲージメントにのみファイルをアタッチでき、コミュニケーションの送信後に添付ファイルやメモを削除することはできません。

アクティブなエンゲージメントリクエストにファイルをアタッチしたり、メモを追加したりするには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページで、ファイルをアタッチしたりメモを追加したりする [アクティブなエンゲージメント] の ID を選択します。
3. [コレスポンデンス] を選択してフォームを展開します。

4. 割り当てられた TAM のメモを入力し、必要に応じてファイルをアタッチします。パスワード、クレジットカードデータ、署名付き URL、個人を特定できる情報などの機密情報をコレスポンデンスで共有しないでください。
5. [Save] を選択します。

Example : エンゲージメントへのメモの追加とファイルの添付



エンゲージメントステータスを変更する

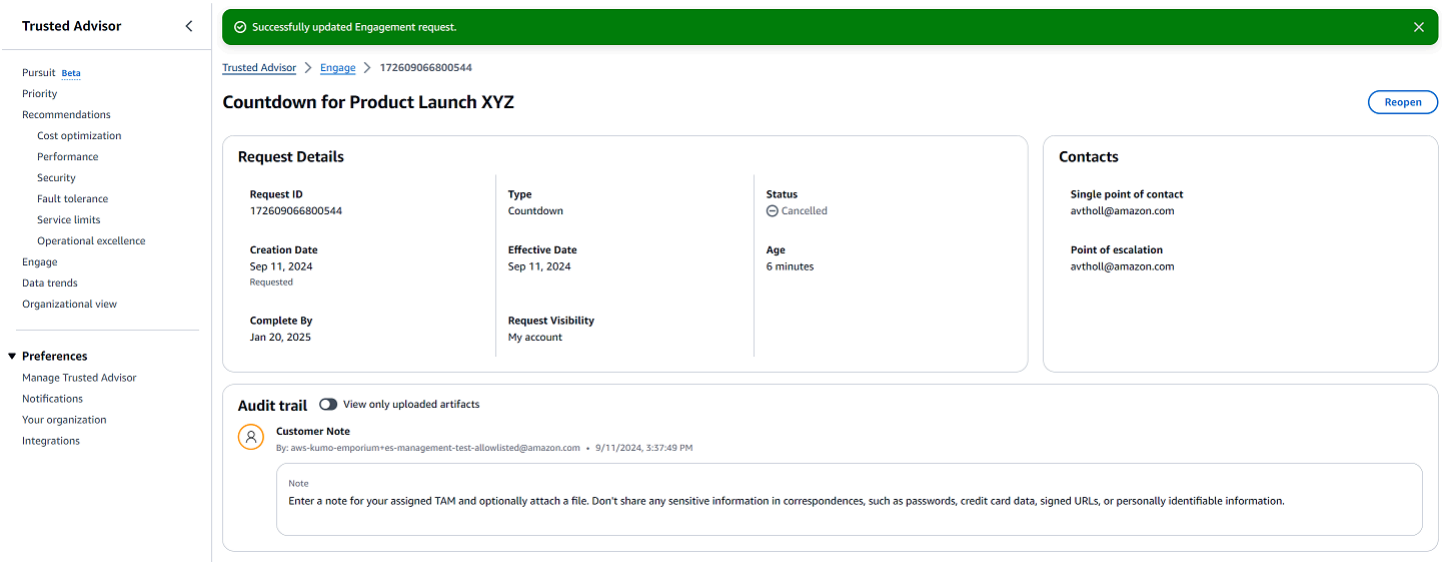
エンゲージメントのステータスを変更して、応答の保留中のエンゲージメントをキャンセルしたり、進行中のエンゲージメントを完了したり、キャンセルまたはクローズとマークされたエンゲージメントを再オープンしたりできます。

エンゲージメントのステータスを変更するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページで、ステータスを変更したい [アクティブなエンゲージメント] の ID を選択します。
3. [エンゲージメント] の詳細ページで、ステータスを [キャンセル済み] または [完了] に変更できます。

   - エンゲージメントのステータスが [応答の保留中] の場合は、[キャンセル] を選択できます。
   - エンゲージメントのステータスが [進行中] の場合は、[完了] を選択できます。
   - クローズされたエンゲージメントの場合は、[再オープン] を選択できます。キャンセルされたエンゲージメントは [応答の保留中] に移動し、完了したエンゲージメントは [進行中] に移動します。

Example : エンゲージメントのステータスの変更



推奨エンゲージメントとリクエストしたエンゲージメントを区別する

エンゲージメントのソースを特定することで、エンゲージメントを自分からリクエストしたのか、AWS アカウント チームが推奨したのかを知ることができます。

[アクティブなエンゲージメント] のさまざまなソースを表示するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページで [発効日] 列を表示し、[推奨] のエンゲージメントと [リクエスト済み] のエンゲージメントを区別します。
   - 推奨: AWS アカウント チームによって作成されたエンゲージメントリクエスト。
   - [リクエスト済み]: ユーザーが作成したエンゲージメントリクエスト。

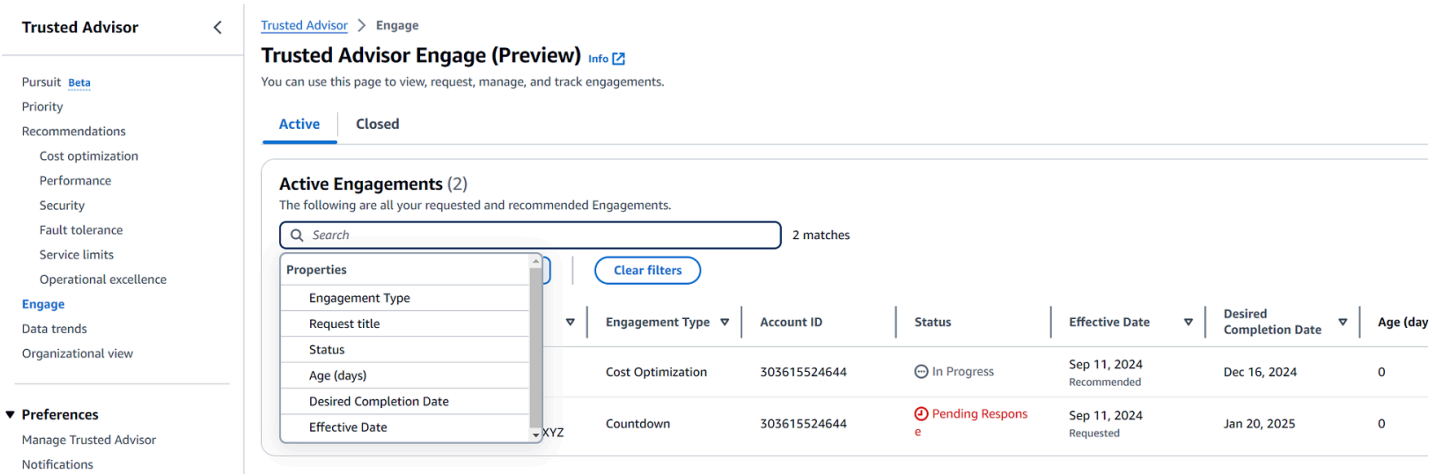
エンゲージメントを検索する

フィルターを使用して、既存のアクティブなエンゲージメントとクローズされたエンゲージメントを検索できます。

エンゲージメントを検索するには:

1. https://console.aws.amazon.com/trustedadvisor/home で Trusted Advisor コンソールにサインインします。
2. [Trusted Advisor Engage] ページでは、次のフィルターから選択できます。
   - [経過期間 (日数)]
   - [エンゲージメントタイプ]
   - [リクエストタイトル]
   - ステータス
   - 希望する完了日
   - 発効日

Example : エンゲージメントを検索する



AWS Trusted Advisor チェックリファレンス

次のリファレンスでは、すべての Trusted Advisor チェック名、説明、および IDsを表示できます。Trusted Advisor コンソールにサインインして、チェック、推奨アクション、およびそのステータスに関する詳細情報を表示することもできます。

Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合は、AWS Trusted Advisor API と AWS Command Line Interface (AWS CLI) を使用してチェックにアクセスすることもできます。詳細については、以下の各トピックを参照してください。

- Trusted Advisor API の使用を開始する
- AWS Trusted Advisor API リファレンス

> **Note**
>
> Basic Support および Developer Support プランをお持ちの場合は、 Trusted Advisor コンソールを使用して、サービス制限カテゴリのすべてのチェックとセキュリティカテゴリの次のチェックにアクセスできます。
>
> - Amazon EBS パブリックスナップショット
> - Amazon RDS パブリックスナップショット
> - Amazon S3 バケット許可
> - ルートアカウントの MFA

- セキュリティグループ — 開かれたポート

チェックカテゴリ

- コストの最適化
- パフォーマンス
- セキュリティ
- 耐障害性
- サービス制限
- 運用上の優秀性

コストの最適化

コスト最適化カテゴリの次のチェックを使用できます。

チェック名

- AWS アカウントが の一部ではない AWS Organizations
- Amazon Comprehend の使用率の低いエンドポイント
- Amazon EBS の過剰プロビジョニングボリューム
- Amazon EC2 インスタンスの統合 (Microsoft SQL Server 向け)
- 過剰にプロビジョニングされた Amazon EC2 インスタンス (Microsoft SQL サーバー向け)
- 停止している Amazon EC2 インスタンス
- Amazon EC2 リザーブドインスタンスのリース有効期限切れ
- Amazon EC2 リザーブドインスタンスの最適化
- ライフサイクルポリシーが設定されていない Amazon ECR リポジトリ。
- Amazon ElastiCache リザーブドノードの最適化
- Amazon OpenSearch Service リザーブドインスタンス最適化
- Amazon RDS アイドル DB インスタンス
- Amazon Redshift リザーブドノードの最適化
- Amazon Relational Database Service (RDS) リザーブドインスタンスの最適化
- Amazon Route 53 レイテンシーリソースレコードセット

- Amazon S3 バケットライフサイクルポリシーの設定
- Amazon S3 で不完全なマルチパートアップロードを中止するための設定
- ライフサイクルポリシーが設定されていないバージョニングが有効な Amazon S3 バケット
- AWS Lambda 過剰なタイムアウトがある関数
- AWS Lambda エラー率の高い関数
- AWS Lambda メモリサイズの過剰プロビジョニング関数
- コスト最適化に関する AWS Well-Architected のリスクの高い問題
- アイドル状態の Load Balancer
- 非アクティブ AWS Network Firewall
- 非アクティブな VPC インターフェイスエンドポイント
- 非アクティブな Gateway Load Balancer エンドポイント
- 非アクティブな NAT ゲートウェイ
- 低稼働率の Amazon EC2 インスタンス
- Savings Plan
- 関連付けられていない Elastic IP Address
- 利用頻度の低い Amazon EBS ボリューム
- 使用率の低い Amazon Redshift クラスター

AWS アカウントが の一部ではない AWS Organizations

説明

AWS アカウントが適切な管理アカウント AWS Organizations の一部であるかどうかを確認します。

AWS Organizations は、複数のアカウントを一元管理された組織に統合するための AWS アカウント管理サービスです。これにより、請求統合用にアカウントを一元的に構成し、 AWS上のワークロード規模に応じて所有権とセキュリティポリシーを実装できます。

AWS Config ルールの MasterAccountId パラメータを使用して、管理アカウント ID を指定できます。

詳細については、「 とは」を参照してください AWS Organizations。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz127`

ソース

`AWS Config Managed Rule: account-part-of-organizations`

アラート条件

黄: この AWS アカウントは の一部ではありません AWS Organizations。

[Recommended Action] (推奨されるアクション)

この AWS アカウントを の一部として追加します AWS Organizations。

詳細については、「チュートリアル: 組織の作成と設定」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon Comprehend の使用率の低いエンドポイント

説明

エンドポイントのスループット設定をチェックします。このチェックでは、エンドポイントがリアルタイム推論リクエストでアクティブに使用されていない場合に警告が表示されます。連続 15

日以上に使用されないエンドポイントは十分に使用されていないと考えられます。すべてのエンドポイントは、スループットセット 、、および エンドポイントがアクティブである時間の長さの両方に基づいて料金が発生します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`Cm24dfsM12`

アラート条件

黄: エンドポイントはアクティブですが、過去 15 日間、リアルタイム推論リクエストに使用されていません。

[Recommended Action] (推奨されるアクション)

エンドポイントが過去 15 日間使用されていない場合は、Application Autoscaling を使用してリソースのスケーリングポリシーを定義することをお勧めします。

エンドポイントにスケーリングポリシーが定義されていて、過去 30 日間使用されていない場合は、エンドポイントを削除して非同期推論を使用することを検討してください。詳細については、「Deleting an endpoint with Amazon Comprehend」(Amazon Comprehend を使用したエンドポイントの削除) を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- エンドポイント ARN
- プロビジョニングされた推論ユニット
- AutoScaling ステータス
- 理由
- 最終更新日時

Amazon EBS の過剰プロビジョニングボリューム

説明

ルックバック期間中に任意の時点で実行していた Amazon Elastic Block Store (Amazon EBS) ボリュームをチェックします。このチェックは、ワークロードに対して過剰プロビジョニングされた EBS ボリュームがある場合に警告します。ボリュームが過剰にプロビジョニングされている場合、未使用のリソースに対して料金を支払うことになります。シナリオによっては設計による最適化が低下することがありますが、多くの場合、EBS ボリュームの構成を変更することでコストを削減できます。月あたりの推定節約額は、EBS ボリュームの現在の使用率を使用して計算されます。実際の節約額は、ボリュームが一か月間存在しない場合、変動します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`C0r6dfpM03`

アラート条件

黄: ルックバック期間中に過剰にプロビジョニングされた EBS ボリューム。ボリュームが過剰にプロビジョニングされていないかどうかを判断するために、すべてのデフォルトの CloudWatch メトリクス (IOPS とスループットを含む) を考慮します。過剰にプロビジョニングされた EBS ボリュームを識別するために使用されるアルゴリズムは AWS 、 のベストプラクティスに従います。新しいパターンが特定されると、アルゴリズムが更新されます。

[Recommended Action] (推奨されるアクション)

使用量の少ないボリュームをダウンサイジングすることを検討してください。

詳細については、「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

[Report columns] (レポート列)

- ステータス

- リージョン
- ボリューム ID
- ボリュームタイプ
- ボリュームサイズ (GB)
- ボリュームベースライン IOPS
- ボリューム IOPS
- ボリュームバーストスループット
- 推奨ボリュームタイプ
- 推奨ボリュームサイズ (GB)
- 推奨ボリュームベースライン IOPS
- 推奨ボリュームバースト IOPS
- 推奨ボリュームベースラインスループット
- 推奨ボリュームバーストスループット
- ルックバック期間 (日)
- コスト削減の機会 (%)
- 月間削減額の見積もり
- 月間削減額の見積もりの通貨
- 最終更新日時

Amazon EC2 インスタンスの統合 (Microsoft SQL Server 向け)

説明

直近 24 時間以内に SQL Server を実行している Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをチェックします。このチェックでは、インスタンスの SQL Server ライセンス数が最小数よりも少ない場合に警告を受け取ります。Microsoft SQL Server Licensing Guide によると、インスタンスの vCPU が 1 つまたは 2 つのみであっても、4 つの vCPUs ライセンスの料金を支払うことになります。小さめの SQL Server インスタンスを統合して、コストの削減に役立てることができます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

Qsdfp3A4L2

アラート条件

黄: SQL Server を使用するインスタンスの vCPU の数が 4 つ未満です。

[Recommended Action] (推奨されるアクション)

小規模な SQL Server ワークロードを、少なくとも 4 個の vCPU を使用するインスタンスに統合することを検討します。

その他のリソース

- AWSでの Microsoft SQL Server
- での Microsoft ライセンス AWS
- Microsoft SQL Server ライセンスガイド

[Report columns] (レポート列)

- ステータス
- リージョン
- [インスタンス ID]
- インスタンスタイプ
- vCPU
- 最小 vCPU
- SQL Server エディション
- 最終更新日時

過剰にプロビジョニングされた Amazon EC2 インスタンス (Microsoft SQL サーバー向け)

説明

直近 24 時間以内に SQL Server を実行している Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをチェックします。SQL Server データベースには、各インスタンスについてコンピューティング性能の制限があります。SQL Server Standard エディションを使用するインスタンスでは、最大 48 個の vCPU を使用できます。SQL Server Web を使用するインスタンスでは、最大 32 個の vCPU を使用できます。このチェックでは、インスタンスがこの vCPU 制限を超えた場合に警告を受け取ります。

インスタンスが過剰にプロビジョニングされている場合は、料金全額を支払う必要があるにもかかわらず、パフォーマンスは向上しません。コストの削減に資するよう、インスタンスの数とサイズを管理できます。

推定月間削減額は、SQL Server インスタンスが使用できる vCPU の最大数を備え、かつ、オンデマンド料金を使用する同じインスタンスファミリーを使用して計算されます。実際の節約額は、リザーブドインスタンス (RI) を使用しているかどうか、またはインスタンスが 1 日実行されているかどうかに応じて異なります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`Qsdfp3A4L1`

アラート条件

- 赤: SQL Server Standard エディションを使用するインスタンスには、48 個を超える vCPU があります。
- 赤: SQL Server Web エディションを使用するインスタンスには、32 個を超える vCPU があります。

[Recommended Action] (推奨されるアクション)

SQL Server Standard エディションでは、48 個の vCPU を持つ同じインスタンスファミリーのインスタンスに変更することを検討してください。SQL Server Web エディションでは、32 個の vCPU を持つ同じインスタンスファミリーのインスタンスに変更することを検討してください。メモリを大量に消費する場合は、メモリ最適化 R5 インスタンスに変更することを検討してください。詳細については、「Best Practices for Deploying Microsoft SQL Server on Amazon EC2」(Amazon EC2 に Microsoft Amazon EC2 で SQL Server をデプロイするためのベストプラクティス) 」を参照してください。

その他のリソース

- AWSでの Microsoft SQL Server
- Launch Wizard を使用して、EC2 での SQL Server のデプロイを簡素化できます。

[Report columns] (レポート列)

- ステータス
- リージョン
- [インスタンス ID]
- インスタンスタイプ
- vCPU
- SQL Server エディション
- 最大 vCPU
- 推奨インスタンスタイプ
- 月間削減額の見積もり
- 最終更新日時

停止している Amazon EC2 インスタンス

説明

30 日以上停止している Amazon EC2 インスタンスがあるかどうかを確認します。

AllowedDays AWS Config パラメータで、許可される日数の値を指定できます。

詳細については、「インスタンスをすべて終了しているのに、Amazon EC2 の料金が請求されるのはなぜですか?」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz150`

ソース

`AWS Config Managed Rule: ec2-stopped-instance`

アラート条件

- 黄: 許可されている日数よりも長く停止している Amazon EC2 インスタンスがあります。

[Recommended Action] (推奨されるアクション)

30 日以上停止している Amazon EC2 インスタンスを確認します。不要なコストが発生しないように、必要のなくなったインスタンスはすべて終了してください。

詳細については、「インスタンスの終了」を参照してください。

その他のリソース

- Amazon EC2 オンデマンド料金

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EC2 リザーブドインスタンスのリース有効期限切れ

説明

30 日以内に有効期限が切れる Amazon EC2 リザーブドインスタンスのチェック、または過去 30 日間に有効期限が切れた Amazon EC2 リザーブドインスタンスのチェック。

リザーブドインスタンスは、自動的に更新されません。予約の対象となる Amazon EC2 インスタンスを引き続き中断なく使用できますが、オンデマンド料金が適用されます。新しいリザーブドインスタンスに有効期限が切れたインスタンスと同じパラメータを設定するか、別のパラメータを持つリザーブドインスタンスを購入することができます。

月あたりの推定節約額は、同じインスタンスタイプのオンデマンド料金とリザーブドインスタンス料金の差額です。

チェック ID

`1e93e4c0b5`

アラート条件

- 黄: リザーブドインスタンスのリースが 30 日以内に期限切れになります。
- 黄: リザーブドインスタンスのリースが過去 30 日間で期限切れになりました。

[Recommended Action] (推奨されるアクション)

期限切れが近いリザーブドインスタンスを交換するために、新しいリザーブドインスタンスを購入することを検討してください。詳細については、「リザーブドインスタンスの購入方法」および「リザーブドインスタンスの購入」を参照してください。

その他のリソース

- リザーブドインスタンス
- インスタンスタイプ

[Report columns] (レポート列)

- ステータス
- ゾーン
- インスタンスタイプ
- プラットフォーム
- Instance Count
- 現在の月額コスト

- 月間削減額の見積もり
- 有効期限日
- Reserved Instance ID
- 理由

Amazon EC2 リザーブドインスタンスの最適化

説明

を使用する上で重要な点は AWS 、リザーブドインスタンス (RI) の購入とオンデマンドインスタンスの使用のバランスを取ることです。このチェックは、オンデマンドインスタンスの使用で発生するコストの削減に役立つ RI のレコメンデーションを示します。

このレコメンデーションは、過去 30 日間のオンデマンドの使用量を分析することによって作成されます。その後、使用量は、予約の対象となるカテゴリに分類されます。使用量の生成されたカテゴリ内の予約のすべての組み合わせがシミュレートされ、購入する RI の各タイプごとの推奨数が特定されます。このシミュレーションと最適化のプロセスにより、お客様のコストを最大限に節約できます。このチェックでは、スタンダードリザーブドインスタンスに基づくレコメンデーションと一部前払い支払いオプションについて説明します。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

cX3c2R1chu

アラート条件

黄: 部分的な前払い RI の使用を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

より詳細でカスタマイズされた推奨事項については、Cost Explorer ページを参照してください。さらに、「buying guide」(購入ガイド) を参照して、RI の購入方法と利用可能なオプションを理解しましょう。

その他のリソース

- RI と、RI によりどのようにコストを節約できるかについての情報は、こちらをご覧ください。

- この推奨事項の詳細については、「 Trusted Advisor のよくある質問」の「Reserved Instance Optimization Check Questions」(リザーブドインスタンスの最適化チェックに関する質問) を参照してください。

[Report columns] (レポート列)

- リージョン
- インスタンスタイプ
- プラットフォーム
- 購入する RI の推奨数
- 想定される RI の平均使用量
- 推定節約額とレコメンデーション (月額)
- RI の前払いコスト
- RI の推定コスト (月額)
- 推奨 RI 購入後の推定オンデマンドコスト (月額)
- 推定損益分岐点 (月額)
- ルックバック期間 (日)
- 期間 (年)

ライフサイクルポリシーが設定されていない Amazon ECR リポジトリ。

説明

プライベート Amazon ECR リポジトリに少なくとも 1 つのライフサイクルポリシーが設定されているかどうかを確認します。ライフサイクルポリシーでは、古いまたは未使用のコンテナイメージを自動的にクリーンアップする一連のルールを定義することができます。これにより、イメージのライフサイクル管理を制御できるようになり、Amazon ECR リポジトリをより適切に整理し、全体的なストレージコストを削減できます。

詳細については、「ライフサイクルポリシー」を参照してください。

チェック ID

```
c18d2gz128
```

ソース

```
AWS Config Managed Rule: ecr-private-lifecycle-policy-configured
```

アラート条件

黄: Amazon ECR プライベートリポジトリにライフサイクルポリシーが設定されていません。

[Recommended Action] (推奨されるアクション)

プライベート Amazon ECR リポジトリに少なくとも 1 つのライフサイクルポリシーを作成することを検討してください。

詳細については、「ライフサイクルポリシーの作成」を参照してください。

その他のリソース

- ライフサイクルポリシー
- ライフサイクルポリシーの作成
- ライフサイクルポリシーの例

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon ElastiCache リザーブドノードの最適化

説明

ElastiCache の使用状況をチェックし、リザーブドノードの購入に関するレコメンデーションを示します。このレコメンデーションは、ElastiCache オンデマンドの使用で発生するコストを削減するために提供されます。このレコメンデーションは、過去 30 日間のオンデマンドの使用量を分析することによって作成されます。

この分析を使用して、生成された使用状況カテゴリの予約のすべての組み合わせがシミュレートされます。これにより、削減額が最大になるように、購入するリザーブドノードの各タイプ数が推奨されます。このチェックは、1 年または 3 年のコミットメントでの一部前払いオプションに基づくレコメンデーションをカバーします。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

`h3L1otH3re`

アラート条件

黄: ElastiCache リザーブドノードの購入を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

詳細な推奨事項、カスタマイズオプション (ルックバック期間、支払いオプションなど)、および ElastiCache リザーブドノードの購入については、Cost Explorer ページを参照してください。

その他のリソース

- ElastiCache リザーブドノードと、ElastiCache リザーブドノードによりどのようにコストを節約できるかについての情報は、こちらをご覧ください。
- この推奨事項の詳細については、「 Trusted Advisor のよくある質問」の「Reserved Instance Optimization Check Questions」(リザーブドインスタンスの最適化チェックに関する質問) を参照してください。
- フィールドの詳細については、Cost Explorer のドキュメントを参照してください。

[Report columns] (レポート列)

- リージョン
- ファミリー
- ノードの種類
- 製品の説明
- 購入するリザーブドノードの推奨数
- リザーブドノードの想定平均使用量
- 推定節約額とレコメンデーション (月額)
- リザーブドノードの前払いコスト
- リザーブドノードの推定コスト (月額)
- 推奨されるリザーブドノードの購入後の推定オンデマンドコスト (月額)
- 推定損益分岐点 (月額)
- ルックバック期間 (日)
- 期間 (年)

Amazon OpenSearch Service リザーブドインスタンス最適化

説明

Amazon OpenSearch Service の使用状況を確認して、リザーブドインスタンスの購入に関するレコメンデーションを提供します。このレコメンデーションは、OpenSearch オンデマンドの使用で発生するコストを削減するために提供されます。このレコメンデーションは、過去 30 日間のオンデマンドの使用量を分析することによって作成されます。

この分析を使用して、生成された使用状況カテゴリの予約のすべての組み合わせがシミュレートされます。これにより、削減額が最大になるように、購入するリザーブドインスタンスの各タイプ数を推奨することができます。このチェックは、1 年または 3 年のコミットメントでの一部前払いオプションに基づくレコメンデーションをカバーします。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

`7ujm6yhn5t`

アラート条件

黄: Amazon OpenSearch Service のリザーブドインスタンスの購入を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

詳細な推奨事項、カスタマイズオプション (ルックバック期間、支払いオプションなど)、および Amazon OpenSearch Service リザーブドインスタンスの購入については、Cost Explorer ページを参照してください。

その他のリソース

- Amazon OpenSearch Service リザーブドインスタンスと、Amazon OpenSearch Service リザーブドインスタンスによりどのようにコストを節約できるかについての情報は、こちらをご覧ください。
- この推奨事項の詳細については、「 Trusted Advisor のよくある質問」の「Reserved Instance Optimization Check Questions」(リザーブドインスタンスの最適化チェックに関する質問) を参照してください。
- フィールドの詳細については、Cost Explorer のドキュメントを参照してください。

[Report columns] (レポート列)

- リージョン

- インスタンスクラス
- インスタンスサイズ
- 購入するリザーブドインスタンスの推奨数
- リザーブドインスタンスの想定平均使用量
- 推定節約額とレコメンデーション (月額)
- リザーブドインスタンスの前払いコスト
- リザーブドインスタンスの推定コスト (月額)
- 推奨されるリザーブドインスタンスの購入後の推定オンデマンドコスト (月額)
- 推定損益分岐点 (月額)
- ルックバック期間 (日)
- 期間 (年)

Amazon RDS アイドル DB インスタンス

説明

アイドル状態と思われるデータベース (DB) インスタンスに対する Amazon Relational Database Service (Amazon RDS) の設定をチェックします。

DB インスタンスの接続が長時間にわたって確立されていない場合は、インスタンスを削除してコストを削減できます。過去 7 日間にインスタンスが接続していない DB インスタンスはアイドル状態と見なされます。インスタンス上のデータの永続的ストレージが必要な場合は、低コストのオプション (DB スナップショットの作成や保持など) を使用できます。手動で作成された DB スナップショットは、ユーザーが削除するまで保持されます。

チェック ID

`Ti39halfu8`

アラート条件

黄: アクティブな DB インスタンスは、過去 7 日間に接続されていません。

[Recommended Action] (推奨されるアクション)

アイドル状態の DB インスタンスのスナップショットを作成し、停止または削除することを検討してください。DB インスタンスを停止すると、そのコストの一部が削減されますが、ストレージコストは削減されません。停止したインスタンスは、設定された保持期間に基づいて、すべての自動バックアップを保持します。通常、DB インスタンスを停止すると、インスタンスを削

除して最終的なスナップショットだけを保持する場合に比べて、追加のコストが発生します。「一時的に Amazon RDS インスタンスを停止する」および「Deleting a DB Instance with a Final Snapshot」(最終スナップショットを使用して DB インスタンスを削除する) を参照してください。

その他のリソース

バックアップと復元

[Report columns] (レポート列)

- リージョン
- DB インスタンス名
- マルチ AZ
- インスタンスタイプ
- プロビジョニングされたストレージ (GB)
- 最終接続から経過した日数
- 推定月間節約額 (オンデマンド)

Amazon Redshift リザーブドノードの最適化

説明

Amazon Redshift の使用量をチェックし、リザーブドノードの購入に関するレコメンデーションを示して、Amazon Redshift オンデマンドの使用によって発生するコストを削減します。

このレコメンデーションは、過去 30 日間のオンデマンドの使用量を分析することによって生成されます。この分析を使用して、生成された使用状況カテゴリの予約のすべての組み合わせがシミュレートされます。これにより、削減額が最大になるように、購入するリザーブドノードの各タイプの最適数が推奨されます。このチェックは、1 年または 3 年のコミットメントでの一部前払いオプションに基づくレコメンデーションをカバーします。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

`1qw23er45t`

アラート条件

黄: Amazon Redshift リザーブドノードの購入を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

詳細な推奨事項、カスタマイズオプション (ルックバック期間、支払いオプションなど)、および Amazon Redshift リザーブドノードの購入については、Cost Explorer ページを参照してください。

その他のリソース

- Amazon Redshift リザーブドノードと、Amazon Redshift リザーブドノードによりどのようにコストを節約できるかについての情報は、こちらをご覧ください。
- この推奨事項の詳細については、「 Trusted Advisor のよくある質問」の「Reserved Instance Optimization Check Questions」(リザーブドインスタンスの最適化チェックに関する質問) を参照してください。
- フィールドの詳細については、Cost Explorer のドキュメントを参照してください。

[Report columns] (レポート列)

- リージョン
- ファミリー
- ノードの種類
- 購入するリザーブドノードの推奨数
- リザーブドノードの想定平均使用量
- 推定節約額とレコメンデーション (月額)
- リザーブドノードの前払いコスト
- リザーブドノードの推定コスト (月額)
- 推奨されるリザーブドノードの購入後の推定オンデマンドコスト (月額)
- 推定損益分岐点 (月額)
- ルックバック期間 (日)
- 期間 (年)

Amazon Relational Database Service (RDS) リザーブドインスタンスの最適化

説明

RDS の使用量をチェックし、RDS オンデマンドの使用によって発生するコストの削減に役立つリザーブドインスタンスの購入に関するレコメンデーションを示します。

このレコメンデーションは、過去 30 日間のオンデマンドの使用量を分析することによって生成されます。この分析を使用して、生成された使用状況カテゴリの予約のすべての組み合わせがシミュレートされます。これにより、削減額が最大になるように、購入するリザーブドインスタンスの各タイプの最適数が推奨されます。このチェックは、1 年または 3 年のコミットメントでの一部前払いオプションに基づくレコメンデーションをカバーします。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

1qazXsw23e

アラート条件

黄: Amazon RDS リザーブドインスタンスの購入を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

詳細な推奨事項、カスタマイズオプション (ルックバック期間、支払いオプションなど)、および Amazon RDS リザーブドインスタンスの購入については、Cost Explorer ページを参照してください。

その他のリソース

- Amazon RDS リザーブドインスタンスと、Amazon RDS リザーブドインスタンスによりどのようにコストを節約できるかについての情報は、こちらをご覧ください。
- この推奨事項の詳細については、「 Trusted Advisor のよくある質問」の「Reserved Instance Optimization Check Questions」(リザーブドインスタンスの最適化チェックに関する質問) を参照してください。
- フィールドの詳細については、Cost Explorer のドキュメントを参照してください。

[Report columns] (レポート列)

- リージョン
- ファミリー
- インスタンスタイプ
- ライセンスモデル
- データベースの編集
- データベースエンジン
- デプロイオプション

- 購入するリザーブドインスタンスの推奨数
- リザーブドインスタンスの想定平均使用量
- 推定節約額とレコメンデーション (月額)
- リザーブドインスタンスの前払いコスト
- リザーブドインスタンスの推定コスト (月額)
- 推奨されるリザーブドインスタンスの購入後の推定オンデマンドコスト (月額)
- 推定損益分岐点 (月額)
- ルックバック期間 (日)
- 期間 (年)

Amazon Route 53 レイテンシーリソースレコードセット

説明

非効率的に設定されている Amazon Route 53 レイテンシーレコードセットをチェックします。

Amazon Route 53 がネットワークレイテンシーが最も低い AWS リージョン にクエリをルーティングできるようにするには、異なるリージョンの特定のドメイン名 (example.com など) のレイテンシーリソースレコードセットを作成する必要があります。1 つのドメイン名に対してレイテンシーリソースレコードセットを 1 つだけ作成すると、すべてのクエリが 1 つのリージョンにルーティングされ、レイテンシーベースルーティングの追加料金が発生しますが、メリットはありません。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`51fC20e7I2`

アラート条件

黄: 特定のドメイン名用に設定されているレイテンシーリソースレコードセットは 1 つだけです。

[Recommended Action] (推奨されるアクション)

複数のリージョンにリソースがある場合は、それぞれのリージョンにレイテンシーリソースレコードセットを定義してください。「レイテンシーに基づくルーティング」を参照してください。

リソースが 1 つのみの場合は AWS リージョン、複数のリソースを作成し AWS リージョン 、それぞれにレイテンシーリソースレコードセットを定義することを検討してください。「レイテンシーベースのルーティング」を参照してください。

複数の を使用しない場合は AWS リージョン、シンプルなリソースレコードセットを使用する必要があります。「Working with Resource Record Sets」(リソースレコードセットを使用する) を参照してください。

その他のリソース

- Amazon Route 53 デベロッパーガイド
- Amazon Route 53 の料金

[Report columns] (レポート列)

- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名
- リソースレコードセットのタイプ

Amazon S3 バケットライフサイクルポリシーの設定

説明

Amazon S3 バケットにライフサイクルポリシーが設定されているかどうかを確認します。Amazon S3 ライフサイクルポリシーは、バケット内の Amazon S3 オブジェクトがそのライフサイクル全体を通して、コスト効率の高い方法で保存されることを保証します。これは、データ保持とストレージに関する規制要件を満たすために重要です。ポリシー設定は、Amazon S3 サービスがオブジェクトのグループに適用するアクションを定義するルールセットです。ライフサイクルポリシーを利用することで、自動でオブジェクトを低コストのストレージクラスに移行したり、古くなったときに削除したりできます。例えば、オブジェクトを作成してから 30 日後に Amazon S3 Standard-IA ストレージに移行したり、1 年後に Amazon S3 Glacier に移行したりできます。

また、オブジェクトの有効期限を定義して、一定の期間が経過すると Amazon S3 がユーザーに代わってオブジェクトを削除することもできます。

AWS Config ルールのパラメータを使用してチェック設定を調整できます。

詳細については、「Managing your storage lifecycle」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz100`

ソース

`AWS Config Managed Rule: s3-lifecycle-policy-check`

アラート条件

黄: Amazon S3 バケットにライフサイクルポリシーが設定されていません。

[Recommended Action] (推奨されるアクション)

Amazon S3 バケットにライフサイクルポリシーが設定されていることを確認してください。

組織に保持ポリシーがない場合は、Amazon S3 Intelligent-Tiering を使用してコストを最適化することを検討してください。

Amazon S3 ライフサイクルポリシーを定義する方法については、「バケットのライフサイクル設定の指定」を参照してください。

Amazon S3 Intelligent-Tiering に関する情報については、「Amazon S3 Intelligent-Tiering ストレージクラス」を参照してください。

その他のリソース

バケットのライフサイクル設定の指定

S3 ライフサイクル設定の例

[Report columns] (レポート列)

- ステータス
- リージョン

- リソース
- AWS Config ルール
- 入力パラメータ

Amazon S3 で不完全なマルチパートアップロードを中止するための設定

説明

各 Amazon S3 バケットで、7 日後に未完了のマルチパートアップロードを中止するライフサイクルルールが設定されていることを確認します。ライフサイクルルールを使用してこれらの不完全なアップロードを中止し、関連するストレージを削除することをお勧めします。

> **Note**
>
> このチェックの結果は毎日 1 回以上自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。変更が表示されるまでに数時間かかる場合があります。ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、 `BatchUpdateRecommendationResourceExclusion` API を使用して 1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

チェック ID

`c1cj39rr6v`

アラート条件

黄色: ライフサイクルを設定したバケットに、7 日後に未完了のマルチパートアップロードをすべて中止するライフサイクルルールが含まれていません。

[Recommended Action] (推奨されるアクション)

未完了のマルチパートアップロードをすべてクリーンアップするライフサイクルルールが含まれていない状態で、バケットのライフサイクルの設定を確認します。24 時間経過しても完了しないアップロードが完了する可能性はほぼありません。こちらをクリックして、ライフサイクルルールを作成するための手順に従ってください。この手順をバケット内のすべてのオブジェクトに適用することをお勧めします。バケット内の選択したオブジェクトに他のライフサイクルアクションを適用する必要がある場合は、異なるフィルターを使用して複数のルールを設定できます。詳

細については、Storage Lens ダッシュボードを確認するか、ListMultipartUpload API を呼び出してください。

その他のリソース

ライフサイクル設定の作成

不完全なマルチパートアップロードを検出および削除し、Amazon S3 のコストを削減する

マルチパートアップロードを使用したオブジェクトのアップロードとコピー

ライフサイクル設定の要素

ライフサイクルアクションを記述する要素

マルチパートアップロードを中止するライフサイクル設定

[Report columns] (レポート列)

- ステータス
- リージョン
- バケット名
- バケット ARN
- 不完全な MPU を削除するためのライフサイクルルール
- 開始後の日数
- 最終更新日時

ライフサイクルポリシーが設定されていないバージョニングが有効な Amazon S3 バケット

説明

バージョニングが有効化な Amazon S3 バケットにライフサイクルポリシーが設定されているかどうかを確認します。

詳細については、「Managing your storage lifecycle」を参照してください。

AWS Config ルールの bucketNames パラメータを使用して、チェックするバケット名を指定できます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

チェック ID

```
c18d2gz171
```

ソース

```
AWS Config Managed Rule: s3-version-lifecycle-policy-check
```

アラート条件

黄: バージョニングが有効な Amazon S3 バケットにライフサイクルポリシーが設定されていません。

[Recommended Action] (推奨されるアクション)

オブジェクトがライフサイクル全体を通して、コスト効率の高い方法で保存されるように管理するには、Amazon S3 バケットのライフサイクルを設定してください。

詳細については、「バケットのライフサイクル設定の指定」を参照してください。

その他のリソース

Managing your storage lifecycle

バケットのライフサイクル設定の指定

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ

- 最終更新日時

AWS Lambda 過剰なタイムアウトがある関数

説明

高いコストの原因となる高いタイムアウト率の Lambda 関数をチェックします。

Lambda 料金はランタイムと関数に対するリクエストの数に基づきます。関数のタイムアウトが発生すると、再試行が行われる可能性があるエラーが生じます。関数を再試行すると、追加のリクエストとランタイムの料金が発生します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`L4dfs2Q3C3`

アラート条件

黄: 過去 7 日間の任意の日のタイムアウトにより、呼び出しの 10% 超が エラーで終了する関数。

[Recommended Action] (推奨されるアクション)

機能ログ記録と X-ray トレースを検査して、関数の使用時間が長くなっている原因を特定します。API コールやデータベース接続の前後など、関連する部分のコードでログ記録を実施します。デフォルトでは、 AWS SDK クライアントのタイムアウトは、設定された関数の期間よりも長くなる場合があります。API および SDK 接続クライアントを調整して、関数タイムアウト内に再試行または失敗するようにします。想定期間が設定されたタイムアウトより長い場合は、関数のタイムアウト設定を引き上げることができます。詳細については、「Lambda アプリケーションのモニタリングとトラブルシューティング」を参照してください。

その他のリソース

- Lambda アプリケーションのモニタリングとトラブルシューティング

- Lambda Function Retry Timeout SDK
- AWS Lambda で を使用する AWS X-Ray
- の Amazon CloudWatch logs へのアクセス AWS Lambda
- のエラープロセッササンプルアプリケーション AWS Lambda

[Report columns] (レポート列)

- ステータス
- リージョン
- 関数 ARN
- 最大日次タイムアウトレート
- 最大日次タイムアウトレートの日付
- 平均日次タイムアウトレート
- 関数タイムアウト設定 (ミリ秒)
- コンピューティングコストの日次損失
- 平均日次呼び出し
- 当日の呼び出し
- 当日のタイムアウトレート
- 最終更新日時

AWS Lambda エラー率の高い関数

説明

高いコストの原因となる高いエラー率の Lambda 関数をチェックします。

Lambda 料金は関数のリクエストの数と集計ランタイムに基づきます。関数エラーは、追加料金が発生する再試行を引き起こす可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

L4dfs2Q3C2

アラート条件

黄: 過去 7 日間の任意の日に、呼び出しの 10% 超がエラーで終了する関数。

[Recommended Action] (推奨されるアクション)

エラーを低減するために、次のガイドラインを検討します。関数エラーには、関数のコードによって返されるエラーと、関数のランタイムによって返されるエラーが含まれます。

Lambda エラーのトラブルシューティングに役立つように、Lambda は Amazon CloudWatch やなどのサービスと統合されています AWS X-Ray。ログやメトリクス、アラーム、関数コード内の問題を迅速に検出および特定する X-Ray トレーシング、API またはアプリケーションをサポートするその他のリソースを組み合わせて使用することができます。詳細については、「Lambda アプリケーションのモニタリングとトラブルシューティング」を参照してください。

特定のランタイムでのエラー処理の詳細については、「エラー処理と AWS Lambdaでの自動再試行」を参照してください。

その他のトラブルシューティングについては、「Lambda における問題のトラブルシューティング」を参照してください。

AWS Lambda パートナーが提供するモニタリングおよびオブザーバビリティツールのエコシステムから選択することもできます。詳細については、「AWS Lambda パートナー」を参照してください。

その他のリソース

- エラー処理と AWS Lambdaでの自動再試行
- Lambda アプリケーションのモニタリングとトラブルシューティング
- Lambda Function Retry Timeout SDK
- Lambda における問題のトラブルシューティング
- API 呼び出しエラー
- のエラープロセッササンプルアプリケーション AWS Lambda

[Report columns] (レポート列)

- ステータス
- リージョン
- 関数 ARN

- 最大日次エラーレート
- 最大エラーレートの日付
- 平均日次エラーレート
- コンピューティングコストの日次損失
- 当日の呼び出し
- 当日のエラーレート
- *1 日あたりの平均呼び出し数
- 最終更新日時

AWS Lambda メモリサイズの過剰プロビジョニング関数

説明

ルックバック期間中に少なくとも 1 回呼び出された AWS Lambda 関数を確認します。このチェックは、Lambda 関数がメモリサイズに関して過剰プロビジョニングされた場合に警告します。メモリサイズに対して過剰プロビジョニングされた Lambda 関数がある場合、未使用のリソースに対して料金を支払うことになります。シナリオによっては設計による最適化が低下することがありますが、多くの場合、Lambda 関数のメモリ構成を変更することでコストを削減できます。月あたりの推定節約額は、Lambda 関数の現在の使用率を使用して計算されます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`COr6dfpM05`

アラート条件

黄: ルックバック期間中にメモリサイズに対して過剰にプロビジョニングされた Lambda 関数。Lambda 関数が過剰にプロビジョニングされていないかどうかを判断するために、その関数

のすべてのデフォルト CloudWatch メトリクスを考慮します。メモリサイズについて過剰にプロビジョニングされた Lambda 関数を識別するために使用されるアルゴリズムは、 AWS のベストプラクティスに従います。新しいパターンが特定されると、アルゴリズムが更新されます。

[Recommended Action] (推奨されるアクション)

Lambda 関数のメモリサイズを小さくすることを検討してください。

詳細については、「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- 関数名
- 関数バージョン
- メモリサイズ (MB)
- 推奨メモリサイズ (MB)
- ルックバック期間 (日)
- コスト削減の機会 (%)
- 月間削減額の見積もり
- 月間削減額の見積もりの通貨
- 最終更新日時

コスト最適化に関する AWS Well-Architected のリスクの高い問題

説明

コスト最適化の柱で、ワークロードに関するリスクの高い問題 (HRI) をチェックします。このチェックは、お客様の AWS-Well Architected レビューに基づきます。チェック結果は、AWS Well-Architected でワークロード評価を完了したかどうかによって異なります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`Wxdfp4B1L1`

アラート条件

- 赤: AWS Well-Architected のコスト最適化の柱で、少なくとも 1 つのアクティブな高リスクの問題が特定されました。
- 緑: AWS Well-Architected のコスト最適化の柱でアクティブな高リスクの問題は検出されませんでした。

[Recommended Action] (推奨されるアクション)

AWS Well-Architected は、ワークロード評価中に高リスクの問題を検出しました。これらの問題は、リスクを軽減し、費用を節約する機会を提示します。AWS Well-Architected ツールにサインインして、回答を確認し、アクティブな問題を解決するためのアクションを実行します。

[Report columns] (レポート列)

- ステータス
- リージョン
- ワークロードの ARN
- ワークロード名
- レビュー担当者名
- ワークロードタイプ
- ワークロードの開始日
- ワークロードの最終変更日
- コスト最適化について特定された HRI の数
- コスト最適化について解決された HRI の数
- コスト最適化について回答された質問の数
- コスト最適化の柱の質問の総数
- 最終更新日時

アイドル状態の Load Balancer

説明

アイドル状態のロードバランサーについて Elastic Load Balancing の設定をチェックします。

設定されているロードバランサーには料金が発生します。ロードバランサーにバックエンドインスタンスが関連付けられていない場合、またはネットワークトラフィックが厳しく制限されている場合、ロードバランサーは効果的に使用されていません。現在、このチェックは ELB サービス内の Classic Load Balancer タイプのみをチェックします。他の ELB タイプ (Application Load Balancer、Network Load Balancer) は含まれません。

チェック ID

`hjLMh88uM8`

アラート条件

- 黄: ロードバランサーにはアクティブなバックエンドインスタンスがありません。
- 黄: ロードバランサーには正常なバックエンドインスタンスがありません。
- 黄: 過去 7 日間において、ロードバランサーの 1 日あたりのリクエスト数は 100 件未満です。

[Recommended Action] (推奨されるアクション)

ロードバランサーにアクティブなバックエンドインスタンスがない場合は、インスタンスを登録するか、ロードバランサーを削除することを検討してください。「Registering Your Amazon EC2 Instances with Your Load Balancer」(Amazon EC2 インスタンスをロードバランサーに登録する) または「Delete Your Load Balancer」(ロードバランサーを削除する) を参照してください。

ロードバランサーに正常なバックエンドインスタンスがない場合は、「Troubleshooting Elastic Load Balancing: Health Check Configuration」(Elastic Load Balancing のトラブルシューティング: ヘルスチェックの設定) を参照してください。

ロードバランサーのリクエスト数が少ない場合は、ロードバランサーを削除することを検討してください。「ロードバランサーの削除」を参照してください。

その他のリソース

- ロードバランサーの管理
- Elastic Load Balancing をトラブルシューティングする

[Report columns] (レポート列)

- リージョン

- ロードバランサー名
- 理由
- 月間削減額の見積もり

非アクティブ AWS Network Firewall

説明

AWS Network Firewall エンドポイントをチェックし、Network Firewall が非アクティブに見えると警告します。

Network Firewall は、すべてのエンドポイントで過去 30 日間に処理されたデータがない場合、非アクティブと見なされます。Network Firewall エンドポイントには時間単位の料金が発生します。このチェックでは、過去 30 日間に処理されたデータがない Network Firewall にアラートを送信します。未使用の Network Firewall を削除するか、アーキテクチャを更新することをお勧めします。

チェック ID

`c2v1fg0bfw`

アラート条件

- 黄: Network Firewall は過去 30 日間に 0 バイトを処理しました。
- 緑: Network Firewall は、過去 30 日間に 0 バイト以上を処理しました。

[Recommended Action] (推奨されるアクション)

Network Firewall が過去 30 日間使用されていない場合は、Network Firewall の削除を検討してください。

Transit Gateway を VPC 間通信に使用する場合は、一元化されたネットワーク検査アーキテクチャに Network Firewall をデプロイすることを検討してください。これにより、非アクティブな Network Firewall の時間単位の料金を削減できます。

その他のリソース

AWS Network Firewall の料金

を使用した検査デプロイモデル AWS Network Firewall

[Report columns] (レポート列)

- ステータス

- リージョン
- Network Firewall Arn
- VPC Id
- サブネット
- TotalBytesProcessed
- 最終更新日時

非アクティブな VPC インターフェイスエンドポイント

説明

VPC インターフェイスエンドポイントをチェックし、エンドポイントが非アクティブであると思われる場合に警告します。VPC インターフェイスエンドポイントは、過去 30 日間に処理されたデータがない場合、非アクティブと見なされます。VPC インターフェイスエンドポイントには、時間単位の料金とデータ処理コストがかかります。このチェックでは、過去 30 日間に処理されたデータが 0 の VPC インターフェイスエンドポイントについて警告します。未使用の VPC インターフェイスエンドポイントを削除するか、アーキテクチャを更新することをお勧めします。

チェック ID

`c2v1fg0jp6`

アラート条件

- 黄: VPC インターフェイスエンドポイントは過去 30 日間に 0 バイトを処理しました。
- 緑: VPC インターフェイスエンドポイントが過去 30 日間に 0 バイト以上を処理しました

[Recommended Action] (推奨されるアクション)

VPC インターフェイスエンドポイントが過去 30 日間使用されていない場合は、VPC インターフェイスエンドポイントを削除することを検討してください。

Transit Gateway を VPC 間通信に使用する場合は、VPC インターフェイスエンドポイントを一元化されたアーキテクチャにデプロイして、非アクティブな VPC インターフェイスエンドポイントの時間単位の料金を削減することを検討してください。

その他のリソース

- AWS PrivateLink 料金表
- VPC プライベートエンドポイントへの一元化されたアクセス

[Report columns] (レポート列)

- ステータス
- リージョン
- VPC エンドポイント ID
- VPC Id
- サブネット ID
- サービス名
- TotalBytesProcessed
- 最終更新日時

非アクティブな Gateway Load Balancer エンドポイント

説明

Gateway Load Balancer エンドポイントをチェックし、非アクティブに見えると警告します。Gateway Load Balancer エンドポイントは、過去 30 日間に処理されたデータがない場合、十分に活用されていないと見なされます。Gateway Load Balancer エンドポイントには、時間単位の料金とデータ処理料金がかかります。このチェックでは、過去 30 日間に処理されたデータが 0 の Gateway Load Balancer エンドポイントにアラートが送信されます。未使用の Gateway Load Balancer エンドポイントを削除するか、アーキテクチャを更新することをお勧めします。

チェック ID

`c2v1fg0k35`

アラート条件

- 黄: Gateway Load Balancer エンドポイントが過去 30 日間に 0 バイトを処理しました
- 緑: Gateway Load Balancer エンドポイントが過去 30 日間に 0 バイト以上を処理しました

[Recommended Action] (推奨されるアクション)

Gateway Load Balancer エンドポイントが過去 30 日間使用されていない場合は、VPC エンドポイントを削除することを検討してください。

Transit Gateway を VPC 間通信に使用する場合は、Gateway Load Balancer エンドポイントを集中型ネットワーク検査アーキテクチャにデプロイして、非アクティブな Gateway Load Balancer エンドポイントの時間料金を削減することを検討してください。

その他のリソース

AWS PrivateLink の料金

AWS Gateway Load Balancer と を使用した一元化された検査アーキテクチャ AWS Transit Gateway

[Report columns] (レポート列)

- ステータス
- リージョン
- VPC エンドポイント ID
- VPC Id
- サブネット ID
- サービス名
- TotalBytesProcessed
- 最終更新日時

非アクティブな NAT ゲートウェイ

説明

NAT ゲートウェイに非アクティブなゲートウェイがないかどうかを確認します。過去 30 日間にデータ (0 バイト) が処理されなかった場合、NAT ゲートウェイは非アクティブと見なされます。NAT ゲートウェイには時間単位の料金とデータ処理料金があります。

チェック ID

`c2v1fg022t`

アラート条件

- 黄: NAT ゲートウェイは過去 30 日間に 0 バイトを処理しました
- 緑: 過去 30 日間に NAT ゲートウェイが 0 バイト以上を処理しました

[Recommended Action] (推奨されるアクション)

過去 30 日間使用されておらず、VPC 外の外部ネットワークアクセスに必要ではない NAT ゲートウェイを削除することを検討してください。

Transit Gateway を VPC 間通信に使用する場合は、インターネットアーキテクチャへの出力用に一元化された NAT Gateway をデプロイすることを検討してください。これにより、非アクティブな NAT ゲートウェイからの時間単位のコストを削減できます。

その他のリソース

NAT ゲートウェイの料金

インターネットへの一元的な出力

[Report columns] (レポート列)

- ステータス
- リージョン
- NAT ゲートウェイ ID
- サブネット ID
- VPC Id
- TotalBytesFromDest
- TotalBytesFromSrc
- TotalBytes
- 最終更新日時

低稼働率の Amazon EC2 インスタンス

説明

過去 14 日間の任意の時点で実行していた Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをチェックします。このチェックでは、過去 4 日間の毎日の CPU 使用率が 10% 以下で、ネットワーク I/O が 5 MB 以下である場合にアラートが発生します。

実行中のインスタンスでは、時間単位の利用料金が発生します。シナリオによっては設計によって使用率が低下することがありますが、多くの場合、インスタンスの数とサイズを管理することでコストを削減できます。

月あたりの推定節約額は、オンデマンドインスタンスの現在の使用率、およびインスタンスが十分に活用されていない可能性のある推定日数を使用して計算されます。実際の節約額は、リザーブドインスタンスまたはスポットインスタンスを使用しているかどうか、またはインスタンスが 1 日実行されているかどうかに応じて異なります。毎日の使用量データを取得するには、このチェックのレポートをダウンロードします。

チェック ID

Qch7DwouX1

アラート条件

黄: 過去 14 日間のうち少なくとも 4 日で、インスタンスの 1 日の平均 CPU 使用率が 10% 以下で、ネットワーク I/O が 5 MB 以下でした。

[Recommended Action] (推奨されるアクション)

使用量の少ないインスタンスを停止または終了するか、Auto Scaling を使用してインスタンスの数をスケールすることを検討してください。詳細については、「インスタンスの停止と起動」、「インスタンスの終了」、および「Auto Scaling とは」を参照してください。

その他のリソース

- Amazon EC2 のモニタリング
- インスタンスメタデータとユーザーデータ
- Amazon CloudWatch ユーザーガイド
- Auto Scaling デベロッパーガイド

[Report columns] (レポート列)

- リージョン/AZ
- [インスタンス ID]
- インスタンス名
- インスタンスタイプ
- 月間削減額の見積もり
- CPU 使用率 (14 日間の平均)
- ネットワーク I/O (14 日間の平均)
- 使用率が低い日数

Savings Plan

説明

過去 30 日間の Amazon EC2、Fargate、および Lambda の使用量をチェックし、Savings Plan の購入に関するレコメンデーションを示します。このレコメンデーションにより、割引料金と引

き換えに、1 年間または 3 年間のドルで測定された 1 時間あたりの一貫した使用量をコミットできます。

これらは、より詳細なレコメンデーション情報を取得できる AWS Cost Explorer から取得されています。Cost Explorer から Savings Plans を購入することもできます。このレコメンデーションは、RI レコメンデーションの代替とみなされます。1 つのレコメンデーションのみに従うことをお勧めします。両方のレコメンデーションに従うと、オーバーコミットメントにつながる可能性があります。

このチェックは、一括請求 (コンソリデーティッドビリング) にリンクされたアカウントでは使用できません。このチェックのレコメンデーションは、支払いアカウントでのみ利用できます。

チェック ID

`vZ2c2W1srf`

アラート条件

黄: Savings Plans の購入を最適化すると、コスト削減に役立ちます。

[Recommended Action] (推奨されるアクション)

より詳細でカスタマイズされた推奨事項と Savings Plans の購入については、Cost Explorer ページを参照してください。

その他のリソース

- Savings Plan ユーザーガイド
- Savings Plans のよくある質問

[Report columns] (レポート列)

- Savings Plan タイプ
- お支払い方法
- 前払い料金
- 購入する時間単位のコミットメント
- 推定平均使用量
- 月間削減額の見積もり
- 推定節約率
- 期間 (年)
- ルックバック期間 (日)

関連付けられていない Elastic IP Address

説明

実行中の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関連付けられていない Elastic IP アドレス (EIP) をチェックします。

EIP は、動的なクラウドコンピューティングのために設計された静的 IP アドレスです。従来の静的 IP アドレスとは異なり、EIP はパブリック IP アドレスをアカウント内の別のインスタンスに再マッピングすることで、インスタンスまたはアベイラビリティーゾーンの障害をマスクします。実行中のインスタンスに関連付けられていない EIP には、わずかな料金が課されます。

チェック ID

`Z4AUBRNSmz`

アラート条件

黄: 割り当てられた Elastic IP アドレス (EIP) は、実行中の Amazon EC2 インスタンスに関連付けられていません。

[Recommended Action] (推奨されるアクション)

EIP を実行中のアクティブなインスタンスに関連付けるか、関連付けられていない EIP を解放します。詳細については、「Associating an Elastic IP Address with a Different Running Instance」(Elastic IP アドレスを別の実行中のインスタンスに関連付ける) および「Elastic IP アドレスを解放する」を参照してください。

その他のリソース

Elastic IP アドレス

[Report columns] (レポート列)

- リージョン
- IP アドレス

利用頻度の低い Amazon EBS ボリューム

説明

Amazon Elastic Block Store (Amazon EBS) ボリューム設定をチェックし、ボリュームの使用率が低いと思われる場合に警告を表示します。

課金は、ボリュームの作成時に開始されます。ボリュームが一定期間アタッチされていないままの場合や、書き込みアクティビティが非常に低い (ブートボリュームを除く) 場合、ボリュームの利用頻度が低くなります。コストを削減するには、利用頻度の低いボリュームを削除することをお勧めします。

チェック ID

DAvU99Dc4C

アラート条件

黄: ボリュームがアタッチされていないか、過去 7 日間の 1 日あたりの IOPS が 1 未満でした。

[Recommended Action] (推奨されるアクション)

コストを削減するには、スナップショットを作成してボリュームを削除することを検討してください。詳細については、「Amazon EBS スナップショットの作成」および「Amazon EBS ボリュームの削除」を参照してください。

その他のリソース

- Amazon Elastic Block Store (Amazon EBS)
- ボリュームのステータスのモニタリング

[Report columns] (レポート列)

- リージョン
- ボリューム ID
- ボリューム名
- ボリュームタイプ
- ボリュームサイズ
- 月間ストレージコスト
- スナップショット ID
- スナップショット名
- スナップショット作成後に経過した期間

> **Note**
>
> アカウントをオプトインした場合は AWS Compute Optimizer、代わりに Amazon EBS の過剰プロビジョニングボリュームチェックを使用することをお勧めします。詳細については、

「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

使用率の低い Amazon Redshift クラスター

説明

使用率が低いと思われるクラスターについて、Amazon Redshift 設定をチェックします。

Amazon Redshift クラスターが長時間接続されていない場合や、CPU の使用量が少ない場合は、低コストのオプション (クラスターのダウンサイジング、クラスターのシャットダウンと最終スナップショットの作成など) を使用できます。最終的なスナップショットは、クラスターを削除した後も保持されます。

チェック ID

`G31sQ1E9U`

アラート条件

- 黄: 実行中のクラスターは、過去 7 日間接続されていません。
- 黄: 実行中のクラスターでは、過去 7 日間の 99% で、クラスター全体の平均 CPU 使用率が 5% 未満でした。

[Recommended Action] (推奨されるアクション)

クラスターをシャットダウンして最終的なスナップショットを作成するか、クラスターをダウンサイジングすることを検討してください。「Shutting Down and Deleting Clusters」(クラスターのシャットダウンと削除) および「Resizing a Cluster」(クラスターのサイズ変更) を参照してください。

その他のリソース

Amazon CloudWatch ユーザーガイド

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター
- インスタンスタイプ
- 理由

- 月間削減額の見積もり

パフォーマンス

サービスクォータ (以前は制限と呼ばれていました) をチェックしてサービスのパフォーマンスを向上させ、プロビジョニングされたスループットを活用して使用率が高いインスタンスを監視することによって未使用のリソースを検出できます。

パフォーマンスカテゴリの次のチェックを使用できます。

チェック名

- 読み取りワークロードのプロビジョニングが不十分な Amazon Aurora DB クラスター
- Amazon DynamoDB Auto Scaling が有効化されていない
- Amazon EBS 最適化が有効化されていない
- Amazon EBS プロビジョンド IOPS (SSD) ボリュームアタッチ設定
- Amazon EBS のプロビジョニング不足ボリューム
- Amazon EC2 Auto Scaling グループが起動テンプレートに関連付けられていない
- Amazon EC2 から EBS スループット最適化
- EC2 仮想化タイプが準仮想化
- Amazon ECS メモリのハード制限
- Amazon EFS スループットモードの最適化
- Amazon RDS 自動バキュームパラメータが無効になっています
- Amazon RDS DB クラスターは最大 64 TiB のボリュームのみをサポートします
- 異なるインスタンスクラスを持つクラスター内の Amazon RDS DB インスタンス
- インスタンスサイズが異なるクラスター内の Amazon RDS DB インスタンス
- Amazon RDS DB のメモリパラメータがデフォルトと異なります
- Amazon RDS enable_index_OnlyScan パラメータは無効になっています。
- Amazon RDS enable_indexscan パラメータは無効になっています
- Amazon RDS general_logging パラメータが有効になっています
- Amazon RDS InnoDB_Change_Buffering パラメータは最適値よりも小さい値を使用しています
- Amazon RDS innodb_open_files パラメータが低いです
- Amazon RDS innodb_stats_persistent パラメータは無効になっています
- システム容量のプロビジョニングが不十分な Amazon RDS インスタンス

- Amazon RDS のマグネティックボリュームが使用中です。
- Amazon RDS パラメータグループでは Huge pages は使用されません
- Amazon RDS クエリキャッシュパラメータは有効になっています
- Amazon RDS リソース、インスタンスクラスの更新が必須です。
- Amazon RDS リソースのメジャーバージョンの更新が必須です。
- ライセンス付きのサポート終了エンジンエディションを使用する Amazon RDS リソース
- Amazon Route 53 エイリアスリソースレコードセット
- AWS Lambda メモリサイズのプロビジョニング不足関数
- AWS Lambda 同時実行制限が設定されていない関数
- パフォーマンスに関する AWS Well-Architected のリスクの高い問題
- CloudFront 代替ドメイン名
- コンテンツ配信の最適化 (CloudFront)
- CloudFront ヘッダー転送とキャッシュヒット率
- 高 CPU 使用率の Amazon EC2 インスタンス

読み取りワークロードのプロビジョニングが不十分な Amazon Aurora DB クラスター

説明

Amazon Aurora DB クラスターに、読み取りワークロードをサポートするリソースがあるかどうかを確認します。

チェック ID

`c1qf5bt038`

アラート条件

黄色:

データベース読み取りの増加: データベースの負荷が高く、データベースは行の書き込みや更新よりも多くの行を読み取っていました。

[Recommended Action] (推奨されるアクション)

クエリを調整してデータベースの負荷を軽減するか、クラスター内のライター DB インスタンスと同じインスタンスクラスとサイズを持つリーダー DB インスタンスを DB クラスターに追加することをお勧めします。現在の設定では、読み取り操作が主な原因となり、データベースの負荷

が継続的に高くなっている DB インスタンスが 1 つ以上あります。クラスターに別の DB インスタンスを追加し、読み取りワークロードを DB クラスターの読み取り専用エンドポイントに送信することで、これらの操作を分散します。

その他のリソース

Aurora DB クラスターには、読み取り専用接続のためのリーダーエンドポイントが 1 つあります。このエンドポイントは、負荷分散を使用して DB クラスターでデータベースロードの最も大きな原因になっているクエリを管理します。リーダーエンドポイントは、これらのステートメントを Aurora リードレプリカに送信し、プライマリインスタンスの負荷を軽減します。リーダーエンドポイントは、クラスター内の Aurora リードレプリカの数に応じて、同時実行可能な SELECT クエリを処理するための容量をスケールすることもできます。

詳細については、「DB クラスターに Aurora レプリカを追加する」および「Aurora DB クラスターのパフォーマンスとスケーリングの管理」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- データベース読み取り (カウント) の増加
- 最終検出期間
- 最終更新日時

Amazon DynamoDB Auto Scaling が有効化されていない

説明

自動スケーリングまたはオンデマンドが Amazon DynamoDB テーブルおよびグローバルセカンダリインデックスで有効になっているかどうかを確認します。

Amazon DynamoDB Auto Scaling は Application Auto Scaling サービスを使用し、実際のトラフィックパターンに応じてプロビジョンドスループットキャパシティをユーザーに代わって動的に調節します。これにより、テーブルまたはグローバルセカンダリインデックスで、プロビジョンされた読み込みおよび書き込み容量が拡張され、トラフィックの急激な増加をスロットリングなしに処理できるようになります。ワークロードが減ると、Application Auto Scaling はスループットを低下させ、未使用のプロビジョンされた容量に料金が発生しないようにします。

AWS Config ルールのパラメータを使用してチェック設定を調整できます。

詳細については、「DynamoDB Auto Scaling によるスループットキャパシティの自動管理」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c18d2gz136

ソース

AWS Config マネージドルール: dynamodb-autoscaling-enabled

アラート条件

黄: 自動スケーリングまたはオンデマンドが DynamoDB テーブル、グローバルセカンダリインデックス、またはその両方で有効になっていません。

[Recommended Action] (推奨されるアクション)

ワークロード要件に基づいて DynamoDB テーブルやグローバルセカンダリインデックスのプロビジョニングされたスループットを自動的にスケーリングするメカニズムがすでにある場合を除き、Amazon DynamoDB テーブルの自動スケーリングを有効にすることを検討してください。

詳細については、「AWS マネジメントコンソールと DynamoDB Auto Scaling の使用」を参照してください。

その他のリソース

DynamoDB Auto Scaling によるスループットキャパシティの自動管理

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール

- 入力パラメータ
- 最終更新日時

Amazon EBS 最適化が有効化されていない

説明

Amazon EC2 インスタンスに対して Amazon EBS 最適化が有効になっているかどうか確認します。

Amazon EBS 最適化インスタンスは、最適化された設定スタックを使用し、Amazon EBS I/O 用に専用のキャパシティを追加で提供します。このように最適化することで、Amazon EBS I/O と、インスタンスからのその他のトラフィックとの間の競合を最小に抑え、Amazon EBS ボリュームの最高のパフォーマンスを実現します。

詳細については、「Amazon EBS 最適化インスタンスを使用する」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz142`

ソース

AWS Config マネージドルール: ebs-optimized-instance

アラート条件

黄: Amazon EBS 最適化は、サポートされている Amazon EC2 インスタンスで有効になっていません。

[Recommended Action] (推奨されるアクション)

サポートされているインスタンスで Amazon EBS 最適化を有効にしてください。

詳細については、「Enable EBS optimization at launch」を参照してください。

その他のリソース

Amazon EBS 最適化インスタンス

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EBS プロビジョンド IOPS (SSD) ボリュームアタッチ設定

説明

Amazon EBS の最適化が可能で EBS 最適化されていない Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにアタッチされていないプロビジョンド IOPS (SSD) ボリュームをチェックします。

Amazon Elastic Block Store (Amazon EBS) のプロビジョンド IOPS (SSD) ボリュームは、EBS 最適化インスタンスにアタッチされている場合にのみ、予期されたパフォーマンスを提供するように設計されています。

チェック ID

`PPkZrjsH2q`

アラート条件

黄: EBS 最適化が可能な Amazon EC2 インスタンスにはプロビジョンド IOPS (SSD) ボリュームがアタッチされていますが、そのインスタンスは EBS 最適化されていません。

[Recommended Action] (推奨されるアクション)

EBS 最適化されている新しいインスタンスを作成し、ボリュームをデタッチして、そのボリュームを新しいインスタンスに再アタッチします。詳細については、「Amazon EBS-Optimized Instances」(Amazon EBS 最適化インスタンス) および「インスタンスへの Amazon EBS ボリュームのアタッチ」を参照してください。

その他のリソース

- Amazon EBS ボリュームの種類
- Amazon EBS ボリュームパフォーマンス

[Report columns] (レポート列)

- ステータス
- リージョン/AZ
- ボリューム ID
- ボリューム名
- ボリュームのアタッチ
- [インスタンス ID]
- インスタンスタイプ
- EBS 最適化

Amazon EBS のプロビジョニング不足ボリューム

説明

ルックバック期間中に任意の時点で実行していた Amazon Elastic Block Store (Amazon EBS) ボリュームをチェックします。このチェックは、ワークロードに対してプロビジョニング不足である EBS ボリュームがある場合に警告します。一貫した高い使用率は、パフォーマンスが最適化され安定していることを示しますが、アプリケーションに十分なリソースがない可能性も示唆しています。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`C0r6dfpM04`

アラート条件

黄: ルックバック期間中にプロビジョニングが不足していた EBS ボリューム。ボリュームのプロビジョニングが不足していないかどうかを判断するために、すべてのデフォルトの CloudWatch メトリクス (IOPS とスループットを含む) を考慮します。プロビジョニング不足の EBS ボリュームを識別するために使用されるアルゴリズムは、 AWS のベストプラクティスに従います。新しいパターンが特定されると、アルゴリズムが更新されます。

[Recommended Action] (推奨されるアクション)

使用量の多いボリュームをアップサイジングすることを検討してください。

詳細については、「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- ボリューム ID
- ボリュームタイプ
- ボリュームサイズ (GB)
- ボリュームベースライン IOPS
- ボリューム IOPS
- ボリュームバーストスループット
- 推奨ボリュームタイプ
- 推奨ボリュームサイズ (GB)
- 推奨ボリュームベースライン IOPS
- 推奨ボリュームバースト IOPS
- 推奨ボリュームベーススループット
- 推奨ボリュームバーストスループット
- ルックバック期間 (日)
- パフォーマンスリスク
- 最終更新日時

Amazon EC2 Auto Scaling グループが起動テンプレートに関連付けられていない

説明

Amazon EC2 Auto Scaling グループが、EC2 起動テンプレートから作成されたものかどうかを確認します。

起動テンプレートを使用して Amazon EC2 Auto Scaling グループを作成し、Auto Scaling グループの最新の機能や改善点に確実にアクセスできます。例えば、バージョニングや複数のインスタンスタイプなどです。

詳細については、「起動テンプレート」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz102`

ソース

AWS Config マネージドルール: autoscaling-launch-template

アラート条件

黄: Amazon EC2 Auto Scaling グループが有効な起動テンプレートに関連付けられていません。

[Recommended Action] (推奨されるアクション)

Amazon EC2 起動テンプレートを使用して Amazon EC2 Auto Scaling グループを作成します。

詳細については、「Auto Scaling グループの起動テンプレートを作成する」を参照してください。

その他のリソース

- 起動テンプレート

- 起動テンプレートの作成

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EC2 から EBS スループット最適化

説明

アタッチされている Amazon EC2 インスタンスの最大スループットキャパシティーによってパフォーマンスの影響を受ける可能性がある Amazon EBS ボリュームをチェックします。

パフォーマンスを最適化するには、アタッチされた EBS ボリュームの合計最大スループットよりも Amazon EC2 インスタンスの最大スループットが大きいことを確認することをお勧めします。このチェックでは、EBS 最適化インスタンスごとに前日の各 5 分間の合計 (協定世界時 (UTC) に基づく) EBS ボリュームスループットが計算され、これらの期間の半分以上の使用量が EC2 インスタンスの最大スループットの 95% を超えた場合に警告が表示されます。

チェック ID

Bh2xRR2FGH

アラート条件

黄: 前日 (UTC) に、EC2 インスタンスにアタッチされた EBS ボリュームの総スループット (メガバイト/秒) が、50% 超の時間にわたって、インスタンスと EBS ボリューム間の公開スループットの 95% を超えました。

[Recommended Action] (推奨されるアクション)

Amazon EBS ボリュームの最大スループット (「Amazon EBS ボリュームの種類」を参照) を、それらがアタッチされている Amazon EC2 インスタンスの最大スループットと比較します。「Instance Types That Support EBS Optimization」(EBS 最適化をサポートするインスタンスタイプ) を参照してください。

最適なパフォーマンスを実現するために、Amazon EBS に対してより高いスループットをサポートするインスタンスにボリュームをアタッチすることを検討してください。

その他のリソース

- Amazon EBS ボリュームの種類
- Amazon EBS 最適化インスタンス
- ボリュームのステータスのモニタリング
- 「インスタンスへの Amazon EBS ボリュームのアタッチ」を参照してください。
- インスタンスからの Amazon EBS ボリュームのデタッチ
- Amazon EBS ボリュームの削除

[Report columns] (レポート列)

- ステータス
- リージョン
- [インスタンス ID]
- インスタンスタイプ
- 最大に近い時間

EC2 仮想化タイプが準仮想化

説明

Amazon EC2 インスタンスの仮想化タイプが準仮想化かどうかをチェックします。

可能な場合は、準仮想インスタンスの代わりにハードウェア仮想マシン (HVM) インスタンスを使用するのがベストプラクティスです。これは、HVM 仮想化の機能強化や HVM AMI で PV ドライバが利用可能になったことにより、従来 PV と HVM のゲストの間に存在していたパフォーマンスのギャップが解消されたからです。現行世代のインスタンスタイプは PV AMI をサポートしない点に注意することが重要です。そのため、HVM インスタンスタイプを選択すると最高のパフォーマンスと最新のハードウェアとの互換性が得られます。

詳細については、「Linux AMI 仮想化タイプ」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c18d2gz148

ソース

AWS Config マネージドルール: ec2-paravirtual-instance-check

アラート条件

黄: Amazon EC2 インスタンスの仮想化タイプが準仮想化です。

[Recommended Action] (推奨されるアクション)

Amazon EC2 インスタンスに HVM 仮想化を使用し、互換性のあるインスタンスタイプを使用してください。

適切な仮想化タイプを選択する方法については、「インスタンスタイプ変更の互換性」を参照してください。

その他のリソース

インスタンスタイプ変更の互換性

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon ECS メモリのハード制限

説明

Amazon ECS のタスク定義に、そのコンテナの定義に対するメモリ制限が設定されているかどうかを確認します。タスク内のすべてのコンテナ用に予約されるメモリの合計量は、タスクのメモリー値より小さくする必要があります。

詳細については、「コンテナ定義」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c18d2gz176

ソース

AWS Config マネージドルール: ecs-task-definition-memory-hard-limit

アラート条件

黄: Amazon ECS メモリのハード制限が設定されていません。

[Recommended Action] (推奨されるアクション)

Amazon ECS タスクにメモリを割り当てて、メモリが不足しないようにしてください。コンテナが指定されたメモリを超えようとすると、コンテナは強制終了されます。

詳細については、「Amazon ECS のタスクにメモリを割り当てるにはどうすればよいですか?」を参照してください。

その他のリソース

クラスター予約

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EFS スループットモードの最適化

説明

お客様の Amazon EFS ファイルシステムが現在、バーストスループットモードを使用するように設定されているかどうかを確認します。

EFS のバーストスループットモード [1] のファイルシステムは、一貫したベースラインレベルのスループット (EFS スタンダードストレージのデータの GiB あたり 50 KiB/秒) を実現し、「バーストクレジット」が利用可能な場合は、クレジットモデルを使用してより高いレベルの「バーストスループット」パフォーマンスを実現します。バーストクレジットを使い果たすと、ファイルシステムのパフォーマンスがこの低いベースラインレベルに抑えられ、その結果、速度が低下したり、タイムアウトになったり、エンドユーザーやアプリケーションのパフォーマンスに影響を与えたりする可能性があります。

チェック ID

`c1dfprch02`

アラート条件

- 黄:ファイルシステムはバーストスループットモードを使用しています。

[Recommended Action] (推奨されるアクション)

ユーザーとアプリケーションが希望するスループットを達成できるように、ファイルシステム設定をエラスティックスループットモード [2] に更新することをお勧めします。エラスティックスループットモードでは、AWS リージョン [3] によって異なりますが、ファイルシステムで最大 10 GiB/秒の読み取りスループットまたは 3 GiB/秒の書き込みスループットを達成できます。お支払いいただくのは使用したスループットに対してのみです。ファイルシステムの設定を更新して、必要に応じてエラスティックスループットモードとバーストスループットモードを切り替え

ることができることと、エラスティックスループットモードのファイルシステムではデータ転送に追加料金が発生することに注意してください [4]。

その他のリソース

- [1] Amazon EFS パフォーマンススループットモード
- [2] Amazon EFS パフォーマンスエラスティックスループットモード
- [3] Amazon EFS のクォータと制限
- [4] Amazon EFS 料金表

[Report columns] (レポート列)

- ステータス
- リージョン
- EFS ファイルシステム ID
- スループットモード
- 最終更新日時

Amazon RDS 自動バキュームパラメータが無効になっています

説明

DB インスタンスの自動バキュームパラメータは無効になっています。自動バキュームを無効にすると、テーブルとインデックスが肥大化し、パフォーマンスに影響します。

DB パラメータグループの自動バキュームを有効にすることをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用でき

ません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt025`

アラート条件

黄色: DB パラメータグループの自動バキュームは無効になっています。

[Recommended Action] (推奨されるアクション)

DB パラメータグループの自動バキュームパラメータを有効にしてください。

その他のリソース

PostgreSQL データベースには、バキュームと呼ばれる定期的なメンテナンスが必要です。PostgreSQL の自動バキュームは、VACCUUM コマンドと ANALYZE コマンドの実行を自動化します。このプロセスはテーブル統計を収集し、デッド行を削除します。自動バキュームを無効にすると、テーブルの増加、インデックスの肥大化、古い統計がデータベースのパフォーマンスに影響します。

詳細については、「Understanding autovacuum in Amazon RDS for PostgreSQL environments」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS DB クラスターは最大 64 TiB のボリュームのみをサポートします

説明

DB クラスターは最大 64 TiB のボリュームをサポートします。最新のエンジンバージョンは、最大 128 TiB のボリュームをサポートします。DB クラスターのエンジンバージョンを最新バージョンにアップグレードして、最大 128 TiB のボリュームをサポートすることをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt017`

アラート条件

黄色: DB クラスターは最大 64 TiB のボリュームのみをサポートします。

[Recommended Action] (推奨されるアクション)

DB クラスターのエンジンバージョンをアップグレードして、最大 128 TiB のボリュームをサポートするようにします。

その他のリソース

単一の Amazon Aurora DB クラスターでアプリケーションをスケールアップする場合、ストレージ制限が 128 TiB の場合は制限に達しない可能性があります。ストレージ制限を増やすことで、データを削除したり、データベースを複数のインスタンスに分割したりするのを防ぐことができます。

詳細については、「Amazon Aurora size limits」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- 現行のエンジンバージョン
- 推奨値
- 最終更新日時

異なるインスタンスクラスを持つクラスター内の Amazon RDS DB インスタンス

説明

DB クラスター内のすべてのインスタンスに同じ DB インスタンスクラスとサイズを使用することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用でき

ません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt009`

アラート条件

赤: DB クラスターには、異なるインスタンスクラスの DB インスタンスがあります。

[Recommended Action] (推奨されるアクション)

DB クラスター内のすべての DB インスタンスに同じインスタンスクラスを使用します。

その他のリソース

DB クラスター内の DB インスタンスが異なる DB インスタンスクラスまたはサイズを使用している場合、DB インスタンスのワークロードに不均衡が生じる可能性があります。フェイルオーバー中、リーダー DB インスタンスのいずれかがライター DB インスタンスに変わります。DB インスタンスが同じ DB インスタンスクラスとサイズを使用する場合は、DB クラスターの DB インスタンスでワークロードを分散できます。

詳細については、「Aurora レプリカ」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

インスタンスサイズが異なるクラスター内の Amazon RDS DB インスタンス

説明

DB クラスター内のすべてのインスタンスに同じ DB インスタンスクラスとサイズを使用することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt008`

アラート条件

赤: DB クラスターには、さまざまなインスタンスサイズの DB インスタンスがあります。

[Recommended Action] (推奨されるアクション)

DB クラスター内のすべての DB インスタンスに同じインスタンスクラスを使用します。

その他のリソース

DB クラスター内の DB インスタンスが異なる DB インスタンスクラスまたはサイズを使用している場合、DB インスタンスのワークロードに不均衡が生じる可能性があります。フェイルオーバー中、リーダー DB インスタンスのいずれかがライター DB インスタンスに変わります。DB インスタンスが同じ DB インスタンスクラスとサイズを使用する場合は、DB クラスターの DB インスタンスでワークロードを分散できます。

詳細については、「Aurora レプリカ」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS DB のメモリパラメータがデフォルトと異なります

説明

DB インスタンスのメモリパラメータがデフォルト値と大きく異なります。これらの設定はパフォーマンスに影響が及び、エラーの原因となる可能性があります。

DB インスタンスのカスタムメモリパラメータを、DB パラメータグループのデフォルト値に再設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt020`

アラート条件

黄色: DB パラメータグループには、デフォルト値とはかなり異なるメモリパラメータがあります。

[Recommended Action] (推奨されるアクション)

メモリパラメータをデフォルト値にリセットします。

その他のリソース

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS enable_index_OnlyScan パラメータは無効になっています。

説明

クエリプランナーまたはオプティマイザーは、インデックスのみのスキャン計画タイプが無効になっている場合は使用できません。

enable_indexonlyscan パラメータの値を 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt028`

アラート条件

黄色: DB パラメータグループの enable_indexonlyscan パラメータは無効になっています。

[Recommended Action] (推奨されるアクション)

enable_indexonlyscan パラメーターを 1 に設定します。

その他のリソース

enable_indexonlyscan パラメーターを無効にすると、クエリプランナーは最適な実行プランを選択できなくなります。クエリプランナーは、インデックススキャンなどの別のプランタイプを使用するため、クエリのコストと実行時間が長くなる可能性があります。インデックスのみのスキャンプランタイプでは、テーブルデータにアクセスせずにデータを取得します。

詳細については、PostgreSQL ドキュメント Web サイトの「enable_indexonlyscan (boolean)」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS enable_indexscan パラメータは無効になっています

説明

クエリプランナーまたはオプティマイザーは、インデックスのみのスキャン計画タイプが無効になっている場合は使用できません。

enable_indexscan パラメータの値を 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt029`

アラート条件

黄色: DB パラメータグループの enable_indexscan パラメータは無効になっています。

[Recommended Action] (推奨されるアクション)

パラメータ enable_indexscan を 1 に設定します。

その他のリソース

enable_indexscan パラメーターを無効にすると、クエリプランナーは最適な実行プランを選択できなくなります。クエリプランナーは、インデックススキャンなどの別のプランタイプを使用するため、クエリのコストと実行時間が長くなる可能性があります。

詳細については、PostgreSQL ドキュメント Web サイトの「enable_indexonlyscan (boolean)」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS general_logging パラメータが有効になっています

説明

DB インスタンスの一般ログ記録が有効になっています。この設定は、データベースの問題のトラブルシューティングに役立ちます。しかし、一般ログ記録を有効にすると、入出力操作の量と割り当てられるストレージ容量が増え、競合やパフォーマンスの低下につながる可能性があります。

一般ログ記録の使用状況の要件を確認してください。general_logging パラメーターの値を 0 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt037`

アラート条件

黄色: DB パラメータグループでは general_logging が有効になっています。

[Recommended Action] (推奨されるアクション)

一般ログ記録の使用状況の要件を確認してください。必須ではない場合は、general_logging パラメーターの値を 0 に設定することをお勧めします。

その他のリソース

general_logging パラメーター値が 1 の場合、一般クエリーログが有効になります。一般クエリログには、データベースサーバー操作の記録が含まれます。サーバーは、クライアントが接続または切断したときにこのログに情報を書き込み、ログにはクライアントから受け取った各 SQL 文が含まれます。一般クエリログは、クライアントでエラーが発生した疑いがあり、クライアントがデータベースサーバーに送信した情報を検索したい場合に役立ちます。

詳細については、「RDS for MySQL データベースログの概要」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS InnoDB_Change_Buffering パラメータは最適値よりも小さい値を使用しています

説明

変更バッファリングでは、MySQL DB インスタンスは、セカンダリインデックスを維持するために必要ないくつかの書き込みを延期することができます。この機能は、低速ディスクを使用する環境で有効でした。バッファリング設定を変更することで DB のパフォーマンスはわずかに向上しましたが、クラッシュリカバリの遅延やアップグレード中のシャットダウン時間の増加の原因となりました。

innodb_change_buffering パラメーターの値を NONE に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt021`

アラート条件

黄色: DB パラメータグループの innodb_change_buffering パラメータは最適値が低く設定されています。

[Recommended Action] (推奨されるアクション)

DB パラメータグループの innodb_change_buffering パラメータ値を NONE に設定します。

その他のリソース

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance」を参照してください。

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS innodb_open_files パラメータが低いです

説明

innodb_open_files パラメータは、InnoDB が一度に開くことができるファイル数を制御します。InnoDB は、mysqld の実行時にすべてのログファイルとシステムテーブルスペースファイルを開きます。

お使いの DB インスタンスは、InnoDB が一度に開くことができる最大ファイル数の値が低くなっています。innodb_open_files パラメータ値を少なくとも 65 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

c1qf5bt033

アラート条件

黄色: DB パラメータグループの InnoDB オープンファイル設定に誤りがあります。

[Recommended Action] (推奨されるアクション)

innodb_open_files パラメータ値を少なくとも 65 に設定します。

その他のリソース

innodb_open_files パラメータは、InnoDB が一度に開くことができるファイル数を制御します。InnoDB は、mysqld の実行中、すべてのログファイルとシステムテーブルスペースファイルを開いたままにします。ファイル単位のストレージモデルを使用する場合、InnoDB はいくつかの.ibd ファイルを開く必要もあります。innodb_open_files の設定が低いと、データベースのパフォーマンスに影響し、サーバーが起動しなくなる可能性があります。

詳細については、MySql ドキュメント Web サイトの「InnoDB Startup Options and System Variables - innodb_open_files」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS innodb_stats_persistent パラメータは無効になっています

説明

DB インスタンスは、InnoDB 統計をディスクに保持するように設定されていません。統計が保存されていない場合は、インスタンスが再起動してテーブルにアクセスするたびに再計算されます。これにより、クエリ実行プランにばらつきが生じます。このグローバルパラメータの値はテーブルレベルで変更できます。

innodb_stats_persistent パラメーター値を ON 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt032`

アラート条件

黄色: DB パラメータグループには、ディスクに保持されないオプティマイザ統計があります。

[Recommended Action] (推奨されるアクション)

innodb_stats_persistent パラメータ値を ON に設定します。

その他のリソース

innodb_stats_persistent パラメーターが ON に設定されている場合、オプティマイザ統計はインスタンスの再起動時に保持されます。これにより、実行プランの安定性と一貫したクエリパフォーマンスが向上します。テーブルを作成または変更するときに STATS_PERSISTENT 句を使用することにより、グローバル統計の永続性をテーブルレベルで変更できます。

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

システム容量のプロビジョニングが不十分な Amazon RDS インスタンス

説明

Amazon RDS インスタンスまたは Amazon Aurora DB インスタンスに、動作に必要なシステム容量があるかどうかを確認します。

チェック ID

`c1qf5bt039`

アラート条件

黄色:

メモリ不足による強制終了: OS レベルでのメモリ不足により、データベースホスト上のプロセスが停止すると、メモリ不足 (OOM) キラーのカウンターが動作します。

過剰な数のスワップ: os.memory.swap.in および os.memory.swap.out のメトリクス値が高い場合。

[Recommended Action] (推奨されるアクション)

メモリの使用量を減らすか、メモリの割り当て量の多い DB インスタンスタイプを使用するようにクエリを調整することをお勧めします。インスタンスのメモリが不足すると、データベースのパフォーマンスに影響を及ぼします。

その他のリソース

メモリ不足による強制終了が検出された: Linux カーネルは、ホスト上で実行されているプロセスがオペレーティングシステムから物理的に利用可能なメモリを超えるメモリを必要とする場合に、メモリ不足 (OOM) キラーを呼び出します。この場合、メモリ不足 (OOM) キラーはシステムメモリを解放してシステムの稼働を継続するため、実行中のプロセスをすべて確認し、1 つ以上のプロセスを停止します。

スワップが検出されている: データベースホストのメモリが不足している場合、オペレーティングシステムはスワップスペース内のディスクに最も使用されていないページをいくつか送信します。このオフロードプロセスは、データベースのパフォーマンスに影響を及ぼします。

詳細については、「Amazon RDS インスタンスタイプ」および「Scaling yourAmazon RDS instance」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- メモリ不足による強制終了 (カウント)
- 過剰なスワップ (カウント)
- 最終検出期間
- 最終更新日時

Amazon RDS のマグネティックボリュームが使用中です。

説明

DB インスタンスはマグネティックストレージを使用しています。ほとんどの DB インスタンスには、マグネティックストレージは推奨されません。別のストレージタイプとして、汎用 (SSD) またはプロビジョンド IOPS を選択してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用でき

ません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt000`

アラート条件

黄色: Amazon RDS リソースではマグネティックストレージを使用しています。

[Recommended Action] (推奨されるアクション)

別のストレージタイプとして、汎用 (SSD) またはプロビジョンド IOPS を選択してください。

その他のリソース

マグネティックストレージは旧世代のストレージタイプです。新しいストレージ要件には、汎用 (SSD) またはプロビジョンド IOPS が推奨されます。これらのストレージタイプは、より高い一貫したパフォーマンスを実現し、ストレージサイズの選択肢も広がります。

詳細については、「旧世代ボリューム」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS パラメータグループでは Huge pages は使用されません

説明

Large pages はデータベースのスケーラビリティを高めることができますが、DB インスタンスは Large pages を使用していません。DB インスタンスの DB パラメータグループで、use_large_pages パラメータを ONLY に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt024`

アラート条件

黄色: DB パラメータグループでは Large pages は使用されません。

[Recommended Action] (推奨されるアクション)

DB パラメータグループ内で use_large_pages パラメータ値を ONLY に設定します。

その他のリソース

詳細については、「サポートされている RDS for Oracle インスタンスで HugePages をオンにする」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS クエリキャッシュパラメータは有効になっています

説明

変更によってクエリキャッシュの削除が必要になった場合、DB インスタンスは停止しているように見えます。通常ワークロードでは、クエリキャッシュのメリットは得られません。クエリキャッシュは、MySQL バージョン 8.0 から削除されました。query_cache_type パラメータを 0 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。

DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt022`

アラート条件

黄色: DB パラメータグループではクエリキャッシュが有効になっています。

[Recommended Action] (推奨されるアクション)

DB パラメータグループの query_cache_type パラメータ値を 0 に設定します。

その他のリソース

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS リソース、インスタンスクラスの更新が必須です。

説明

データベースは、旧世代の DB インスタンスクラスを実行しています。旧世代の DB インスタンスクラスは、コスト、パフォーマンス、またはその両方が向上した DB インスタンスクラスに置き換えられました。DB インスタンスには、新しい世代の DB インスタンスクラスを使用して実行することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt015`

アラート条件

赤: DB インスタンスはサポート終了の DB インスタンスクラスを使用しています。

[Recommended Action] (推奨されるアクション)

最大インスタンスクラスにアップグレードします。

その他のリソース

詳細については、「DB インスタンスクラスでサポートされている DB エンジン」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン

- リソース
- DB インスタンスクラス
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS リソースのメジャーバージョンの更新が必須です。

説明

DB エンジンの、現行メジャーバージョンのデータベースはサポートされません。新しい機能や拡張機能を含む最新のメジャーバージョンにアップグレードすることをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

```
c1qf5bt014
```

アラート条件

赤: RDS リソースはサポート終了のメジャーバージョンを使用しています。

[Recommended Action] (推奨されるアクション)

DB エンジンを最新のメジャーバージョンにアップグレードします。

その他のリソース

Amazon RDS は、データベースを最新バージョンに保つため、サポートされているデータベースエンジンの新しいバージョンをリリースしています。新しいバージョンには、データベースエンジンのバグ修正、セキュリティの強化、およびその他の改善が含まれる場合があります。ブルー/グリーンデプロイを使用することで、DB インスタンスのアップグレードに必要なダウンタイムを最小限に抑えることができます。

詳細については、以下のリソースを参照してください。

- DB インスタンス エンジンバージョンのアップグレード
- Amazon Aurora の更新
- データベース更新のために Amazon RDS ブルー/グリーンデプロイを使用する

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- エンジンバージョンの現行バージョン
- 推奨値
- 最終更新日時

ライセンス付きのサポート終了エンジンエディションを使用する Amazon RDS リソース

説明

現在のライセンスサポートを継続するには、メジャーバージョンを Amazon RDS がサポートする最新のエンジンバージョンにアップグレードすることをお勧めします。データベースのエンジンバージョンは、現在のライセンスではサポートされません。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt016`

アラート条件

赤: Amazon RDS リソースは、ライセンス込みモデルのサポート終了エンジンエディションを使用しています。

[Recommended Action] (推奨されるアクション)

ライセンスモデルを引き続き使用するには、データベースを Amazon RDS でサポートされている最新バージョンにアップグレードすることをお勧めします。

その他のリソース

詳細については、[Oracle のメジャーバージョンのアップグレード]を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン

- リソース
- エンジン名
- 現行のエンジンバージョン
- 推奨値
- エンジン名
- 最終更新日時

Amazon Route 53 エイリアスリソースレコードセット

説明

パフォーマンスを向上させ、コストを節約するために、エイリアスリソースレコードセットに変更できるリソースレコードセットをチェックします。

エイリアスリソースレコードセットは、DNS クエリを AWS リソース (Elastic Load Balancing ロードバランサーや Amazon S3 バケットなど) または別の Route 53 リソースレコードセットにルーティングします。エイリアスリソースレコードセットを使用すると、Route 53 は DNS クエリをリソースに AWS 無料でルーティングします。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`B913Ef6fb4`

アラート条件

- 黄: リソースレコードセットは Amazon S3 ウェブサイトの CNAME です。
- 黄: リソースレコードセットは Amazon CloudFront ディストリビューションの CNAME です。
- 黄: リソースレコードセットは Elastic Load Balancing ロードバランサーの CNAME です。

[Recommended Action] (推奨されるアクション)

リストされた CNAME リソースレコードセットをエイリアスリソースレコードセットに置き換えます。「Choosing Between Alias and Non-Alias Resource Record Sets」(エイリアスのリソースレコードセットと非エイリアスのリソースレコードセットの選択) を参照してください。

また、 AWS リソースに応じて、レコードタイプを CNAME から A または AAAA に変更する必要があります。「Values that You Specify When You Create or Edit Amazon Route 53 Resource

Record Sets」(Amazon Route 53 リソースレコードセットの作成または編集時に指定する値) を参照してください。

その他のリソース

AWS リソースへのクエリのルーティング

[Report columns] (レポート列)

- ステータス
- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名
- リソースレコードセットのタイプ
- リソースレコードセットの識別子
- エイリアス先

AWS Lambda メモリサイズのプロビジョニング不足関数

説明

ルックバック期間中に少なくとも 1 回呼び出された AWS Lambda 関数を確認します。このチェックは、Lambda 関数がメモリサイズに関してプロビジョニング不足である場合に警告します。メモリサイズについてプロビジョニング不足である Lambda 関数がある場合、これらの関数の完了に時間がかかります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`C0r6dfpM06`

アラート条件

黄: ルックバック期間中にメモリサイズのプロビジョニングが不足していた Lambda 関数。Lambda 関数のプロビジョニングが不足していないかどうかを判断するために、その関数のすべてのデフォルト CloudWatch メトリクスを考慮します。メモリサイズのプロビジョニング不足の Lambda 関数を識別するために使用されるアルゴリズムは、 AWS のベストプラクティスに従います。新しいパターンが特定されると、アルゴリズムが更新されます。

[Recommended Action] (推奨されるアクション)

Lambda 関数のメモリサイズを大きくすることを検討してください。

詳細については、「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- 関数名
- 関数バージョン
- メモリサイズ (MB)
- 推奨メモリサイズ (MB)
- ルックバック期間 (日)
- パフォーマンスリスク
- 最終更新日時

AWS Lambda 同時実行制限が設定されていない関数

説明

AWS Lambda 関数が関数レベルの同時実行制限で設定されているかどうかを確認します。

同時実行は、AWS Lambda 関数が同時に処理している未完了のリクエスト数です。Lambda は、同時実行リクエストごとに、実行環境の個別のインスタンスをプロビジョニングします。

ルールの concurrencyLimitLow パラメータと ConcurrencyLimitHigh パラメータ AWS Config を使用して、予約済み同時実行数の最小制限と最大制限を指定できます。

詳細については、「Lambda 関数のスケーリング」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz181`

ソース

AWS Config マネージドルール: lambda-concurrency-check

アラート条件

黄: Lambda 関数に同時実行数の制限が設定されていません。

[Recommended Action] (推奨されるアクション)

Lambda 関数に同時実行が設定されていることを確認します。Lambda 関数に同時実行数の制限を設けると、関数がリクエストを確実かつ予測どおりに処理できるようになります。同時実行数の制限を設けると、トラフィックの急増によって関数が処理しきれなくなるリスクを軽減できます。

詳細については、「予約済同時実行数の設定」を参照してください。

その他のリソース

- Lambda 関数のスケーリング
- 予約済同時実行数の設定

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ

- 最終更新日時

パフォーマンスに関する AWS Well-Architected のリスクの高い問題

説明

パフォーマンスの柱で、ワークロードに関するリスクの高い問題 (HRI) をチェックします。このチェックは、お客様の AWS-Well Architected レビューに基づきます。チェック結果は、AWS Well-Architected でワークロード評価を完了したかどうかによって異なります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`Wxdfp4B1L2`

アラート条件

- 赤: AWS Well-Architected のパフォーマンスの柱で、少なくとも 1 つのアクティブな高リスクの問題が特定されました。
- 緑: AWS Well-Architected のパフォーマンスの柱でアクティブな高リスクの問題は検出されませんでした。

[Recommended Action] (推奨されるアクション)

AWS Well-Architected は、ワークロード評価中に高リスクの問題を検出しました。これらの問題は、リスクを軽減し、費用を節約する機会を提示します。AWS Well-Architected ツールにサインインして、回答を確認し、アクティブな問題を解決するためのアクションを実行します。

[Report columns] (レポート列)

- ステータス
- リージョン
- ワークロードの ARN

- ワークロード名
- レビュー担当者名
- ワークロードタイプ
- ワークロードの開始日
- ワークロードの最終変更日
- パフォーマンスについて特定された HRI の数
- パフォーマンスについて解決された HRI の数
- パフォーマンスについて回答された質問の数
- パフォーマンスの柱の質問の総数
- 最終更新日時

CloudFront 代替ドメイン名

説明

DNS 設定が正しく設定されていない代替ドメイン名 (CNAMES) がないか、Amazon CloudFront ディストリビューションをチェックします。

CloudFront ディストリビューションに代替ドメイン名が含まれる場合、ドメインの DNS 設定は、そのディストリビューションに DNS クエリをルーティングする必要があります。

> **Note**
>
> このチェックでは、Amazon Route 53 DNS と Amazon CloudFront ディストリビューションが同じ AWS アカウントで設定されていることが前提になります。そのため、アラートリストには、それ以外の場合にこの AWS アカウントの外部の DNS 設定で機能すると予期されているリソースが含まれる場合があります。

チェック ID

`N420c450f2`

アラート条件

- 黄: CloudFront ディストリビューションには代替ドメイン名が含まれていますが、DNS 設定が CNAME レコードまたは Amazon Route 53 エイリアスリソースレコードで正しくセットアップされていません。

- 黄: CloudFront ディストリビューションには代替ドメイン名が含まれていますが、リダイレクトが多すぎるため、 Trusted Advisor は DNS 設定を評価できませんでした。
- 黄: CloudFront ディストリビューションには代替ドメイン名が含まれていますが、他の理由で Trusted Advisor は DNS 設定を評価できませんでした。おそらく、タイムアウトが原因です。

[Recommended Action] (推奨されるアクション)

DNS 設定を更新して、DNS クエリを CloudFront ディストリビューションにルーティングします。「Using Alternate Domain Names (CNAMEs)」(代替ドメイン名 (CNAME) の使用) を参照してください。

DNS サービスとして Amazon Route 53 を使用している場合は、「ドメイン名を使用したトラフィックの Amazon CloudFront ディストリビューションへのルーティング」を参照してください。チェックがタイムアウトした場合は、チェックを更新してみてください。

その他のリソース

Amazon CloudFront 開発者ガイド

[Report columns] (レポート列)

- ステータス
- ディストリビューション ID
- ディストリビューションドメイン名
- 代替ドメイン名
- 理由

コンテンツ配信の最適化 (CloudFront)

説明

Amazon Simple Storage Service (Amazon S3) バケットからのデータ転送が、 AWS グローバルコンテンツ配信サービスである Amazon CloudFront を使用して高速化される可能性があるケースをチェックします。

コンテンツを配信するために CloudFront を設定すると、コンテンツに対するリクエストは、コンテンツがキャッシュされている最も近いエッジロケーションに自動的にルーティングされます。このルーティングでは、可能な限り最高のパフォーマンスでコンテンツをユーザーに配信できます。バケットに格納されているデータと比較して、転送されるデータの比率が高いと場合、Amazon CloudFront を使用してデータを配信することによってメリットが生まれる可能性があることを示しています。

チェック ID

796d6f3D83

アラート条件

- 黄: チェックの前 30 日間に GET リクエストによってバケットからユーザーに転送 (OUT) されたデータ量は、バケットに保存されている平均データ量の少なくとも 25 倍です。
- 赤: チェックの前 30 日間に GET リクエストによってバケットからユーザーに転送 (OUT) されたデータ量は、少なくとも 10 TB、かつ、バケットに保存されている平均データ量の少なくとも 25 倍です。

[Recommended Action] (推奨されるアクション)

より良いパフォーマンスのために CloudFront の使用を検討してください。「Amazon CloudFront Product Details」(Amazon CloudFront 製品の詳細) を参照してください。

転送されるデータが 1 か月あたり 10 TB 以上の場合は、「Amazon CloudFront の料金」を参照して、可能なコスト削減を検討してください。

その他のリソース

- Amazon CloudFront デベロッパーガイド
- AWS 導入事例: PBS

[Report columns] (レポート列)

- ステータス
- リージョン
- バケット名
- S3 ストレージ (GB)
- データ転送 (OUT) (GB)
- ストレージへの転送の比率

CloudFront ヘッダー転送とキャッシュヒット率

説明

CloudFront が現在クライアントから受け取り、オリジンサーバーに転送する HTTP リクエストヘッダーをチェックします。

日付やユーザーエージェントなどの一部のヘッダーは、キャッシュヒット率 (CloudFront エッジキャッシュから提供されるリクエストの割合) を大幅に低下させます。これにより、CloudFront

はより多くのリクエストをオリジンに転送する必要があるため、オリジンへの負荷が高くなり、パフォーマンスが低下します。

チェック ID

N415c450f2

アラート条件

黄: CloudFront がオリジンに転送する 1 つ以上のリクエストヘッダーにより、キャッシュヒット率が大幅に低下する可能性があります。

[Recommended Action] (推奨されるアクション)

リクエストヘッダーが、キャッシュヒット率への悪影響を正当化するのに十分なメリットを提供するかどうかを検討します。特定のヘッダーの値にかかわらず、オリジンが同じオブジェクトを返す場合は、そのヘッダーをオリジンに転送するように CloudFront を設定しないことをお勧めします。詳細については、「Configuring CloudFront to Cache Objects Based on Request Headers」(リクエストヘッダーに基づいてオブジェクトをキャッシュするように CloudFront を設定する) を参照してください。

その他のリソース

- CloudFront エッジキャッシュから提供されるリクエストの比率の向上
- CloudFront キャッシュ統計レポート
- HTTP リクエストヘッダーと CloudFront の動作

[Report columns] (レポート列)

- ディストリビューション ID
- ディストリビューションドメイン名
- キャッシュ動作のパスパターン
- ヘッダー

高 CPU 使用率の Amazon EC2 インスタンス

説明

過去 14 日間の任意の時点で実行していた Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをチェックします。4 日以上で 1 日あたりの CPU 使用率が 90% 以上の場合、アラートが送信されます。

使用率が一貫して高い場合は、パフォーマンスが最適化され、安定している場合があります。ただし、アプリケーションに十分なリソースがない可能性もあります。毎日の CPU 使用量データを取得するには、このチェックのレポートをダウンロードします。

チェック ID

ZRxQlPsb6c

アラート条件

黄: インスタンスは、過去 14 日間のうち少なくとも 4 日間で、1 日の平均 CPU 使用率が 90% を超えていました。

[Recommended Action] (推奨されるアクション)

インスタンスをさらに追加することを検討してください。需要に基づいてインスタンス数をスケーリングする方法については、「What is Auto Scaling?」(Auto Scaling とは) を参照してください。

その他のリソース

- Amazon EC2 のモニタリング
- インスタンスメタデータとユーザーデータ
- Amazon CloudWatch ユーザーガイド
- Amazon EC2 Auto Scaling ユーザーガイド

[Report columns] (レポート列)

- リージョン/AZ
- [インスタンス ID]
- インスタンスタイプ
- インスタンス名
- 14 日間の平均 CPU 使用率
- CPU 使用率が 90% を超えた日数

セキュリティ

セキュリティカテゴリの次のチェックを使用できます。

> **Note**
>
> で Security Hub を有効にした場合は AWS アカウント、 Trusted Advisor コンソールで検出結果を表示できます。詳細については、での AWS Security Hub コントロールの表示 AWS Trusted Advisor を参照してください。
> カテゴリ: 復旧 > 回復力を持つコントロールを除き、 AWS Foundational Security Best Practices セキュリティ標準ですべてのコントロールを表示できます。サポートされるコントロールのリストについては、AWS Security Hub ユーザーガイドの「AWS Foundational Security Best Practices controls」を参照してください。

チェック名

- Application Load Balancer のセキュリティグループ
- Amazon CloudWatch ロググループの保持期間
- Microsoft SQL Server を使用した Amazon EC2 インスタンスのサポートの終了
- Microsoft Windows Server を使用した Amazon EC2 インスタンスのサポートの終了
- Ubuntu LTS を使用した Amazon EC2 インスタンスの標準サポートの終了
- 転送中のデータの暗号化を使用しない Amazon EFS クライアント
- Amazon EBS パブリックスナップショット
- Amazon RDS Aurora ストレージの暗号化は無効になっています
- Amazon RDS エンジンのマイナーバージョンアップグレードが必須です。
- Amazon RDS パブリックスナップショット
- Amazon RDS セキュリティグループのアクセスリスク
- Amazon RDS ストレージの暗号化は無効になっています。
- S3 バケットを直接指定する Amazon Route 53 の CNAME レコードの不一致
- Amazon Route 53 MX リソースレコードセットと Sender Policy Framework
- Amazon S3 バケット許可
- DNS 解決が無効になっている Amazon VPC ピアリング接続
- Application Load Balancer ターゲットグループの暗号化プロトコル
- AWS Backup リカバリポイントの削除を防ぐためのリソースベースのポリシーがないボールト
- AWS CloudTrail ログ記録
- AWS CloudTrail 管理イベントのログ記録

- AWS Lambda 非推奨ランタイムを使用する関数
- セキュリティに関する AWS Well-Architected のリスクの高い問題
- IAM 証明書ストアの CloudFront 独自 SSL 証明書
- オリジンサーバーの CloudFront 独自 SSL 証明書
- ELB リスナーのセキュリティ
- Classic Load Balancer セキュリティグループ
- 露出したアクセスキー
- IAM アクセスキーローテーション
- IAM Access Analyzer の外部アクセス
- IAM パスワードポリシー
- IAM SAML 2.0 ID プロバイダー
- ルートアカウントの MFA
- ルートユーザーアクセスキー
- セキュリティグループ — 開かれたポート
- セキュリティグループ — 無制限アクセス

Application Load Balancer のセキュリティグループ

説明

Application Load Balancer とその Amazon EC2 ターゲットにアタッチされているセキュリティグループを確認します。Application Load Balancer セキュリティグループは、リスナーで設定されたインバウンドポートのみを許可する必要があります。ターゲットのセキュリティグループは、ターゲットがロードバランサーからトラフィックを受信するのと同じポートで、インターネットからの直接接続を受け入れないでください。

セキュリティグループがロードバランサー用に設定されていないポートへのアクセスを許可したり、ターゲットへの直接アクセスを許可したりすると、データ損失や悪意のある攻撃のリスクが高まります。

このチェックでは、次のグループが除外されます。

- IP アドレスまたは EC2 インスタンスに関連付けられていないターゲットグループ。
- IPv6 トラフィックのセキュリティグループルール。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

8604e947f2

アラート条件

- 赤: ターゲットにはパブリック IP とセキュリティグループがあり、トラフィックポート上のインバウンド接続をどこからでも許可します (0.0.0.0/0)。
- 赤: Application Load Balancer では認証が有効になっており、ターゲットはトラフィックポート上のインバウンド接続をどこからでも許可します (0.0.0.0/0)。
- 黄: ターゲットのセキュリティグループは、トラフィックポート上のインバウンド接続をどこからでも許可します (0.0.0.0/0)。
- 黄: Application Load Balancer セキュリティグループは、対応するリスナーを持たないポートでのインバウンド接続を許可します。
- 緑: Application Load Balancer セキュリティグループは、リスナーと一致するポートでのみインバウンド接続を許可します。

[Recommended Action] (推奨されるアクション)

セキュリティを向上させるには、セキュリティグループが必要なトラフィックフローのみを許可していることを確認してください。

- Application Load Balancer のセキュリティグループは、リスナーで設定された同じポートに対してのみインバウンド接続を許可する必要があります。
- ロードバランサーとターゲットに排他的なセキュリティグループを使用します。
- ターゲットセキュリティグループは、関連付けられているロードバランサー (複数可) からのトラフィックポートへの接続のみを許可する必要があります。

その他のリソース

- セキュリティグループを使用して AWS リソースへのトラフィックを制御する

- Application Load Balancer のセキュリティグループ

[Report columns] (レポート列)

- ステータス
- リージョン
- 対象グループ
- ALB 名
- ALB SG ID
- ターゲット SG ID
- 認証が有効
- 最終更新日時

Amazon CloudWatch ロググループの保持期間

説明

Amazon CloudWatch ロググループの保持期間が 365 日または特定の日数に設定されているかどうかを確認します。

デフォルトでは、ログは無制限に保持され、失効しません。ただし、業界の規制や特定の期間の法的要件に準拠するように、ロググループごとに保持ポリシーを調整することができます。

AWS Config ルールの LogGroupNames と MinRetentionTime パラメータを使用して、最小保持期間とロググループ名を指定できます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz186`

ソース

AWS Config Managed Rule: cw-loggroup-retention-period-check

アラート条件

黄: Amazon CloudWatch ロググループの保持期間が希望する最小日数を下回っています。

[Recommended Action] (推奨されるアクション)

Amazon CloudWatch Logs に保存されているログデータには、コンプライアンス要件を満たすために 365 日を超える保存期間を設定します。

詳細については、「CloudWatch Logs でのログデータ保管期間の変更」を参照してください。

その他のリソース

CloudWatch のログ保持期間の変更

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Microsoft SQL Server を使用した Amazon EC2 インスタンスのサポートの終了

説明

直近 24 時間以内に実行されている Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの SQL Server バージョンをチェックします。このチェックでは、ご利用のバージョンのサポートが終了に近づいているか、または終了している場合に警告を受け取ります。SQL Server の各バージョンでは、5 年間のメインストリームサポートと 5 年間の延長サポートを含む 10 年間のサポートが提供されます。サポートの終了後には、SQL Server バージョンは定期的なセキュリティ更新を受け取らなくなります。サポートされていないバージョンの SQL Server でアプリケーションを実行すると、セキュリティまたはコンプライアンスのリスクが生じる可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`Qsdfp3A4L3`

アラート条件

- 赤: EC2 インスタンスには、サポートが終了した SQL Server バージョンがあります。
- 黄: EC2 インスタンスには、12 か月以内にサポートが終了する SQL Server バージョンがあります。

[Recommended Action] (推奨されるアクション)

SQL Server のワークロードをモダナイズするには、Amazon Aurora などの AWS クラウド ネイティブデータベースへのリファクタリングを検討してください。詳細については、「 を使用した Windows ワークロードのモダナイズ AWS」を参照してください。

フルマネージドデータベースに移行するには、Amazon Relational Database Service (Amazon RDS) への再プラットフォーム化を検討します。詳細については、「Amazon RDS for SQL Server」を参照してください。

Amazon EC2 で SQL Server をアップグレードするには、オートメーションランブックを使用してアップグレードを簡素化することを検討してください。詳細については、AWS Systems Manager のドキュメントを参照してください。

Amazon EC2 で SQL Server をアップグレードできない場合は、Windows Server 向けサポート終了移行プログラム (EMP) を検討してください。詳細については、EMP のウェブサイトを参照してください。

その他のリソース

- で SQL Server のサポート終了に備える AWS
- AWSでの Microsoft SQL Server

[Report columns] (レポート列)

- ステータス
- リージョン
- [インスタンス ID]
- SQL Server バージョン
- サポートサイクル
- サポートの終了
- 最終更新日時

Microsoft Windows Server を使用した Amazon EC2 インスタンスのサポートの終了

説明

このチェックでは、ご利用のバージョンのサポートが終了に近づいているか、または終了している場合に警告を受け取ります。Windows Server の各バージョンは、10 年間のサポートを提供しています。これには、5 年間のメインストリームサポートと 5 年間の延長サポートが含まれます。サポートの終了後には、Windows Server バージョンは定期的なセキュリティ更新を受け取らなくなります。Windows Server の未サポートのバージョンでアプリケーションを実行すると、アプリケーションのセキュリティやコンプライアンスにリスクが生じます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`Qsdfp3A4L4`

アラート条件

- 赤: EC2 インスタンスには、サポートが終了している Windows Server バージョン (Windows Server 2003、2003 R2、2008、2008 R2) があります。

- 黄: EC2 インスタンスには、18 か月以内にサポートが終了する Windows Server バージョン (Windows Server 2012、2012 R2) があります。

[Recommended Action] (推奨されるアクション)

Windows Server ワークロードをモダナイズするには、Windows ワークロードのモダナイズで使用できるさまざまなオプションを検討してください AWS。

Windows Server ワークロードをアップグレードしてより新しいバージョンの Windows Server で実行するときは、自動化ランブックを使用できます。詳細については、AWS Systems Manager のドキュメントを参照してください。

以下の一連の手順に従ってください。

- Windows Server のバージョンのアップグレード
- アップグレードの際のハードの停止と起動
- EC2Config を使用している場合は、EC2Launch に移行してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- [インスタンス ID]
- Windows Server バージョン
- サポートサイクル
- サポートの終了
- 最終更新日時

Ubuntu LTS を使用した Amazon EC2 インスタンスの標準サポートの終了

説明

このチェックでは、ご利用のバージョンのサポートが終了に近づいているか、終了している場合に警告します。次の LTS に移行するか Ubuntu Pro にアップグレードすることで、対策を講じることが重要です。サポート終了後、18.04 LTS のマシンはセキュリティ更新を受信できなくなります。Ubuntu Pro サブスクリプションを利用すると、Ubuntu 18.04 LTS デプロイは 2028 年まで Expanded Security Maintenance (ESM) を受け取ることができます。パッチが適用されていないセキュリティの脆弱性により、システムがハッカーにさらされ、重大な侵害が発生する可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dfprch15`

アラート条件

赤: Amazon EC2 インスタンスに、標準サポートが終了した Ubuntu バージョン (Ubuntu 18.04 LTS、18.04.1 LTS、18.04.2 LTS、18.04.3 LTS、18.04.4 LTS、18.04.5 LTS、18.04.6 LTS)

黄色: Amazon EC2 インスタンスに、6 か月以内に標準サポートが終了する Ubuntu バージョン (Ubuntu 20.04 LTS、20.04.1 LTS、20.04.2 LTS、20.04.3 LTS、20.04.4 LTS、20.04.5 LTS、20.04.6 LTS) が含まれています。

緑: すべての Amazon EC2 インスタンスが準拠しています。

[Recommended Action] (推奨されるアクション)

Ubuntu 18.04 LTS インスタンスをサポートされている LTS バージョンにアップグレードするには、こちらの記事に記載されている手順に従ってください。Ubuntu 18.04 LTS インスタンスを Ubuntu Pro にアップグレードするには、 AWS License Manager コンソールにアクセスし、「AWS License Manager ユーザーガイド」に記載された手順に従ってください。Ubuntu インスタンスを Ubuntu Pro にアップグレードする手順を説明したデモをご覧いただける Ubuntu ブログも参照してください。

その他のリソース

料金については、サポート にお問い合わせください。

[Report columns] (レポート列)

- ステータス
- リージョン
- Ubuntu LTS バージョン

- サポートの終了予定日
- [インスタンス ID]
- サポートサイクル
- 最終更新日時

転送中のデータの暗号化を使用しない Amazon EFS クライアント

説明

Amazon EFS ファイルシステムが転送中データの暗号化を使用してマウントされているかどうかを確認します。 AWS では、データを偶発的な公開や不正アクセスから保護するため、すべてのデータフローで転送中データの暗号化を使用することを推奨しています。Amazon EFS では、Amazon EFS マウントヘルパーを使用して「-o tls」によるマウント設定を使用し、TLS v1.2 を使用して転送中のデータを暗号化することを推奨しています。

チェック ID

`c1dfpnchv1`

アラート条件

黄色: Amazon EFS ファイルシステムの 1 つ以上の NFS クライアントが、転送中のデータを暗号化するために必要な推奨されるマウント設定を使用していません。

緑: Amazon EFS ファイルシステムのすべての NFS クライアントが、転送中のデータを暗号化するために必要な推奨されるマウント設定を使用しています。

[Recommended Action] (推奨されるアクション)

Amazon EFS で転送中のデータの暗号化機能を利用するには、Amazon EFS マウントヘルパーおよび推奨されるマウント設定を使用して、ファイルシステムを再マウントすることをお勧めします。

> **Note**
>
> 一部の Linux ディストリビューションには、デフォルトで TLS 機能をサポートする stunnel のバージョンは含まれていません。サポートされていない Linux ディストリビューションを使用している場合 (「Amazon Elastic File System ユーザーガイド」の「サポートされているディストリビューション」を参照)、推奨されるマウント設定で再マウントする前にアップグレードすることをお勧めします。 Amazon Elastic File System

その他のリソース

- Encrypting data in transit

[Report columns] (レポート列)

- ステータス
- リージョン
- EFS ファイルシステム ID
- 接続が暗号化されていない AZ
- 最終更新日時

Amazon EBS パブリックスナップショット

説明

Amazon Elastic Block Store (Amazon EBS) ボリュームスナップショットのアクセス許可設定をチェックし、スナップショットが一般にアクセス可能である場合に警告します。

スナップショットを公開すると、すべての AWS アカウント およびユーザーにスナップショット上のすべてのデータへのアクセス許可が付与されます。特定のユーザーまたはアカウントとのみスナップショットを共有するには、スナップショットをプライベートとしてマークします。次に、スナップショットデータを共有するユーザーまたはアカウントを指定します。ブロックパブリックアクセスを「すべての共有をブロック」モードで有効にしている場合、パブリックスナップショットはパブリックにアクセスできず、このチェックの結果に表示されないことに注意してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

チェック ID

`ePs02jT06w`

アラート条件

赤: EBS ボリュームスナップショットはパブリックにアクセス可能です。

[Recommended Action] (推奨されるアクション)

スナップショット内のすべてのデータをすべての AWS アカウント およびユーザーと共有することが確実でない限り、アクセス許可を変更します。スナップショットをプライベートとしてマークし、アクセス許可を付与するアカウントを指定します。詳細については、「Amazon EBS スナップショットの共有」を参照してください。EBS スナップショットのパブリックアクセスのブロックを使用して、データへのパブリックアクセスを許可する設定を管理します。このチェックは、 Trusted Advisor コンソールのビューから除外することはできません。

スナップショットのアクセス許可を直接変更するには、 AWS Systems Manager コンソールでランブックを使用します。詳細については、「AWSSupport-ModifyEBSSnapshotPermission」を参照してください。

その他のリソース

Amazon EBS スナップショット

[Report columns] (レポート列)

- ステータス
- リージョン
- ボリューム ID
- スナップショット ID
- 説明

Amazon RDS Aurora ストレージの暗号化は無効になっています

説明

Amazon RDS では、 AWS Key Management Serviceで管理しているキーを使用して、すべてのデータベースエンジンの保存時の暗号化をサポートしています。Amazon RDS 暗号化を使用するアクティブな DB インスタンスでは、ストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットのように暗号化されます。

Aurora DB クラスターの作成時に暗号化が有効になっていない場合は、復号化されたスナップショットを暗号化された DB クラスターに復元する必要があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、3～5 Trusted Advisor 日間、 で Amazon RDS のレコメンデーションを表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt005`

アラート条件

赤: Amazon RDS Aurora リソースでは暗号化が有効になっていません。

[Recommended Action] (推奨されるアクション)

DB クラスターの保管中のデータの暗号化を有効にします。

その他のリソース

DB インスタンスの作成時に暗号化を有効にすることも、回避策を使用してアクティブな DB インスタンスの暗号化を有効にすることもできます。復号化された DB クラスターを暗号化された DB クラスターに変更することはできません。ただし、複合化されたスナップショットを暗号化された DB クラスターに復元することはできます。復号されたスナップショットから復元する場合は、 AWS KMS キーを指定する必要があります。

詳細については、「Amazon Aurora リソースの暗号化」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース

- エンジン名
- 最終更新日時

Amazon RDS エンジンのマイナーバージョンアップグレードが必須です。

説明

データベースリソースで最新のマイナー DB エンジンバージョンが実行されていません。最新のマイナーバージョンには、最新のセキュリティ修正プログラムやその他の改善が含まれています。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、3～5 Trusted Advisor 日間、 で Amazon RDS のレコメンデーションを表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

```
c1qf5bt003
```

アラート条件

黄: Amazon RDS リソースは最新のマイナー DB エンジンバージョンを実行していません。

[Recommended Action] (推奨されるアクション)

最新バージョンにアップグレードします。

その他のリソース

最新の DB エンジンのマイナーバージョンには、最新のセキュリティと機能の修正が含まれているため、このバージョンでデータベースを保守することをお勧めします。DB エンジンのマイナーバージョンのアップグレードには、DB エンジンの同じメジャーバージョンの以前のマイナーバージョンと後方互換性のあるデータベースの変更のみが含まれます。

詳細については、「DB インスタンスのエンジンバージョンのアップグレード」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- 現行のエンジンバージョン
- 推奨値
- 最終更新日時

Amazon RDS パブリックスナップショット

説明

Amazon Relational Database Service (Amazon RDS) DB スナップショットのアクセス許可設定をチェックし、スナップショットがパブリックとしてマークされている場合に警告します。

スナップショットを公開すると、すべての AWS アカウント およびユーザーにスナップショット上のすべてのデータへのアクセス許可が付与されます。スナップショットを特定のユーザーまたはアカウントをのみ共有する場合は、そのスナップショットをプライベートとしてマークします。その後にスナップショットデータを共有するユーザーまたはアカウントを指定します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

チェック ID

rSs93HQwa1

アラート条件

赤: Amazon RDS スナップショットはパブリックとしてマークされています。

[Recommended Action] (推奨されるアクション)

スナップショット内のすべてのデータをすべての AWS アカウント およびユーザーと共有することが確実でない限り、アクセス許可を変更します。スナップショットをプライベートとしてマークし、アクセス許可を付与するアカウントを指定します。詳細については、「DB スナップショットまたは DB クラスタースナップショットの共有」を参照してください。このチェックは、 Trusted Advisor コンソールのビューから除外することはできません。

スナップショットのアクセス許可を直接変更するには、 AWS Systems Manager コンソールでランブックを使用できます。詳細については、「AWSSupport-ModifyRDSSnapshotPermission」を参照してください。

その他のリソース

Amazon RDS DB インスタンスのバックアップと復元

[Report columns] (レポート列)

- ステータス
- リージョン
- DB インスタンスまたはクラスター ID
- スナップショット ID

Amazon RDS セキュリティグループのアクセスリスク

説明

Amazon Relational Database Service (Amazon RDS) のセキュリティグループ設定をチェックし、セキュリティグループルールでデータベースへの過度なアクセスが許可されている場合に警告します。セキュリティグループルールの推奨設定は、特定の Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループまたは特定の IP アドレスからのアクセスのみを許可することです。

> **Note**
>
> このチェックでは、toAmazon RDS インスタンスにアタッチされているセキュリティグループのみが評価されます。 https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

チェック ID

`nNauJisYIT`

アラート条件

- 黄: DB セキュリティグループルールは、次のポートのいずれかでグローバルアクセス権を付与する Amazon EC2 セキュリティグループを参照しています: 20、21、22、1433、1434、3306、3389、4333、5432、5500。
- 赤: DB セキュリティグループルールはグローバルアクセス権を付与します (CIDR ルールのサフィックスは /0)。
- 緑: DB セキュリティグループには、許容ルールは含まれません。

[Recommended Action] (推奨されるアクション)

EC2-Classic は 2022 年 8 月 15 日に廃止されました。Amazon RDS インスタンスを VPC に移動し、Amazon EC2 セキュリティグループを使用することをお勧めします。DB インスタンスを VPC に移動する方法の詳細については、「VPC 外の DB インスタンスを VPC に移動する」を参照してください。

Amazon RDS インスタンスを VPC に移行できない場合は、セキュリティグループのルールを確認し、承認された IP アドレスまたは IP 範囲へのアクセスを制限します。セキュリティグループを編集するには、AuthorizeDBSecurityGroupIngress API または AWS Management Consoleを使用します。詳細については、「DB セキュリティグループの操作」を参照してください。

その他のリソース

- Amazon RDS セキュリティグループ
- クラスレスドメイン間ルーティング
- TCP と UDP のポート番号のリスト

[Report columns] (レポート列)

- ステータス
- リージョン

- RDS セキュリティグループ名
- 受信ルール
- 理由

Amazon RDS ストレージの暗号化は無効になっています。

説明

Amazon RDS では、 AWS Key Management Serviceで管理しているキーを使用して、すべてのデータベースエンジンの保存時の暗号化をサポートしています。Amazon RDS 暗号化を使用するアクティブな DB インスタンスでは、ストレージに保存されているデータは、自動バックアップ、リードレプリカ、スナップショットのように暗号化されます。

DB インスタンスの作成時に暗号化が有効になっていない場合は、暗号化を有効にする前に、復号化されたスナップショットの暗号化されたコピーを復元する必要があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、3～5 Trusted Advisor 日間、 で Amazon RDS のレコメンデーションを表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

c1qf5bt006

アラート条件

赤: Amazon RDS リソースでは暗号化が有効になっていません。

[Recommended Action] (推奨されるアクション)

DB インスタンスの保管中のデータの暗号化を有効にします。

その他のリソース

DB インスタンスを暗号化できるのは、DB インスタンスを作成するときだけです。既存のアクティブな DB インスタンスを暗号化するには:

元の DB インスタンスの暗号化されたコピーを作成する

1. DB インスタンスのスナップショットを作成します。
2. ステップ 1 で作成したスナップショットの暗号化されたコピーを作成します。
3. 暗号化されたスナップショットから DB インスタンスを復元します。

詳細については、以下のリソースを参照してください。

- Amazon RDS リソースを暗号化する
- DB スナップショットのコピー

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- 最終更新日時

S3 バケットを直接指定する Amazon Route 53 の CNAME レコードの不一致

説明

Amazon S3 バケットのホスト名を直接指す CNAME レコードを持つ Amazon Route 53 ホストゾーンをチェックし、CNAME が S3 バケット名と一致しない場合にアラートを出します。

チェック ID

c1ng44jvbm

アラート条件

赤: Amazon Route 53 ホストゾーンに、S3 バケットのホスト名の不一致を示す CNAME レコードがあります。

緑: Amazon Route 53 ホストゾーンと一致しない CNAME レコードはありませんでした。

[Recommended Action] (推奨されるアクション)

CNAME レコードを S3 バケットのホスト名に指定する場合は、設定した CNAME またはエイリアスレコードと一致するバケットが存在することを確認する必要があります。これにより、CNAME レコードが偽装されるリスクを回避できます。また、権限のない AWS ユーザーがドメインで障害や悪意のあるウェブコンテンツをホストしないようにします。

CNAME レコードが S3 バケットのホスト名に直接指定されないようにするには、オリジンアクセスコントロール (OAC) を使用し、Amazon CloudFront を通じて S3 バケットのウェブアセットにアクセスすることを検討してください。

CNAME を Amazon S3 バケットのホスト名に関連付ける方法の詳細については、「CNAME レコードを使用した Amazon S3 URL のカスタマイズ」を参照してください。

その他のリソース

- ホスト名を Amazon S3 バケットに関連付ける方法
- CloudFront を使用した Amazon S3 オリジンへのアクセスの制限

[Report columns] (レポート列)

- ステータス
- ホストゾーン ID
- ホストゾーン ARN
- 一致する CNAME レコード
- 一致しない CNAME レコード
- 最終更新日時

Amazon Route 53 MX リソースレコードセットと Sender Policy Framework

説明

MX レコードごとに、 は有効な SPF 値を含む関連付けられた TXT レコードをチェックします。TXT レコード値は「v=spf1」で始まる必要があります。SPF レコードタイプは、Internet Engineering Task Force (IETF) によって廃止されました。Route 53 では、SPF レコードの代わりに TXT レコードを使用するのがベストプラクティスではありません。MX レコードに有効な SPF 値を持つ TXT レコードが少なくとも 1 つ関連付けられている場合、 はこのチェックを緑として Trusted Advisor 報告します。

チェック ID

`c9D319e7sG`

アラート条件

- 緑: MX リソースレコードセットには、有効な SPF 値を含む TXT リソースレコードがあります。
- 黄: MX リソースレコードセットには、有効な SPF 値を含む TXT または SPF リソースレコードがあります。
- 赤: MX リソースレコードセットには、有効な SPF 値を含む TXT または SPF リソースレコードがありません。

[Recommended Action] (推奨されるアクション)

MX リソースレコードセットごとに、有効な SPF 値を含む TXT リソースレコードセットを作成します。詳細については、「Sender Policy Framework: SPF Record Syntax」(Sender Policy Framework: SPF レコード構文) および「Amazon Route 53 コンソールを使用したリソースレコードセットの作成」を参照してください。

その他のリソース

- MX レコードタイプ
- SPF レコードタイプ
- re:Post ガイダンス
- RFC 7208

[Report columns] (レポート列)

- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名

- ステータス

Amazon S3 バケット許可

説明

オープンアクセス許可を持つ、または認証された AWS ユーザーへのアクセスを許可する Amazon Simple Storage Service (Amazon S3) のバケットをチェックします。

このチェックでは、明示的なバケットアクセス許可、およびそのアクセス許可をオーバーライドする可能性のあるバケットポリシーが調べられます。Amazon S3 バケットのすべてのユーザーにリストアクセス許可を付与することは推奨されません。これらのアクセス許可により、意図しないユーザーがバケット内のオブジェクトを頻繁にリストすることがあります。結果として、予想される料金よりも高くなる可能性があります。すべてのユーザーにアップロードと削除のアクセス許可を付与すると、バケットのセキュリティの脆弱性が生じる可能性があります。

チェック ID

`Pfx0RwqBli`

アラート条件

- 黄色: バケット ACL では、[全員] または [認証済みの AWS ユーザー] に対して「リスト」アクセスが許可されます。
- 黄: バケットポリシーは、あらゆる種類のオープンアクセスを許可します。
- 黄: バケットポリシーには、パブリックアクセス権を付与するステートメントがあります。[Block public and cross-account access to buckets that have public policies] (パブリックポリシーが設定されているバケットへのパブリックアクセスとクロスアカウントアクセスをブロック) がオンになり、パブリックステートメントが削除されるまで、そのアカウントの許可されたユーザーのみにアクセスが制限されます。
- 黄： Trusted Advisor ポリシーを確認するアクセス許可がないか、他の理由でポリシーを評価できませんでした。
- 赤色: バケット ACL では、[全員] または [認証済みの AWS ユーザー] に対して「アップロード」および「削除」アクセスが許可されます。
- 緑: すべての Amazon S3 は、ACL および/またはバケットポリシーに準拠しています。

[Recommended Action] (推奨されるアクション)

バケットがオープンアクセスを許可している場合、オープンアクセスが本当に必要かどうかを判断します。例えば、静的ウェブサイトをホストするには、Amazon CloudFront を使用して

Amazon S3 でホストされているコンテンツを配信できます。anAmazon CloudFront デベロッパーガイド」の「Amazon S3 オリジンへのアクセスの制限」を参照してください。 Amazon CloudFront 可能であれば、バケットのアクセス許可を更新して、所有者または特定のユーザーへのアクセスを制限します。Amazon S3 のパブリックアクセスのブロックを使用して、データへのパブリックアクセスを許可する設定を管理します。「バケットとオブジェクトのアクセス許可の設定」を参照してください。

その他のリソース

Managing Access Permissions to Your Amazon S3 Resources (Amazon S3 リソースへのアクセス許可の管理)

Amazon S3 バケットのブロックパブリックアクセス設定の構成

[Report columns] (レポート列)

- ステータス
- リージョン名
- リージョン API パラメータ
- バケット名
- ACL でリストを許可
- ACL でアップロード/削除を許可
- ポリシーでアクセスを許可

DNS 解決が無効になっている Amazon VPC ピアリング接続

説明

VPC ピアリング接続で、アクセプターとリクエスター VPC の両方の DNS 解決が有効になっているかどうかを確認します。

VPC ピアリング接続の DNS 解決により、パブリック DNS ホスト名がプライベート IPv4 アドレスに解決されるように VPC からクエリを実行することができます。これにより、ピアリングされた VPC 内のリソース間の通信に DNS 名を使用できるようになります。VPC ピアリング接続の DNS 解決により、アプリケーションの開発と管理が簡単になり、エラーが発生しにくくなります。また、リソースは常に VPC ピアリング接続を介してプライベートに通信できます。

AWS Config ルールの vpcIds パラメータを使用して VPC IDs を指定できます。

詳細については、「VPC ピアリング接続の DNS 解決を有効にする」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz124`

ソース

`AWS Config Managed Rule: vpc-peering-dns-resolution-check`

アラート条件

黄: VPC ピアリング接続のアクセプター VPC とリクエスタ VPC の両方で DNS 解決が有効になっていません。

[Recommended Action] (推奨されるアクション)

VPC ピアリング接続の DNS 解決を有効にします。

その他のリソース

- VPC ピアリング接続オプションを変更する
- VPC 内の DNS 属性

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Application Load Balancer ターゲットグループの暗号化プロトコル

説明

Application Load Balancer (ALB) ターゲットグループが HTTPS プロトコルを使用して、バックエンドターゲットタイプのインスタンスまたは IP の転送中の通信を暗号化していることを確認します。ALB とバックエンドターゲット間の HTTPS リクエストは、転送中のデータの機密性を維持するのに役立ちます。

チェック ID

`c2vlfg0p1w`

アラート条件

- 黄: HTTP を使用する Application Load Balancer ターゲットグループ。
- 緑: HTTPS を使用する Application Load Balancer ターゲットグループ。

[Recommended Action] (推奨されるアクション)

HTTPS アクセスをサポートするようにバックエンドのターゲットタイプのインスタンスまたは IP を設定し、HTTPS プロトコルを使用して ALB とバックエンドのターゲットタイプのインスタンスまたは IP 間の通信を暗号化するようにターゲットグループを変更します。

その他のリソース

転送中の暗号化を強制する

Application Load Balancer のターゲットタイプ

Application Load Balancer のルーティング設定

Elastic Load Balancing でのデータ保護

[Report columns] (レポート列)

- ステータス
- リージョン
- ALB Arn
- ALB 名
- ALB VPC ID
- ターゲットグループ ARN

- ターゲットグループ名
- ターゲットグループプロトコル
- 最終更新日時

AWS Backup リカバリポイントの削除を防ぐためのリソースベースのポリシーがないボールト

説明

AWS Backup ボールトに、復旧ポイントの削除を防止するリソースベースのポリシーがアタッチされているかどうかを確認します。

リソースベースのポリシーにより、リカバリポイントが予期せず削除されるのを防ぐことができるため、バックアップデータに対して最小特権でアクセス制御を行うことができます。

ルールの principalArnList パラメータ AWS Config でルールにチェックさせたくない AWS Identity and Access Management ARNsを指定できます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz152
```

ソース

```
AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled
```

アラート条件

黄: 復旧ポイントの削除を防ぐためのリソースベースのポリシーがない AWS Backup ボールトがあります。

[Recommended Action] (推奨されるアクション)

復旧ポイントが予期せず削除されないように、 AWS Backup ボールトのリソースベースのポリシーを作成します。

ポリシーに
は、backup:DeleteRecoveryPoint、backup:UpdateRecoveryPointLifecycle、backup:PutBackupVaultAcce
権限を含む「拒否」ステートメントを含める必要があります。

詳細については、「Set access policies on backup vaults」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CloudTrail ログ記録

説明

の使用を確認します AWS CloudTrail。CloudTrail は、アカウントで行われた AWS API コールに関する情報を記録 AWS アカウント することで、 のアクティビティの可視性を高めます。このログを使用して、特定のユーザーが指定期間にどのようなアクションを行ったか、指定期間に特定のリソースに対してどのユーザーがアクションを実行したかを判断できます。

CloudTrail はログファイルを Amazon Simple Storage Service (Amazon S3) バケットに配信するため、CloudTrail には、そのバケットに対する書き込みアクセス許可が必要です。証跡をすべてのリージョンに適用する場合 (新しい証跡を作成した場合のデフォルト)、証跡は Trusted Advisor レポートに複数回表示されます。

チェック ID

`vjafUGJ9H0`

アラート条件

- 黄: CloudTrail は、証跡のログ配信エラーを報告します。

- 赤: リージョンの証跡が作成されていないか、証跡のログ記録がオフになっています。

[Recommended Action] (推奨されるアクション)

証跡を作成してコンソールからログ記録を開始するには、AWS CloudTrail コンソールに移動します。

ログ記録を開始するには、「Stopping and Starting Logging for a Trail」(証跡のログ記録の停止と開始) を参照してください。

ログ配信エラーが発生した場合は、バケットが存在し、必要なポリシーがバケットにアタッチされていることを確認してください。「Amazon S3 バケットポリシー」を参照してください。

その他のリソース

- AWS CloudTrail ユーザーガイド
- サポートされるリージョン
- サポートされるサービス

[Report columns] (レポート列)

- ステータス
- リージョン
- 証跡名
- ログ記録のステータス
- バケット名
- ログ配信日

AWS CloudTrail 管理イベントのログ記録

説明

の使用を確認します AWS CloudTrail。CloudTrail は、 のアクティビティの可視性を向上させます AWS アカウント。これを行うには、アカウントで行われた AWS API コールに関する情報を記録します。このログを使用して、特定のユーザーが指定期間にどのようなアクションを行ったか、指定期間に特定のリソースに対してどのユーザーがアクションを実行したかを判断できます。

CloudTrail はログファイルを Amazon Simple Storage Service (Amazon S3) バケットに配信するため、CloudTrail には、そのバケットに対する書き込みアクセス許可が必要です。証跡がすべての AWS リージョン に適用される場合 (新しい証跡を作成するときのデフォルト) 、証跡はレポートに Trusted Advisor 複数回表示されます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c25hn9x03v`

アラート条件

- 赤: の証跡が作成されないか AWS リージョン、どの証跡でもログ記録が有効になっていません。
- 黄: CloudTrail は有効ですが、すべての証跡でログ配信エラーが報告されます。
- 緑: CloudTrail は有効になっており、ログ配信エラーは報告されません。

[Recommended Action] (推奨されるアクション)

証跡を作成してコンソールからログ記録を開始するには、AWS CloudTrail コンソールを開きます。

ログ記録を開始するには、「Stopping and Starting Logging for a Trail」(証跡のログ記録の停止と開始) を参照してください。

ログ配信エラーが表示された場合は、バケットが存在し、必要なポリシーがバケットにアタッチされていることを確認します。「Amazon S3 バケットポリシー」を参照してください。

その他のリソース

- AWS CloudTrail ユーザーガイド
- サポートされるリージョン
- サポートされるサービス
- 組織の証跡の作成

[Report columns] (レポート列)

- ステータス
- リージョン
- ログ記録が有効

- 報告された配信エラー
- 最終更新日時

AWS Lambda 非推奨ランタイムを使用する関数

説明

非推奨に近づいているランタイムを使用するように $LATEST バージョンが設定されている場合、または非推奨になっている Lambda 関数をチェックします。非推奨のランタイムは、セキュリティ更新プログラムやテクニカルサポートの対象外です。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

公開された Lambda 関数のバージョンは不変です。つまり、呼び出すことはできますが、更新することはできません。更新できるのは Lambda 関数の $LATEST バージョンのみです。詳細については、「Lambda 関数のバージョン」を参照してください。

チェック ID

`L4dfs2Q4C5`

アラート条件

- 赤: 関数の $LATEST バージョンは、既に廃止されているランタイムを使用するように設定されています。
- 黄: 関数の $LATEST バージョンは、180 日以内に廃止されるランタイムで実行されています。

[Recommended Action] (推奨されるアクション)

もうすぐ非推奨になるランタイムで実行されている関数がある場合は、サポート対象のランタイムへの移行に向けて準備する必要があります。詳細については、「Runtime support policy」(ランタイムサポートポリシー) を参照してください。

使用しなくなった以前の関数バージョンを削除することをお勧めします。

その他のリソース

Lambda ランタイム

[Report columns] (レポート列)

- ステータス
- リージョン
- 関数 ARN
- ランタイム
- 非推奨になるまでの日数
- 廃止日
- 平均日次呼び出し
- 最終更新日時

セキュリティに関する AWS Well-Architected のリスクの高い問題

説明

セキュリティの柱で、ワークロードに関するリスクの高い問題 (HRI) をチェックします。このチェックは、お客様の AWS-Well Architected レビューに基づきます。チェック結果は、AWS Well-Architected でワークロード評価を完了したかどうかによって異なります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`Wxdfp4B1L3`

アラート条件

- 赤: AWS Well-Architected のセキュリティの柱で、少なくとも 1 つのアクティブな高リスクの問題が特定されました。

- 緑: AWS Well-Architected のセキュリティの柱でアクティブな高リスクの問題は検出されませんでした。

[Recommended Action] (推奨されるアクション)

AWS Well-Architected は、ワークロード評価中に高リスクの問題を検出しました。これらの問題は、リスクを軽減し、費用を節約する機会を提示します。AWS Well-Architected ツールにサインインして、回答を確認し、アクティブな問題を解決するためのアクションを実行します。

[Report columns] (レポート列)

- ステータス
- リージョン
- ワークロードの ARN
- ワークロード名
- レビュー担当者名
- ワークロードタイプ
- ワークロードの開始日
- ワークロードの最終変更日
- セキュリティについて特定された HRI の数
- セキュリティについて解決された HRI の数
- セキュリティについての質問の数
- セキュリティの柱の質問の総数
- 最終更新日時

IAM 証明書ストアの CloudFront 独自 SSL 証明書

説明

IAM 証明書ストア内の CloudFront 代替ドメイン名の SSL 証明書をチェックします。このチェックでは、証明書の期限が切れている場合、近日中に証明書の期限が切れる場合、証明書で古い暗号化が使用されている場合、またはディストリビューションに対して証明書が正しく構成されていない場合にアラートが発生します。

代替ドメイン名のカスタム証明書の有効期限が切れると、CloudFront コンテンツを表示するブラウザにウェブサイトのセキュリティに関する警告メッセージが表示されることがあります。SHA-1 ハッシュアルゴリズムを使用して暗号化された証明書は、Chrome や Firefox などのほとんどのウェブブラウザで廃止されています。

証明書には、オリジンドメイン名、またはビューワーリクエストのホストヘッダー内のドメイン名のいずれかに一致するドメイン名が含まれている必要があります。一致しない場合、CloudFront は HTTP ステータスコード 502 (不正なゲートウェイ) をユーザーに返します。詳細については、「代替ドメイン名と HTTPS の使用」を参照してください。

チェック ID

N425c450f2

アラート条件

- 赤: カスタム SSL 証明書の有効期限が切れています。
- 黄: カスタム SSL 証明書は今後 7 日で期限切れになります。
- 黄: カスタム SSL 証明書が SHA-1 ハッシュアルゴリズムを使用して暗号化されています。
- 黄: ディストリビューション内の 1 つ以上の代替ドメイン名が、カスタム SSL 証明書の [Common Name] (共通名) フィールドにも [Subject Alternative Names] (サブジェクト代替名) フィールドにも表示されません。

[Recommended Action] (推奨されるアクション)

を使用してサーバー証明書 AWS Certificate Manager をプロビジョニング、管理、デプロイすることをお勧めします。ACM を使用すると、新しい証明書をリクエストしたり、既存の ACM または外部証明書を AWS リソースにデプロイしたりできます。ACM が提供する証明書は無料で、自動的に更新できます。ACM の使用の詳細については、AWS Certificate Manager ユーザーガイドを参照してください。ACM がサポートするリージョンを確認するには、「」の「AWS Certificate Manager エンドポイントとクォータ」を参照してください AWS 全般のリファレンス。

期限切れの証明書または期限切れが近い証明書を更新します。証明書の更新の詳細については、「IAM でのサーバー証明書の管理」を参照してください。

SHA-1 ハッシュアルゴリズムを使用して暗号化された証明書を、SHA-256 ハッシュアルゴリズムを使用して暗号化された証明書に置き換えます。

証明書を、[Common Names] (共通名) フィールドまたは [Subject Alternative Domain Names] (サブジェクト代替ドメイン名) フィールドに該当する値を含む証明書に置き換えます。

その他のリソース

HTTPS 接続を使用したオブジェクトへのアクセス

証明書のインポート

AWS Certificate Manager ユーザーガイド

[Report columns] (レポート列)

- ステータス
- ディストリビューション ID
- ディストリビューションドメイン名
- 証明書名
- 理由

オリジンサーバーの CloudFront 独自 SSL 証明書

説明

オリジンサーバーで、有効期限が切れている SSL 証明書、有効期限が近づいている SSL 証明書、欠落している SSL 証明書、または古い暗号化を使用している SSL 証明書をチェックします。証明書に上記のいずれかの問題がある場合、CloudFront は HTTP ステータスコード 502 (不正なゲートウェイ) を使用してコンテンツのリクエストに応答します。

SHA-1 ハッシュアルゴリズムを使用して暗号化された証明書は、Chrome や Firefox などのウェブブラウザで非推奨になる予定です。CloudFront ディストリビューションに関連付けた SSL 証明書の数によっては、このチェックにより、CloudFront ディストリビューションのオリジンとして Amazon EC2 または Elastic Load Balancing AWS を使用している場合など、ウェブホスティングプロバイダーの請求書に 1 か月あたり数セントが追加される場合があります。このチェックでは、オリジン証明書チェーンまたは認証局は検証されません。これらは CloudFront 設定で確認できます。

チェック ID

N430c450f2

アラート条件

- 赤: オリジンの SSL 証明書の有効期限が切れているか、存在しません。
- 黄: オリジンの SSL 証明書は今後 30 日以内に期限切れになります。
- 黄: オリジンの SSL 証明書が SHA-1 ハッシュアルゴリズムを使用して暗号化されています。
- 黄: オリジンの SSL 証明書が見つかりません。タイムアウトや他の HTTPS 接続の問題により、接続が失敗した可能性があります。

[Recommended Action] (推奨されるアクション)

有効期限が切れているか、間もなく期限切れになる場合は、オリジンで証明書を更新します。

証明書が存在しない場合は追加します。

SHA-1 ハッシュアルゴリズムを使用して暗号化された証明書を、SHA-256 ハッシュアルゴリズムを使用して暗号化された証明書に置き換えます。

その他のリソース

代替ドメイン名と HTTPS の使用

[Report columns] (レポート列)

- ステータス
- ディストリビューション ID
- ディストリビューションドメイン名
- オリジン
- 理由

ELB リスナーのセキュリティ

説明

暗号化された通信に推奨されるセキュリティ設定を使用しないリスナーを持つクラシックロードバランサーをチェックします。 AWS では、安全なプロトコル (HTTPS または SSL)、up-to-date セキュリティポリシー、安全な暗号とプロトコルを使用することをお勧めします。フロントエンド接続 (クライアントからロードバランサー) に安全なプロトコルを使用すると、クライアントとロードバランサーの間でリクエストが暗号化されます。これにより、より安全な環境が作成されます。Elastic Load Balancing は、セキュリティに関する AWS のベストプラクティスに準拠する暗号化およびプロトコルを使用する事前定義済みのセキュリティポリシーを提供します。新しい構成が利用可能になると、事前定義済みのポリシーの新しいバージョンがリリースされます。

チェック ID

`a2sEc6ILx`

アラート条件

- 赤: ロードバランサーには、セキュアプロトコル (HTTPS) で設定されたリスナーがありません。
- 黄: ロードバランサーの HTTPS リスナーは、弱い暗号を含むセキュリティポリシーで設定されています。

- 黄: ロードバランサーの HTTPS リスナーに、推奨されるセキュリティポリシーが設定されていません。
- 緑: ロードバランサーに少なくとも 1 つの HTTPS リスナーがあり、すべての HTTPS リスナーが推奨ポリシーで設定されています。

[Recommended Action] (推奨されるアクション)

ロードバランサーへのトラフィックをセキュリティで保護する必要がある場合は、フロントエンド接続に HTTPS または SSL プロトコルを使用します。

ロードバランサーを事前定義済みの SSL セキュリティポリシーの最新バージョンにアップグレードします。

推奨される暗号とプロトコルのみを使用してください。

詳細については、「Listener Configurations for Elastic Load Balancing」(Elastic Load Balancing のリスナー設定) を参照してください。

その他のリソース

- リスナー設定のクイックリファレンス
- ロードバランサーの SSL ネゴシエーション設定を更新する
- SSL Negotiation Configurations for Elastic Load Balancing (Elastic Load Balancing の SSL ネゴシエーション設定)
- SSL セキュリティポリシーのテーブル

[Report columns] (レポート列)

- ステータス
- リージョン
- ロードバランサー名
- ロードバランサーのポート
- 理由

Classic Load Balancer セキュリティグループ

説明

ロードバランサー用に設定されていないポートへのアクセスを許可するセキュリティグループで設定されたロードバランサーをチェックします。

ロードバランサー用に設定されていないポートへのアクセスがセキュリティグループで許可されている場合、データの損失や悪意のある攻撃のリスクが高くなります。

チェック ID

xSqX82fQu

アラート条件

- 黄: ロードバランサーに関連付けられた Amazon VPC セキュリティグループのインバウンドルールは、ロードバランサーのリスナー設定で定義されていないポートへのアクセスを許可します。
- 緑: ロードバランサーに関連付けられた Amazon VPC セキュリティグループのインバウンドルールは、ロードバランサーリスナー設定で定義されていないポートへのアクセスを許可しません。

[Recommended Action] (推奨されるアクション)

セキュリティグループルールを設定して、ロードバランサーのリスナー設定で定義されたポートとプロトコル、および Path MTU Discovery をサポートする ICMP プロトコルのみにアクセスを制限します。「Listeners for Your Classic Load Balancer」(Classic Load Balancer のリスナー) および「Security Groups for Load Balancers in a VPC」(VPC のロードバランサーのセキュリティグループ) を参照してください。

セキュリティグループがない場合は、ロードバランサーに新しいセキュリティグループを適用します。ロードバランサーのリスナー設定で定義されているポートとプロトコルのみにアクセスを制限するセキュリティグループルールを作成します。「VPC でのロードバランサーのセキュリティグループ」を参照してください。

その他のリソース

- Elastic Load Balancing ユーザーガイド
- Classic Load Balancer を移行する
- Classic Load Balancer を設定する

[Report columns] (レポート列)

- ステータス
- リージョン
- ロードバランサー名
- セキュリティグループ ID
- 理由

露出したアクセスキー

説明

一般に露出されているアクセスキー、およびアクセスキーが侵害された結果である可能性のある Amazon Elastic Compute Cloud (Amazon EC2) の不規則な使用状況について頻繁に使用されているコードリポジトリをチェックします。

アクセスキーは、アクセスキー ID とそれに対応するシークレットアクセスキーで構成されます。露出したアクセスキーは、アカウントや他のユーザーにセキュリティ上のリスクの原因となり、不正な活動や不正使用に起因する過度の請求が発生する可能性があるだけでなく、AWS カスタマーアグリーメントの違反になることがあります。

アクセスキーが露出している場合は、直ちにアカウントを保護してください。アカウントを過剰な料金から保護するために、 は AWS 一時的に一部の AWS リソースを作成する機能を制限します。これにより、アカウントのセキュリティが確保されるわけではありません。課金される可能性のある不正使用を部分的に制限するだけです。

> **Note**
>
> このチェックでは、露出したアクセスキーまたは侵害された EC2 インスタンスの識別は保証されません。アクセスキーと AWS リソースの安全性とセキュリティは、最終的にお客様の責任となります。
>
> > **Note**
> >
> > このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> > ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

アクセスキーの期限が表示され AWS アカウント た場合、不正使用がその日付までに停止されない場合、 は を停止 AWS することがあります。アラートがエラー状態であると思われる場合は、AWS サポートまで問い合わせてください。

に表示される情報は、アカウントの最新の状態を反映していない Trusted Advisor 可能性があります。アカウントで公開されているすべてのアクセスキーが解決されるまで、公開されたアクセ

スキーが解決済みとしてマークされることはありません。このデータ同期には、最大 1 週間かかる場合があります。

チェック ID

12Fnkpl8Y5

アラート条件

- 赤: 侵害された可能性がある - AWS は、インターネットで公開され、侵害された (使用された) 可能性があるアクセスキー ID と対応するシークレットアクセスキーを特定しました。
- 赤: 公開済み – AWS は、インターネットで公開されているアクセスキー ID と対応するシークレットアクセスキーを特定しました。
- 赤: 疑わしいです - Amazon EC2 の不規則な使用は、アクセスキーが侵害された可能性があることを示唆していますが、インターネット上で公開されていると識別されてはいません。

[Recommended Action] (推奨されるアクション)

影響を受けるアクセスキーを可能な限り早急に削除します。キーが IAM ユーザーに関連付けられている場合は、「IAM ユーザーのアクセスキーの管理」を参照してください。

アカウントで不正使用がないか確認してください。AWS Management Console にサインインし、疑わしいリソースがないか各サービスコンソールを確認します。Amazon EC2 インスタンスの実行、スポットインスタンスリクエスト、アクセスキー、IAM ユーザーには特に注意してください。Billing and Cost Management コンソールで全体的な使用状況を確認することもできます。

その他のリソース

- AWS アクセスキーを管理するためのベストプラクティス
- AWS セキュリティ監査ガイドライン

[Report columns] (レポート列)

- アクセスキー ID
- ユーザー名 (IAM またはルート)
- 不正行為のタイプ
- ケース ID
- 更新日時
- 場所
- Deadline
- 使用状況 (USD/日)

IAM アクセスキーローテーション

説明

過去 90 日間にローテーションされていないアクティブな IAM アクセスキーをチェックします。

アクセスキーを定期的にローテーションすると、侵害されたキーが知らないうちにリソースへのアクセスに使用される可能性を削減できます。このチェックでの最後のローテーション日時は、アクセスキーが作成された日または最後にアクティブ化された日です。アクセスキーの番号と日付は `access_key_1_last_rotated` および `access_key_2_last_rotated` 情報を直近の IAM 認証情報レポートから取得されます。

認証情報レポートの再生頻度は制限されているため、このチェックを更新しても最近の変更が反映されない場合があります。詳細については、「AWS アカウントの認証情報レポートの取得」を参照してください。

アクセスキーを作成してローテーションするには、ユーザーに適切な許可が必要です。詳細については、「Allow Users to Manage Their Own Passwords, Access Keys, and SSH Keys」(自らのパスワード、アクセスキー、および SSH キーの管理をユーザーに許可する) を参照してください。

チェック ID

`DqdJqYeRm5`

アラート条件

- 緑: アクセスキーはアクティブで、過去 90 日間にローテーションされています。
- 黄: アクセスキーはアクティブで、過去 2 年間でローテーションされましたが、90 日を超える期間が経過しています。
- 赤: アクセスキーはアクティブで、過去 2 年間ローテーションされていません。

[Recommended Action] (推奨されるアクション)

アクセスキーを定期的にローテーションします。「アクセスキーの更新」および「IAM ユーザーのアクセスキーの管理」を参照してください。

その他のリソース

- IAM ベストプラクティス
- IAM ユーザーのアクセスキーの更新方法。

[Report columns] (レポート列)

- ステータス

- IAM ユーザー
- アクセスキー
- 最後にローテーションしたキー
- 理由

IAM Access Analyzer の外部アクセス

説明

アカウントレベルで IAM Access Analyzer の外部アクセスが存在するかどうかを確認します。

IAM Access Analyzer の外部アクセスアナライザーは、外部エンティティと共有されているアカウント内のリソースを識別するのに役立ちます。次に、アナライザーは検出結果を含む一元化されたダッシュボードを作成します。新しいアナライザーが IAM コンソールでアクティブ化されると、セキュリティチームは過剰なアクセス許可に基づいて、レビューするアカウントを優先できます。外部アクセスアナライザーは、 リソースのパブリックおよびクロスアカウントアクセスの検出結果を作成し、追加料金なしで提供します。

チェック ID

`07602fcad6`

アラート条件

- 赤: アナライザーの外部アクセスはアカウントレベルでアクティブ化されていません。
- 緑: アナライザーの外部アクセスはアカウントレベルでアクティブ化されます。

[Recommended Action] (推奨されるアクション)

アカウントごとに外部アクセスアナライザーを作成すると、セキュリティチームは過剰なアクセス許可に基づいてレビューするアカウントを優先できます。詳細については、「検出結果の開始方法 AWS Identity and Access Management Access Analyzer」を参照してください。

さらに、未使用のアクセスアナライザーを利用するのがベストプラクティスです。これは、未使用のアクセスの検査を簡素化して最小特権に導く有料機能です。詳細については、「IAM ユーザーおよびロールに付与された未使用のアクセスの特定」を参照してください。

その他のリソース

- AWS Identity and Access Management Access Analyzerの使用
- IAM Access Analyzer の更新: 未使用のアクセスを検索し、デプロイ前にポリシーを確認する

[Report columns] (レポート列)

- ステータス
- リージョン
- アカウント外部アクセスアナライザー Arn
- Organization External Access Analyzer の ARN
- 最終更新日時

IAM パスワードポリシー

説明

アカウントのパスワードポリシーをチェックし、パスワードポリシーが有効になっていない場合やパスワードコンテンツの要件が有効になっていない場合に警告します。

パスワードコンテンツの要件は、強力なユーザーパスワードの作成を強制することによって AWS 環境の全体的なセキュリティを強化します。パスワードポリシーを作成または変更すると、変更は新しいユーザーに対してただちに適用されますが、既存のユーザーに対してパスワードの変更は強制されません。

チェック ID

`Yw2K9puPzl`

アラート条件

- 緑: パスワードポリシーが有効で、推奨コンテンツ要件が有効になっています。
- 黄: パスワードポリシーは有効になっていますが、少なくとも 1 つのコンテンツ要件が有効になっていません。

[Recommended Action] (推奨されるアクション)

一部のコンテンツ要件が有効になっていない場合は、有効にすることを検討してください。パスワードポリシーが有効になっていない場合は、パスワードポリシーを作成して設定します。「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。

にアクセスするには AWS Management Console、IAM ユーザーにパスワードが必要です。ベストプラクティスとして、 では、IAM ユーザーを作成する代わりにフェデレーションを使用することを AWS 強くお勧めします。フェデレーションでは、ユーザーは既存の企業認証情報を使用して、 AWS Management Consoleにログインできます。IAM Identity Center を使用してユーザーを作成またはフェデレーションし、アカウントに IAM ロールを引き受けます。

ID プロバイダーとフェデレーションの詳細については、「IAM ユーザーガイド」の「ID プロバイダーとフェデレーション」を参照してください。IAM Identity Center の詳細については、「IAM Identity Center ユーザーガイド」を参照してください。

その他のリソース

パスワードの管理

[Report columns] (レポート列)

- パスワードポリシー
- 大文字
- 小文字
- 数値
- 英数字以外

IAM SAML 2.0 ID プロバイダー

説明

AWS アカウント が SAML 2.0 をサポートする ID プロバイダー (IdP) 経由でアクセスするように設定されているかどうかを確認します。ID を一元化し、外部 ID プロバイダーまたは でユーザーを設定するときは、必ずベストプラクティスに従ってくださいAWS IAM Identity Center。

チェック ID

`c2v1fg0p86`

アラート条件

- 黄: このアカウントは、SAML 2.0 をサポートする ID プロバイダー (IdP) を介したアクセス用に設定されていません。
- 緑: このアカウントは、SAML 2.0 をサポートする ID プロバイダー (IdP) 経由でアクセスするように設定されています。

[Recommended Action] (推奨されるアクション)

の IAM アイデンティティセンターをアクティブ化します AWS アカウント。詳細については、「EnablingIAM Identity Center」を参照してください。IAM Identity Center を有効にすると、権限セットの作成や Identity Center グループへのアクセスの割り当てなどの一般的なタスクを実行できます。詳細については、「一般的なタスク」を参照してください。

IAM Identity Center で人間のユーザーを管理するのがベストプラクティスです。ただし、小規模デプロイでは、短期的に人間のユーザーに対して IAM によるフェデレーティッドユーザーアクセスをアクティブ化できます。詳細については、「SAML 2.0 フェデレーション」を参照してください。

その他のリソース

IAM Identity Centerとは何ですか?

IsIAMとは

[Report columns] (レポート列)

- ステータス
- AWS アカウント ID
- 最終更新日時

ルートアカウントの MFA

説明

ルートアカウントをチェックし、多要素認証 (MFA) が有効でない場合に警告します。

セキュリティを強化するには、MFA を使用してアカウントを保護することをお勧めします。MFA では、 AWS Management Console および関連するウェブサイトを操作するときに、ユーザーが MFA ハードウェアまたは仮想デバイスから一意の認証コードを入力する必要があります。

> **Note**
>
> AWS Organizations 管理アカウントの場合、AWS は にアクセスするときにルートユーザーの多要素認証 (MFA) を必要とします AWS Management Console。
> AWS Organizations メンバーアカウントの場合、AWS は MFA の使用を推奨します。MFA の適用に加えて、 AWS Organizations を使用して複数のアカウントを管理する場合は、SCP を適用してメンバーアカウントのルートユーザーへのアクセスを制限できます。詳細については、「 AWS Organizations ユーザーガイド」の「メンバーアカウントのベストプラクティス」を参照してください。

チェック ID

`7DAFEmoDos`

アラート条件

赤: MFA がルートアカウントで有効になっていません。

[Recommended Action] (推奨されるアクション)

ルートアカウントにログインし、MFA デバイスをアクティブ化します。「MFA ステータスのチェック」および「Setting Up an MFA Device」(MFA デバイスのセットアップ) を参照してください。

セキュリティ認証情報ページにアクセスして、アカウントでいつでも MFA をアクティブ化できます。これを行うには、 でアカウントメニューのドロップダウンを選択しますAWS Management Console。AWS は、FIDO2 や仮想認証など、複数の業界標準の MFA 形式をサポートしています。これにより、ニーズを満たす MFA デバイスを柔軟に選択できます。MFA デバイスの 1 つが失われたり動作が停止したりした場合の回復性のために、複数の MFA デバイスを登録するのがベストプラクティスです。

その他のリソース

詳細については、theIAMユーザーガイド」の「MFA デバイスをアクティブ化する一般的な手順」および AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

ルートユーザーアクセスキー

説明

ルートユーザーのアクセスキーが存在するかどうかを確認します。ルートユーザーのアクセスキーペアを作成しないことを強くお勧めします。ルートユーザーが必要なタスクはごくわずかであり、通常、これらのタスクは頻繁に実行されないため、ルートユーザータスクを実行する AWS Management Console には にログインすることをお勧めします。アクセスキーを作成する前に、長期的なアクセスキーに代わる方法を確認してください。

チェック ID

`c2vlfg0f4h`

アラート条件

赤: ルートユーザーアクセスキーが存在する

緑: ルートユーザーアクセスキーが存在しません

[Recommended Action] (推奨されるアクション)

ルートユーザーのアクセスキー (複数可) を削除します。「ルートユーザーのアクセスキーの削除」を参照してください。このタスクは、ルートユーザーが実行する必要があります。IAM ユーザーまたはロールとしてこれらの手順を実行することはできません。

その他のリソース

ルートユーザーの認証情報を必要とするタスク

紛失または忘れたルートユーザーパスワードのリセット

[Report columns] (レポート列)

- ステータス
- アカウント ID
- 最終更新日時

セキュリティグループ — 開かれたポート

説明

セキュリティグループで特定のポートへの無制限アクセス (0.0.0.0/0) を許可するルールを確認します。

無制限のアクセスでは、悪意のあるアクティビティ (ハッキング、サービス拒否攻撃、データ損失) の機会が増えます。リスクが最も高いポートには赤色のフラグが付けられ、リスクが低いポートには黄色のフラグが付けられます。緑色のフラグが付いたポートは、通常、HTTP や SMTP など、無制限のアクセスを必要とするアプリケーションで使用されます。

この方法でセキュリティグループを意図的に設定した場合は、追加のセキュリティ対策を使用してインフラストラクチャ (IP テーブルなど) を保護することをお勧めします。

> **Note**
>
> このチェックでは、作成したセキュリティグループと IPv4 アドレスのインバウンドルールのみが評価されます。によって AWS Directory Service 作成されたセキュリティグループには赤または黄色のフラグが付けられますが、セキュリティリスクはなく、除外できます。詳細については、「Trusted Advisor FAQ」を参照してください。

チェック ID

HCP4007jGY

アラート条件

- 緑: セキュリティグループは、ポート 80、25、443、または 465 で無制限にアクセスできます。
- 赤: セキュリティグループはリソースにアタッチされ、ポート 20、21、22、1433、1434、3306、3389、4333、5432、または 5500 への無制限のアクセスを提供します。
- 黄: セキュリティグループは、他のポートへの無制限のアクセスを提供します。
- 黄: セキュリティグループはどのリソースにもアタッチされず、無制限のアクセスを提供します。

[Recommended Action] (推奨されるアクション)

アクセスを必要とする IP アドレスのみに制限します。特定の IP アドレスにアクセスを制限するには、サフィックスを /32 に設定します (例: 192.0.2.10/32)。より制限の厳しいルールを作成した後は、必ず過度に許容的なルールを削除してください。

未使用のセキュリティグループを確認して削除します。を使用して AWS Firewall Manager 、 全体のセキュリティグループを大規模に一元的に設定および管理できます。詳細については AWS アカウント、 AWS Firewall Manager ドキュメントを参照してください。

EC2 インスタンスへの SSH (ポート 22) および RDP (ポート 3389) アクセスに Systems Manager Sessions Manager を使用することを検討してください。セッションマネージャーを使用すると、セキュリティグループでポート EC2 と 3389 を有効にすることなく EC2 インスタンスにアクセスできます。

その他のリソース

- Amazon EC2 セキュリティグループ

  TCP と UDP のポート番号のリスト
- クラスレスドメイン間ルーティング
- Session Manager の使用
- AWS Firewall Manager

[Report columns] (レポート列)

- ステータス

- リージョン
- セキュリティグループ名
- セキュリティグループ ID
- プロトコル
- 送信元ポート
- 送信先ポート
- 関連付け

セキュリティグループ — 無制限アクセス

説明

セキュリティグループでリソースへの無制限アクセスを許可するルールをチェックします。

無制限のアクセスでは、悪意のあるアクティビティ (ハッキング、サービス拒否攻撃、データ損失) の機会が増えます。

> **Note**
>
> このチェックでは、作成したセキュリティグループと IPv4 アドレスのインバウンドルールのみが評価されます。によって作成されたセキュリティグループ AWS Directory Service には赤または黄色のフラグが付けられますが、セキュリティリスクはなく、除外できます。詳細については、「Trusted Advisor FAQ」を参照してください。

チェック ID

`1iG5NDGVre`

アラート条件

- 緑: セキュリティグループルールには、ポート 25、80、または 443 の /0 サフィックスが付いた送信元 IP アドレスがあります。
- 黄: セキュリティグループルールには、25、80、または 443 以外のポートのサフィックスが /0 のソース IP アドレスがあり、セキュリティグループはリソースにアタッチされています。
- 赤: セキュリティグループルールには、25、80、または 443 以外のポートの /0 サフィックスを持つソース IP アドレスがあり、セキュリティグループはリソースにアタッチされていません。

[Recommended Action] (推奨されるアクション)

アクセスを必要とする IP アドレスのみに制限します。特定の IP アドレスにアクセスを制限するには、サフィックスを /32 に設定します (例: 192.0.2.10/32)。より制限の厳しいルールを作成した後は、必ず過度に許容的なルールを削除してください。

未使用のセキュリティグループを確認して削除します。を使用して AWS Firewall Manager 、 全体のセキュリティグループを一元的に設定および管理できます。詳細については AWS アカウント、 AWS Firewall Manager ドキュメントを参照してください。

EC2 インスタンスへの SSH (ポート 22) および RDP (ポート 3389) アクセスに Systems Manager Sessions Manager を使用することを検討してください。セッションマネージャーを使用すると、セキュリティグループでポート EC2 と 3389 を有効にすることなく EC2 インスタンスにアクセスできます。

その他のリソース

- Amazon EC2 セキュリティグループ
- クラスレスドメイン間ルーティング
- Session Manager の使用
- AWS Firewall Manager

[Report columns] (レポート列)

- ステータス
- リージョン
- セキュリティグループ名
- セキュリティグループ ID
- プロトコル
- 送信元ポート
- 送信先ポート
- IP 範囲
- 関連付け

耐障害性

耐障害性カテゴリの次のチェックを使用できます。

チェック名

- ALB マルチ AZ
- Amazon Aurora MySQL クラスターでバックトラッキングが有効になっていない
- Amazon Aurora インスタンスアクセシビリティ
- Amazon CloudFront のオリジンフェイルオーバー
- Amazon Comprehend エンドポイントアクセスリスク
- Amazon DocumentDB シングル AZ クラスター
- Amazon DynamoDB のポイントインタイムリカバリ
- Amazon DynamoDB テーブルは Backup プランに含まれていない
- Amazon EBS は AWS Backup プランに含まれていません
- Amazon EBS スナップショット
- Amazon EC2 Auto Scaling では ELB ヘルスチェックが有効になっていない
- Amazon EC2 Auto Scaling グループでキャパシティの再調整が有効
- Amazon EC2 Auto Scaling が複数の AZ にデプロイされていないか、AZ の最小数に達していない
- Amazon EC2 アベイラビリティーゾーンのバランス
- Amazon EC2 詳細モニタリングが有効化されていません
- ブロックモードの Amazon ECS AWS Logs ドライバー
- 単一の AZ を使用した Amazon ECS サービス
- Amazon ECS マルチ AZ 配置戦略
- Amazon EFS マウントターゲット冗長性なし
- Amazon EFS が AWS Backup プランに含まれていない
- Amazon ElastiCache マルチ AZ クラスター
- ElastiCache (Redis OSS) クラスターの自動バックアップ
- Amazon MemoryDB マルチ AZ クラスター
- Amazon MSK ブローカーがホストするパーティションの数が多すぎる
- Amazon MSK クラスターマルチ AZ
- データノードが 3 つ未満の Amazon OpenSearch Service ドメイン
- Amazon RDS バックアップ
- Amazon RDS 継続的バックアップが有効になっていない

- Amazon RDS DB クラスターには 1 つの DB インスタンスがあります。
- すべてのインスタンスが同じアベイラビリティーゾーンにある Amazon RDS DB クラスター
- すべてのリーダーインスタンスが同じアベイラビリティゾーンにある Amazon RDS DB クラスター
- Amazon RDS DB インスタンス拡張モニタリングが有効化されていない
- Amazon RDS DB インスタンスのストレージの自動スケーリングが無効になっています
- Amazon RDS DB インスタンスがマルチ AZ 配置を使用していない
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- Amazon RDS のログ出力パラメータはテーブルに設定されます。
- Amazon RDS の innodb_default_row_format パラメータ設定は安全ではない
- Amazon RDS innodb_flush_log_at_trx_commit パラメータが 1 ではありません
- Amazon RDS max_user_connections パラメータが低くなっています
- Amazon RDS Multi-AZ
- Amazon RDS が AWS Backup プランに含まれていない
- Amazon RDS リードレプリカは書き込み可能モードで開かれます。
- Amazon RDS リソースの自動バックアップは無効になっています。
- Amazon RDS sync_binlog パラメータは無効になっています
- RDS DB クラスターでマルチ AZ レプリケーションが有効になっていない
- RDS マルチ AZ スタンバイインスタンスが有効になっていない
- Amazon RDS ReplicaLag
- Amazon RDS の synchronous_commit パラメータは無効になっています。
- Amazon Redshift クラスターの自動スナップショット
- 削除された Amazon Route 53 ヘルスチェック
- Amazon Route 53 フェイルオーバーリソースレコードセット
- Amazon Route 53 高 TTL リソースレコードセット
- Amazon Route 53 ネームサーバー権限移譲
- Amazon Route 53 Resolver エンドポイントアベイラビリティーゾーンの冗長性
- Amazon S3 バケットロギング

- Amazon S3 バケットレプリケーションが有効になっていない
- Amazon S3 バケットバージョニング
- Application、Network、Gateway Load Balancer が、複数のアベイラビリティーゾーンにまたがっていない
- サブネットで利用可能な IP の自動スケーリング
- Auto Scaling Group ヘルスチェック
- Auto Scaling グループリソース
- AWS CloudHSM 単一の AZ で HSM インスタンスを実行するクラスター
- AWS Direct Connect ロケーションの耐障害性
- AWS Lambda デッドレターキューが設定されていない 関数
- AWS Lambda 失敗時のイベントの送信先
- AWS Lambda VPC 対応関数 (マルチ AZ 冗長性なし)
- AWS Outposts シングルラックデプロイ
- AWS Resilience Hub アプリケーションコンポーネントのチェック
- AWS Resilience Hub ポリシー違反
- AWS Resilience Hub レジリエンススコア
- AWS Resilience Hub 評価期間
- AWS Site-to-Site VPN に DOWN ステータスのトンネルが少なくとも 1 つある
- 信頼性に関する AWS Well-Architected のリスクの高い問題
- Classic Load Balancer に複数のAZが設定されていない
- CLB 接続ドレイン
- ELB ターゲット不均衡
- GWLB - エンドポイント AZ の独立性
- ロードバランサーの最適化
- NAT ゲートウェイ AZ インディペンデンス
- Network Firewall エンドポイント AZ の独立性
- Network Firewall マルチ AZ
- Network Load Balancer のクロスロードバランシング
- NLB - プライベートサブネット内のインターネット向けリソース
- NLB マルチ AZ

- Incident Manager レプリケーションセット AWS リージョン 内の の数
- シングル AZ アプリケーションチェック
- 複数の AZ の VPC インターフェイスエンドポイントネットワークインターフェイス
- VPN トンネルの冗長性
- ActiveMQ アベイラビリティーゾーンの冗長性
- RabbitMQ アベイラビリティーゾーンの冗長性

ALB マルチ AZ

説明

Application Load Balancer が複数のアベイラビリティーゾーン (AZ) を使用するように設定されているかどうかを確認します。AZ は、他のゾーンの障害から隔離された独立した場所です。同じリージョンの複数の AZ にロードバランサーを設定すると、ワークロードの可用性が向上します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dfprch08`

アラート条件

黄色: 単一の AZ に ALB があります。

緑: 2 つ以上の AZ が ALB にあります。

[Recommended Action] (推奨されるアクション)

ロードバランサーが、少なくとも 2 つのアベイラビリティーゾーンで設定されているようにします。

詳細については、「Application Load Balancer のアベイラビリティーゾーン」を参照してください。

その他のリソース

詳細については、次のドキュメントを参照してください。

- Elastic Load Balancing の仕組み
- リージョン、アベイラビリティーゾーン、およびローカルゾーン

[Report columns] (レポート列)

- ステータス
- リージョン
- ALB 名
- ALB ルール
- ALB ARN
- AZ の数
- 最終更新日時

Amazon Aurora MySQL クラスターでバックトラッキングが有効になっていない

説明

Amazon Aurora MySQL クラスターでバックトラッキングが有効になっているかどうかを確認します。

Amazon Aurora MySQL クラスターのバックトラッキングは、新しいクラスターを作成せずに Aurora DB クラスターを以前の時点に復元できる機能です。これにより、スナップショットから復元する必要なく、保持期間内の特定の時点までデータベースをロールバックできます。

ルールの BacktrackWindowInHours パラメータでバックトラック時間枠 (時間) を調整できます AWS Config 。

詳細については、「Aurora DB クラスターのバックトラック」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz131`

ソース

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

アラート条件

黄: Amazon Aurora MySQL クラスターでバックトラッキングが有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon Aurora MySQL クラスターのバックトラッキングを有効にします。

詳細については、「Aurora DB クラスターのバックトラック」を参照してください。

その他のリソース

Aurora DB クラスターのバックトラック

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon Aurora インスタンスアクセシビリティ

説明

Amazon Aurora DB クラスターにプライベートインスタンスとパブリックインスタンスの両方があるケースをチェックします。

プライマリインスタンスが失敗した場合、 レプリカはプライマリ DB インスタンスに昇格できます。レプリカがプライベートである場合、パブリックアクセスのみを持つユーザーは、フェールオーバー後にデータベースに接続できなくなります。クラスター内のすべての DB インスタンスのアクセシビリティを同じにすることをお勧めします。

チェック ID

`xuy7H1avtl`

アラート条件

黄: Aurora DB クラスターのインスタンスは、アクセシビリティが異なります (パブリックとプライベートの混在)。

[Recommended Action] (推奨されるアクション)

DB クラスター内のインスタンスの `Publicly Accessible` 設定を変更して、すべてがパブリックまたはプライベートになるようにします。詳細については、「Modifying a DB Instance Running the MySQL Database Engine」(MySQL データベースエンジンを実行している DB インスタンスの変更) の MySQL インスタンスの手順を参照してください。

その他のリソース

Aurora DB クラスターの耐障害性

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター
- パブリック DB インスタンス
- プライベート DB インスタンス
- 理由

Amazon CloudFront のオリジンフェイルオーバー

説明

Amazon CloudFront の 2 つのオリジンを含むディストリビューションに対してオリジングループが設定されているかどうかを確認します。

詳細については、「CloudFront オリジンフェイルオーバーによる高可用性の最適化」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz112`

ソース

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

アラート条件

黄: Amazon CloudFront オリジンフェイルオーバーは有効化されていません。

[Recommended Action] (推奨されるアクション)

CloudFront ディストリビューションのオリジンフェイルオーバー機能をオンにして、エンドユーザーへのコンテンツ配信の高可用性を確保してください。この機能を有効にすると、プライマリオリジンサーバーが使用できなくなった場合、トラフィックはバックアップオリジンサーバーに自動的にルーティングされます。これにより、潜在的なダウンタイムが最小限に抑えられ、コンテンツの継続的な可用性が確保されます。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon Comprehend エンドポイントアクセスリスク

説明

基盤となるモデルがカスタマーマネージドキーを使用して暗号化されたエンドポイントの AWS Key Management Service（ AWS KMS) キーのアクセス許可をチェックします。カスタマーマネージドキーが無効になっている場合、または、Amazon Comprehend の付与された許可を変更するようにキーポリシーが変更された場合、エンドポイントの可用性が影響を受ける可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> 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のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

チェック ID

`Cm24dfsM13`

アラート条件

赤: カスタマーマネージドキーが無効になっているか、キーポリシーが変更されて、Amazon Comprehend アクセス用に付与されている許可が変更されました。

[Recommended Action] (推奨されるアクション)

カスタマーマネージドキーが無効になっている場合は、有効にすることをお勧めします。詳細については、「キーの有効化」を参照してください。キーポリシーが変更され、エンドポイントを引き続き使用する場合は、 AWS KMS キーポリシーを更新することをお勧めします。詳細については、「キーポリシーの変更」を参照してください。

その他のリソース

AWS KMS アクセス許可

[Report columns] (レポート列)

- ステータス
- リージョン

- エンドポイント ARN
- モデルの ARN
- KMS KeyId
- 最終更新日時

Amazon DocumentDB シングル AZ クラスター

説明

シングル AZ として設定されている Amazon DocumentDB クラスターがあるかどうかを確認します。

きわめて重要なワークロードでは、Amazon DocumentDB ワークロードをシングル AZ アーキテクチャで実行するだけでは不十分であり、コンポーネントの障害から回復するまでに最大 10 分かかることがあります。お客様は、メンテナンス、インスタンス障害、コンポーネント障害、アベイラビリティーゾーン障害が発生した場合の可用性を確保するため、追加のアベイラビリティーゾーンにレプリカインスタンスをデプロイする必要があります。

> **Note**
>
> > **Note**
> >
> > このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> > 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のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

チェック ID

c15vnddn2x

アラート条件

黄色: Amazon DocumentDB クラスターのインスタンスが 3 つ以下のアベイラビリティーゾーンにあります。

緑: Amazon DocumentDB クラスターのインスタンスが 3 つのアベイラビリティーゾーンにあります。

[Recommended Action] (推奨されるアクション)

アプリケーションに高可用性が必要な場合は、レプリカインスタンスを使用して DB インスタンスを変更し、マルチ AZ を有効にします。「Amazon DocumentDB High Availability and Replication」を参照してください。

その他のリソース

Understanding Amazon DocumentDB Cluster Fault Tolerance

リージョンとアベイラビリティーゾーン

[Report columns] (レポート列)

- ステータス
- リージョン
- アベイラビリティーゾーン
- DB クラスター識別子
- DB クラスターの ARN
- 最終更新日時

Amazon DynamoDB のポイントインタイムリカバリ

説明

ポイントインタイムリカバリが Amazon DynamoDB テーブルに対して有効になっているかどうかを確認します。

ポイントインタイムリカバリを使用することで、偶発的な書き込みや削除のオペレーションからDynamoDB テーブルを保護できます。ポイントインタイムリカバリを有効化すれば、オンデマンドバックアップの作成、維持、スケジュールを心配する必要はありません。ポイントインタイムリカバリによって、過去 35 日間の任意の時点にテーブルを復元することができます。DynamoDB では、テーブルの増分バックアップが維持されます。

詳細については、「DynamoDB のポイントインタイムリカバリ」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz138`

ソース

`AWS Config Managed Rule: dynamodb-pitr-enabled`

アラート条件

黄: ポイントインタイムリカバリが Amazon DynamoDB テーブルに対して有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon DynamoDB でポイントインタイムリカバリを有効にすると、テーブルデータを継続的にバックアップできます。

詳細については、「ポイントインタイムリカバリ: 仕組み」を参照してください。

その他のリソース

DynamoDB のポイントインタイムリカバリ

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon DynamoDB テーブルは Backup プランに含まれていない

説明

Amazon DynamoDB テーブルが AWS Backup プランの一部かどうかを確認します。

AWS Backup は、前回のバックアップ以降に行われた変更をキャプチャする DynamoDB テーブルの増分バックアップを提供します。 AWS Backup プランに DynamoDB テーブルを含めると、偶発的なデータ損失シナリオからデータを保護し、バックアッププロセスを自動化できます。これにより、DynamoDB テーブルの信頼性が高くスケーラブルなバックアップソリューションが提供され、貴重なデータを保護し、必要に応じて復旧できるようになります。

詳細については、「 を使用した DynamoDB テーブルのバックアップの作成 AWS Backup」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz107
```

ソース

```
AWS Config Managed Rule: dynamodb-in-backup-plan
```

アラート条件

黄: Amazon DynamoDB テーブルは AWS Backup プランに含まれていません。

[Recommended Action] (推奨されるアクション)

Amazon DynamoDB テーブルが AWS Backup プランの一部であることを確認します。

その他のリソース

スケジュールバックアップ

とは AWS Backup

AWS Backup コンソールを使用したバックアッププランの作成

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EBS は AWS Backup プランに含まれていません

説明

Amazon EBS ボリュームがバックアッププランに存在するかどうかを確認します AWS Backup。

Amazon EBS ボリュームを AWS Backup プランに含めて、それらのボリュームに保存されているデータの定期的なバックアップを自動化します。これにより、データ損失を防ぎ、データ管理が容易になり、必要に応じてデータを復元できるようになります。バックアップ計画は、データを安全に保ち、アプリケーションとサービスの目標復旧時間と目標復旧時点 (RTO/RPO) を達成できるようにするのに役立ちます。

詳細については、「バックアッププランの作成」を参照してください

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz106`

ソース

AWS Config Managed Rule: ebs-in-backup-plan

アラート条件

黄: Amazon EBS ボリュームは AWS Backup プランに含まれていません。

[Recommended Action] (推奨されるアクション)

Amazon EBS ボリュームが AWS Backup プランの一部であることを確認します。

その他のリソース

AWS Backup コンソールを使用したバックアッププランの作成

とは AWS Backup

開始方法 3: スケジュールされたバックアップの作成

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EBS スナップショット

説明

Amazon EBS ボリューム (使用可能または使用中) のスナップショットの経過時間を確認します。Amazon EBS ボリュームがレプリケートされた場合でも、障害が発生する可能性があります。スナップショットは、耐久性のあるストレージとpoint-in-timeリカバリのために toAmazon S3 に保持されます。

チェック ID

H7IgTzjTYb

アラート条件

- 黄: 最新のボリュームスナップショットは 7 ~ 30 日前に作成されました。

- 赤: 最新のボリュームスナップショットが作成されてから 30 日を超える期間が経過しています。
- 赤: ボリュームにはスナップショットがありません。

[Recommended Action] (推奨されるアクション)

ボリュームの週次または月次のスナップショットを作成します。詳細については、「Amazon EBS スナップショットの作成」を参照してください。

EBS スナップショットの作成を自動化するには、 AWS Backupまたは Amazon Data Lifecycle Manager の使用を検討してください。

その他のリソース

Amazon Elastic Block Store (Amazon EBS)

Amazon EBS スナップショット

AWS Backup

Amazon Data Lifecycle Manager

[Report columns] (レポート列)

- ステータス
- リージョン
- ボリューム ID
- ボリューム名
- スナップショット ID
- スナップショット名
- スナップショット作成後に経過した期間
- ボリュームのアタッチ
- 理由

Amazon EC2 Auto Scaling では ELB ヘルスチェックが有効になっていない

説明

Classic Load Balancer に関連付けられた Amazon EC2 Auto Scaling グループで、Elastic Load Balancing のヘルスチェックが使用されているかどうかを確認します。Auto Scaling グループのデフォルトのヘルスチェックは Amazon EC2 ステータスチェックのみです。インスタンスがこ

れらのステータスチェックに合格しない場合、異常とマークされて終了します。Amazon EC2 Auto Scaling が新しい代替インスタンスを起動します。Elastic Load Balancing ヘルスチェックは、Amazon EC2 インスタンスを定期的に監視して異常のあるインスタンスを検出して終了し、新しいインスタンスを起動します。

詳細については、Elastic Load Balancing ヘルスチェックを追加する」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz104`

ソース

`AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required`

アラート条件

黄: Amazon EC2 Auto Scaling グループにアタッチされた Classic Load Balancer は Elastic Load Balancing ヘルスチェックは有効になっていません。

[Recommended Action] (推奨されるアクション)

Classic Load Balancer に関連付けられた Auto Scaling グループで、Elastic Load Balancing のヘルスチェックが使用されているかどうかを確認します。

Elastic Load Balancing ヘルスチェックは、ロードバランサーが正常でリクエストを処理できるかどうかをレポートします。これにより、アプリケーションの高可用性が保証されます。

詳細については、「Auto Scaling グループに Elastic Load Balancing ヘルスチェックを追加する」を参照してください

[Report columns] (レポート列)

- ステータス
- リージョン

- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EC2 Auto Scaling グループでキャパシティの再調整が有効

説明

複数のインスタンスタイプを使用する Amazon EC2 Auto Scaling グループで容量の再分散が有効かどうかを確認します。

Amazon EC2 Auto Scaling グループにキャパシティの再調整を設定すると、インスタンスタイプや購入オプションに関係なく、Amazon EC2 インスタンスがアベイラビリティーゾーン全体に均等に分散されるようになります。CPU 使用率やネットワークトラフィックなど、グループに関連付けられたターゲット追跡ポリシーを使用します。

詳細については、「複数のインスタンスタイプと購入オプションをもつ Auto Scaling グループ」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
AWS Config c18d2gz103
```

ソース

AWS Config マネージドルール: autoscaling-capacity-rebalancing

アラート条件

黄: Amazon EC2 Auto Scaling グループでキャパシティの再調整が有効ではありません。

[Recommended Action] (推奨されるアクション)

複数のインスタンスタイプを使用する Amazon EC2 Auto Scaling グループでキャパシティの再調整が有効かどうかを確認します。

詳細については、「キャパシティーの再調整の有効化 (コンソール)」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EC2 Auto Scaling が複数の AZ にデプロイされていないか、AZ の最小数に達していない

説明

Amazon EC2 Auto Scaling グループが複数のアベイラビリティーゾーンまたは指定された最小数のアベイラビリティーゾーンにデプロイされているかどうかを確認します。高可用性を確保するために、複数のアベイラビリティーゾーンに Amazon EC2 インスタンスをデプロイします。

AWS Config ルールの minAvailibilityZones パラメータを使用して、アベイラビリティーゾーンの最小数を調整できます。

詳細については、「複数のインスタンスタイプと購入オプションをもつ Auto Scaling グループ」を参照してください。

チェック ID

```
c18d2gz101
```

ソース

```
AWS Config Managed Rule: autoscaling-multiple-az
```

アラート条件

赤: Amazon EC2 Auto Scaling グループに設定された複数の AZ がないか、指定されている AZ の最小数を満たしていません。

[Recommended Action] (推奨されるアクション)

Amazon EC2 Auto Scaling グループが複数の AZ で構成されていることを確認してください。高可用性を確保するために、複数のアベイラビリティーゾーンに Amazon EC2 インスタンスをデプロイします。

その他のリソース

起動テンプレートを使用して Auto Scaling グループを作成する

起動設定を使用して Auto Scaling グループを作成する

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon EC2 アベイラビリティーゾーンのバランス

説明

リージョン内のアベイラビリティーゾーン間で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの分散をチェックします。

アベイラビリティーゾーンは、他のアベイラビリティーゾーンの障害から分離された別の場所です。そのため、同じリージョン内の複数のアベイラビリティーゾーン間の安価な低レイテンシーネットワーク接続が発生することがあります。同一のリージョン内の複数のアベイラビリティーゾーンでインスタンスを起動することにより、単一障害点からアプリケーションを保護することができます。

チェック ID

`wuy7G1zxql`

アラート条件

- 黄: リージョンは複数のゾーンにインスタンスを有していますが、分散が不均一です (使用中のアベイラビリティーゾーンにおける最大インスタンス数と最小インスタンス数の差が 20% を超えています)。

- 赤: リージョンは、1 つのアベイラビリティーゾーンにのみインスタンスを有しています。

[Recommended Action] (推奨されるアクション)

複数のアベイラビリティーゾーンで Amazon EC2 インスタンスを均等にバランスよく配置します。これを実行するには、インスタンスを手動で起動するか、Auto Scaling を使用して自動的に実行します。詳細については、「インスタンスの起動」および「Load Balance Your Auto Scaling Group」(Auto Scaling グループの負荷分散) を参照してください。

その他のリソース

- Amazon EC2 Auto Scaling ユーザーガイド
- Amazon EC2 インスタンスのプレイスメントグループ
- Amazon EC2 インスタンスタイプ

[Report columns] (レポート列)

- ステータス
- リージョン
- ゾーン a インスタンス
- ゾーン b インスタンス
- ゾーン c インスタンス
- ゾーン e インスタンス
- ゾーン f インスタンス
- 理由

Amazon EC2 詳細モニタリングが有効化されていません

説明

詳細モニタリングが Amazon EC2 インスタンスに対して有効になっているかどうかを確認します。

Amazon EC2 詳細モニターリングでは、Amazon EC2 の基本モニターリングで使用される 5 分間隔ではなく、高い頻度の 1 分間隔で公開されるメトリクスが用意されています。Amazon EC2 の詳細なモニターリングを有効にすると、Amazon EC2 リソースをより適切に管理できるため、傾向を見つけてアクションを迅速に行うことができます。

詳細については、「基本モニタリングと詳細モニタリング」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`AWS Config c18d2gz144`

ソース

AWS Config マネージドルール: ec2-instance-detailed-monitoring-enabled

アラート条件

黄:Amazon EC2 インスタンスの詳細モニタリングが有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon EC2 インスタンスの詳細モニタリングを有効にして、Amazon EC2 メトリクスデータが Amazon CloudWatch に公開される頻度を増やします (5 分間隔から 1 分間隔に)。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

ブロックモードの Amazon ECS AWS Logs ドライバー

説明

Logs ログドライバーがブロックモードで設定されている Amazon ECS AWSタスク定義をチェックします。ブロッキングモードでドライバーが設定されると、システムの可用性が危険にさらされます。

> **Note**
>
> > **Note**
> >
> > このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> > ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dvkm4z6b`

アラート条件

黄色: awslogs ドライバーのログ記録設定のモードパラメータが「ブロッキング」または「ありません」に設定されています。モードパラメータがないということは、デフォルトのブロッキング設定になっているということです。

緑: Amazon ECS タスク定義で awslogs ドライバーが使用されていないか、awslogs ドライバーがノンブロッキングモードに設定されています。

[Recommended Action] (推奨されるアクション)

可用性のリスクを軽減するには、タスク定義 AWSの Logs ドライバー設定をブロックから非ブロックに変更することを検討してください。ノンブロッキングモードでは、max-buffer-size パラメータの値を設定する必要があります。設定パラメータの詳細およびガイダンスについては、「」を参照してください。Logs コンテナログドライバーの「ノンブロッキングモードで AWSのログ損失の防止」を参照してください。

その他のリソース

AWS logs ログドライバーを使用する

バックプレッシャーを回避するためのコンテナのログ記録オプションを選択する

AWS Logs コンテナログドライバーでのノンブロッキングモードでのログ損失の防止

[Report columns] (レポート列)

- ステータス

- リージョン
- タスク定義 ARN
- コンテナ定義の名前
- 最終更新日時

単一の AZ を使用した Amazon ECS サービス

説明

サービス設定で単一のアベイラビリティーゾーン (AZ) を使用していることをチェックします。

AZ は、他のゾーンの障害から隔離された独立した場所です。そのため、同じ AWS リージョンのアベイラビリティーゾーン間では、安価で低レイテンシーのネットワーク接続がサポートされています。同一のリージョン内の複数のアベイラビリティーゾーンでインスタンスを起動することにより、単一障害点からアプリケーションを保護できます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1z7dfpz01`

アラート条件

- 黄色: Amazon ECS サービスはすべてのタスクを単一の AZ で実行しています。
- 緑: Amazon ECS サービスは少なくとも 2 つの異なる AZ でタスクを実行しています。

[Recommended Action] (推奨されるアクション)

異なるアベイラビリティーゾーンでサービスに対して 1 つ以上のタスクを追加で作成します。

その他のリソース

Amazon ECS のキャパシティとアベイラビリティ

[Report columns] (レポート列)

- ステータス
- リージョン
- ECS クラスター名/ECS サービス名
- アベイラビリティーゾーン数
- 最終更新日時

Amazon ECS マルチ AZ 配置戦略

説明

Amazon ECS サービスが、アベイラビリティーゾーン (AZ) に基づくスプレッド配置戦略を使用していることを確認します。この戦略は、同じ 内のアベイラビリティーゾーン間でタスクを分散 AWS リージョン し、単一の障害点からアプリケーションを保護するのに役立ちます。

Amazon ECS サービスの一部として実行されるタスクの場合、スプレッドはデフォルトのタスク配置戦略です。

このチェックでは、有効な配置戦略リストの最初の戦略または唯一の戦略がスプレッドであることも確認します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c1z7dfpz02
```

アラート条件

- 黄色: アベイラビリティゾーンによるスプレッドが無効になっているか、Amazon ECS サービスの有効な配置戦略リストの第一の戦略ではありません。

- 緑: アベイラビリティゾーンによるスプレッドが、有効な配置戦略リストの第一の戦略であるか、Amazon ECS サービスで有効になっている唯一の配置戦略です。

[Recommended Action] (推奨されるアクション)

タスクをスプレッド配置する戦略を有効にして、タスクを複数の AZ に分散します。アベイラビリティゾーンによるスプレッドが、有効なすべてのタスク配置戦略における第一の戦略であるか、唯一の使用されている戦略であることを確認します。AZ 配置を管理する場合は、別の AZ でミラーリングサービスを使用すると、これらのリスクを軽減できます。

その他のリソース

Amazon ECS タスク配置戦略

[Report columns] (レポート列)

- ステータス
- リージョン
- ECS クラスター名/ECS サービス名
- スプレッドタスク配置戦略が有効化され、正しく適用されている
- 最終更新日時

Amazon EFS マウントターゲット冗長性なし

説明

Amazon EFS ファイルシステムの複数のアベイラビリティーゾーンにマウントターゲットが存在するかどうかを確認します。

アベイラビリティーゾーンは、他のゾーンの障害から隔離された独立した場所です。AWS リージョン内の複数の地理的に分離されたアベイラビリティーゾーンにマウントターゲットを作成することで、Amazon EFS ファイルシステムに最高レベルの可用性と耐久性を実現します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

c1dfprch01

アラート条件

- 黄:ファイルシステムには、単一のアベイラビリティーゾーンで作成された 1 つのマウントターゲットがあります。

  緑:ファイルシステムには、複数のアベイラビリティーゾーンで作成された 2 つ以上のマウントターゲットがあります。

[Recommended Action] (推奨されるアクション)

1 ゾーンストレージクラスを使用する EFS ファイルシステムの場合は、バックアップを新しいファイルシステムに復元して、スタンダードストレージクラスを使用する新しいファイルシステムを作成することをお勧めします。次に、複数のアベイラビリティーゾーンにマウントターゲットを作成します。

スタンダードストレージクラスを使用する EFS ファイルシステムの場合は、複数のアベイラビリティーゾーンにマウントターゲットを作成することをお勧めします。

その他のリソース

- Amazon EFS コンソールを使用したマウントターゲットの管理
- Amazon EFS のクォータと制限

[Report columns] (レポート列)

- ステータス
- リージョン
- EFS ファイルシステム ID
- マウントターゲットの数
- AZ の数
- 最終更新日時

Amazon EFS が AWS Backup プランに含まれていない

説明

Amazon EFS ファイルシステムがバックアッププランに含まれているかどうかを確認します AWS Backup。

AWS Backup は、バックアップの作成、移行、復元、削除を簡素化し、レポートと監査を改善するように設計された統合バックアップサービスです。

詳細については、「Amazon EFS ファイルシステムのバックアップ」を参照してください。

チェック ID

```
c18d2gz117
```

ソース

```
AWS Config Managed Rule: EFS_IN_BACKUP_PLAN
```

アラート条件

赤: Amazon EFS は AWS Backup プランに含まれていません。

[Recommended Action] (推奨されるアクション)

偶発的なデータ損失やデータ破損を防ぐために、Amazon EFS ファイルシステムが AWS Backup プランに含まれていることを確認してください。

その他のリソース

Amazon EFS ファイルシステムのバックアップ

を使用した Amazon EFS のバックアップと復元 AWS Backup。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon ElastiCache マルチ AZ クラスター

説明

単一のアベイラビリティーゾーン (AZ) にデプロイされた ElastiCache クラスターをチェックします。このチェックでは、クラスター内でマルチ AZ が非アクティブである場合に警告が表示されます。

複数の AZ にデプロイすると、異なる AZ の読み取り専用レプリカに非同期でレプリケートされるため、ElastiCache クラスターの可用性が向上します。クラスターの計画的なメンテナンスが行われるか、プライマリノードが使用できない場合、ElastiCache は自動的にレプリカをプライマリに昇格させます。このフェイルオーバーにより、クラスターの書き込み操作を再開でき、管理者が介入する必要はありません。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

ECHdfsQ402

アラート条件

- 緑色: マルチ AZ はクラスター内でアクティブです。
- 黄色: マルチ AZ はクラスター内で非アクティブです。

[Recommended Action] (推奨されるアクション)

プライマリとは異なる AZ に、シャードごとに少なくとも 1 つのレプリカを作成します。

その他のリソース

詳細については、「マルチ AZ による ElastiCache (Redis OSS) のダウンタイムの最小化」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター名
- 最終更新日時

ElastiCache (Redis OSS) クラスターの自動バックアップ

説明

Amazon ElastiCache (Redis OSS) クラスターで自動バックアップが有効になっているかどうか、およびスナップショットの保持期間が指定された制限または 15 日間のデフォルト制限を超えているかどうかを確認します。自動バックアップを有効にすると、ElastiCache はクラスターのバックアップを毎日作成します。

AWS Config ルールの snapshotRetentionPeriod パラメータを使用して、必要なスナップショット保持制限を指定できます。

詳細については、ElastiCache (Redis OSS) のバックアップと復元」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz178`

ソース

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

アラート条件

赤: Amazon ElastiCache (Redis OSS) クラスターで自動バックアップが有効になっていないか、スナップショットの保持期間が制限を下回っています。

[Recommended Action] (推奨されるアクション)

Amazon ElastiCache (Redis OSS) クラスターで自動バックアップが有効になっていて、スナップショットの保持期間が指定された制限または 15 日間のデフォルト制限を超えていることを確認してください。自動バックアップは、データ損失を防ぐのに役立ちます。障害が起こった場合、最新のバックアップからデータを復元して新しいクラスターを作成できます。

詳細については、ElastiCache (Redis OSS) のバックアップと復元」を参照してください。

その他のリソース

詳細については、「自動バックアップのスケジュール」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター名
- 最終更新日時

Amazon MemoryDB マルチ AZ クラスター

説明

単一のアベイラビリティーゾーン (AZ) にデプロイされた MemoryDB クラスターをチェックします。このチェックでは、クラスター内でマルチ AZ が非アクティブである場合に警告が表示されます。

複数の AZ にデプロイすると、異なる AZ の読み取り専用レプリカに非同期でレプリケートされるため、MemoryDB クラスターの可用性が向上します。クラスターの計画的なメンテナンスが行われるか、プライマリノードが使用できない場合、MemoryDB はレプリカを自動的にプライマリノードに昇格します。このフェイルオーバーにより、クラスターの書き込み操作を再開でき、管理者が介入する必要はありません。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
MDBdfsQ401
```

アラート条件

- 緑色: マルチ AZ はクラスター内でアクティブです。
- 黄色: マルチ AZ はクラスター内で非アクティブです。

[Recommended Action] (推奨されるアクション)

プライマリとは異なる AZ に、シャードごとに少なくとも 1 つのレプリカを作成します。

その他のリソース

詳細については、「Minimizing downtime in MemoryDB with Multi-AZ」(マルチ AZ を使用した MemoryDB でのダウンタイムの最小化) を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター名
- 最終更新日時

Amazon MSK ブローカーがホストするパーティションの数が多すぎる

説明

Managed Streaming for Kafka (MSK) クラスターのブローカーに、割り当てられているパーティションの数が推奨数を超えていないことを確認します。

チェック ID

`Cmsvnj8vf1`

アラート条件

- 赤: MSK ブローカーが推奨最大パーティション制限の 100% に達したか、超えています
- 黄: MSK が推奨最大パーティション制限の 80% に達しました

[Recommended Action] (推奨されるアクション)

MSK の推奨ベストプラクティスに従って MSK クラスターを拡張するか、未使用のパーティションをすべて削除してください。

その他のリソース

- クラスターを適切なサイズにする

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター ARN
- ブローカー ID
- パーティション数

Amazon MSK クラスターマルチ AZ

説明

Amazon MSK でプロビジョニングされたクラスターのアベイラビリティーゾーン (AZs) の数を確認します。Amazon MSK クラスターは、連携してデータとロードを分散する複数のブローカーで構成されています。2-AZ クラスターのメンテナンス中またはブローカーの問題により、本稼働が中断される場合があります。

チェック ID

`90046ff5b5`

アラート条件

- 黄: Amazon MSK クラスターは 2 つの AZs
- 緑: Amazon MSK クラスターは 3 つ以上の AZs

[Recommended Action] (推奨されるアクション)

クラスターの可用性を高めるには、3 つの AZs 設定で別のクラスターを作成します。次に、既存のクラスターを、作成した新しいクラスターに移行します。この移行には Amazon MSK レプリケーションを使用できます。

その他のリソース

Amazon MSK の高可用性

Amazon MSK の移行

[Report columns] (レポート列)

- ステータス
- リージョン

- MSK クラスター ARN
- AZ の数
- 最終更新日時

データノードが 3 つ未満の Amazon OpenSearch Service ドメイン

説明

Amazon OpenSearch Service のドメインが少なくとも 3 つのデータノードで構成され、ZoneAwarenessEnabled が true であるかどうかをチェックします。ZoneAwarenessEnabled を有効にすると、Amazon OpenSearch Service は各プライマリシャードとそれに対応するレプリカがそれぞれ異なるアベイラビリティーゾーンに割り当てられるようにします。

詳細については、「Amazon OpenSearch Service でのマルチ AZ ドメインの設定」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz183
```

ソース

```
AWS Config Managed Rule: opensearch-data-node-fault-tolerance
```

アラート条件

黄: Amazon OpenSearch Service ドメインは、3 つ未満のデータノードで構成されています。

[Recommended Action] (推奨されるアクション)

Amazon OpenSearch Service ドメインが少なくとも 3 つのデータノードで構成されていることを確認してください。マルチ AZ ドメインを設定して Amazon OpenSearch Service クラスター

の可用性を高めるには、同じリージョン内の 3 つのアベイラビリティーゾーンにノードを割り当て、データを複製します。これにより、データ損失が防止され、ノードまたはデータセンター (AZ) に障害が発生した場合のダウンタイムが最小限に抑えられます。

詳細については、「Increase availability for Amazon OpenSearch Service by deploying in three Availability Zones」を参照してください。

その他のリソース

- Increase availability for Amazon OpenSearch Service by deploying in three Availability Zones

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon RDS バックアップ

説明

Amazon RDS DB インスタンスの自動バックアップをチェックします。

デフォルトでは、バックアップは 1 日の保持期間で有効になっています。バックアップは、予期しないデータ損失のリスクを軽減し、ポイントインタイムリカバリを可能にします。

チェック ID

opQPADkZvH

アラート条件

赤: DB インスタンスのバックアップ保持期間は 0 日に設定されています。

[Recommended Action] (推奨されるアクション)

アプリケーションの要件に応じて、自動 DB インスタンスのバックアップの保持期間を 1～35 日に設定します。「Working With Automated Backups」(自動バックアップの使用) を参照してください。

その他のリソース

Amazon RDS の開始方法

[Report columns] (レポート列)

- ステータス
- リージョン/AZ
- DB インスタンス
- VPC ID
- バックアップの保持期間

Amazon RDS 継続的バックアップが有効になっていない

説明

Amazon RDS インスタンスが Amazon RDS を使用した自動バックアップまたは の継続的バックアップで有効になっているかどうかを確認します AWS Backup。継続的なバックアップにより、予期しないデータ損失のリスクが軽減され、point-in-timeリカバリが可能になります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`44fde09ab5`

アラート条件

- 赤: Amazon RDS で自動バックアップが有効になっていないか、 で継続的バックアップが有効になっていません AWS Backup。
- 赤: 5.6 より前のバージョンの MySQL は、自動バックアップまたは継続的バックアップをサポートしていません。回復力を提供するには、まずデータベースバージョンをアップグレードしてから、自動バックアップまたは継続的バックアップを有効にします。

- 緑: Amazon RDS でインスタンスの自動バックアップが有効になっています。
- 緑: インスタンスで継続的バックアップが有効になっています AWS Backup。

[Recommended Action] (推奨されるアクション)

Amazon RDS インスタンスに自動バックアップが設定されていることを確認するには、Amazon RDS で保持期間を 0 より長く設定するか、 を使用して継続的なバックアッププランを作成します AWS Backup。

その他のリソース

- Amazon RDS の開始方法
- 自動バックアップの管理
- バックアップの概要
- 継続的バックアップとpoint-in-time復元 (PITR)
- AWS Backup 機能の可用性

[Report columns] (レポート列)

- ステータス
- リージョン
- DB Instance Identifier
- DB インスタンス ARN
- デプロイタイプ
- バックアップタイプ
- 理由
- 最終更新日時

Amazon RDS DB クラスターには 1 つの DB インスタンスがあります。

説明

DB クラスターに少なくともももうひとつの DB インスタンスを追加し、可用性とパフォーマンスを向上させます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt011`

アラート条件

黄色: DB クラスターには DB インスタンスが 1 つしかありません。

[Recommended Action] (推奨されるアクション)

リーダー DB インスタンスを DB クラスターに追加します。

その他のリソース

現在の設定では、読み取りオペレーションと書き込みオペレーションの両方で、1 つの DB インスタンスが使用されています。別の DB インスタンスを追加して、読み取りの再配分とフェイルオーバーオプションを有効にすることができます。

アベイラビリティーゾーンの詳細については、「Amazon Aurora の高可用性」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン

- リソース
- エンジン名
- DB インスタンスクラス
- 最終更新日時

すべてのインスタンスが同じアベイラビリティーゾーンにある Amazon RDS DB クラスター

説明

DB クラスターは現在、1 つのアベイラビリティーゾーンにあります。複数のアベイラビリティーゾーンを使用してアベイラビリティーを向上させます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

```
c1qf5bt007
```

アラート条件

黄色: DB クラスターでは、すべてのインスタンスが同じアベイラビリティーゾーンにあります。

[Recommended Action] (推奨されるアクション)

DB クラスター内の複数のアベイラビリティーゾーンに DB インスタンスを追加します。

その他のリソース

DB インスタンスは、DB クラスター内の複数のアベイラビリティーゾーンに追加することをお勧めします。DB インスタンスを複数のアベイラビリティーゾーンに追加すると、DB クラスターの可用性が向上します。

アベイラビリティーゾーンの詳細については、「Amazon Aurora の高可用性」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- 最終更新日時

すべてのリーダーインスタンスが同じアベイラビリティゾーンにある Amazon RDS DB クラスター

説明

DB クラスターでは、すべてのリーダーインスタンスが同じアベイラビリティーゾーンにあります。リーダーインスタンスを DB クラスタ内の複数のアベイラビリティーゾーンに分散することをお勧めします。

分散によってデータベースの可用性が向上し、クライアントとデータベース間のネットワーク遅延が減少して応答時間が改善されます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt018`

アラート条件

赤: DB クラスターでは、リーダーインスタンスが同じアベイラビリティーゾーンにあります。

[Recommended Action] (推奨されるアクション)

リーダーインスタンスを複数のアベイラビリティーゾーンに分散します。

その他のリソース

アベイラビリティーゾーン (AZs) は、各 AWS リージョン内で停止した場合に分離できるように、互いに異なる場所です。DB クラスターのプライマリインスタンスとリーダーインスタンスを複数の AZ に配信して、DB クラスターの可用性を改善することをお勧めします。マルチ AZ クラスターは AWS Management Console、クラスターの作成時に、 AWS CLI、、または Amazon RDS API を使用して作成できます。また、既存の Aurora クラスターをマルチ AZ クラスターに変更するには、新しいリーダーインスタンスを追加し、別の AZ を指定します。

アベイラビリティーゾーンの詳細については、「Amazon Aurora の高可用性」を参照してください。

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- エンジン名
- 最終更新日時

Amazon RDS DB インスタンス拡張モニタリングが有効化されていない

説明

Amazon RDS DB インスタンスで拡張モニタリングが有効になっているかどうかをチェックします。

Amazon RDS の拡張モニタリングは、DB インスタンスが実行されるオペレーティングシステム (OS) のメトリクスをリアルタイムで提供します。Amazon RDS DB インスタンスのすべてのシステムメトリクスとプロセス情報を Amazon RDS コンソールに表示できます。また、ダッシュボードはカスタマイズできます。拡張モニタリングでは、Amazon RDS インスタンスの運用状況をほぼリアルタイムで把握できるため、運用上の問題に迅速に対応できます。

AWS Config ルールの monitoringInterval パラメータを使用して、必要なモニタリング間隔を指定できます。

詳細については、「Enhanced Monitoring の概要」と「拡張モニタリングの OS メトリクス」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz158
```

ソース

```
AWS Config Managed Rule: rds-enhanced-monitoring-enabled
```

アラート条件

黄: Amazon RDS DB インスタンスで拡張モニタリングが有効になっていないか、必要な間隔に設定されていません。

[Recommended Action] (推奨されるアクション)

Amazon RDS DB インスタンスの拡張モニタリングを有効にすると、Amazon RDS インスタンスのオペレーションステータスの可視性が向上します。

詳細については、「拡張モニタリングを使用した OS メトリクスのモニタリング」を参照してください。

その他のリソース

拡張モニタリングの OS メトリクス

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon RDS DB インスタンスのストレージの自動スケーリングが無効になっています

説明

Amazon RDS DB インスタンスのストレージ自動スケーリングが有効になっていません。データベースのワークロードが増加した場合、RDSストレージの自動スケーリングにより、ダウンタイムなしでストレージ容量が自動的に拡張されます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt013`

アラート条件

赤: DB インスタンスのストレージの自動スケーリングが有効になっていません。

[Recommended Action] (推奨されるアクション)

指定した最大ストレージしきい値で Amazon RDS ストレージ自動スケーリングを有効にします。

その他のリソース

Amazon RDS ストレージの自動スケーリングは、データベースのワークロードが増加したときに、ダウンタイムなしでストレージ容量を自動的に拡張します。ストレージ自動スケーリングはストレージの使用状況をモニタリングし、使用量がプロビジョニングされたストレージ容量に近づくと自動的に容量をスケールアップします。Amazon RDS が DB インスタンスに割り当てるストレージの上限を指定することができます。ストレージの自動スケーリングに追加料金はかかりません。DB インスタンスに割り当てられた Amazon RDS リソースに対してのみ料金が発生します。Amazon RDS ストレージの自動スケーリングを有効にすることをお勧めします。

詳細については、「Amazon RDS ストレージのオートスケーリングによる容量の自動管理 」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS DB インスタンスがマルチ AZ 配置を使用していない

説明

マルチ AZ 配置を使用することをお勧めします。マルチ AZ 配置により、DB インスタンスの可用性と耐久性が向上します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt019`

アラート条件

黄色: DB インスタンスはマルチ AZ 配置を使用していません。

[Recommended Action] (推奨されるアクション)

影響を受ける DB インスタンスにマルチ AZ を設定します。

その他のリソース

Amazon RDS マルチ AZ 配置では、Amazon RDS は自動的にプライマリデータベースインスタンスを作成し、異なるアベイラビリティゾーンのインスタンスにデータをレプリケートします。障害を検出すると、Amazon RDS は手動操作なしで自動的にスタンバイインスタンスにフェイルオーバーします。

詳細については、「料金」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- エンジン名
- 最終更新日時

Amazon RDS DiskQueueDepth

説明

RDS インスタンスのデータベースストレージへのキューに入っている書き込みの数が、運用上の調査が必要となるレベルまで増加したことを、CloudWatch メトリクス DiskQueueDepth が示しているかどうかを確認します。

チェック ID

`Cmsvnj8db3`

アラート条件

- 赤: DiskQueueDepth CloudWatch メトリクスが 10 を超えました

- 黄: DiskQueueDepth CloudWatch メトリクスが 5 より大きくかつ 10 以下
- 緑: DiskQueueDepth CloudWatch メトリクスが 5 以下

[Recommended Action] (推奨されるアクション)

読み取り/書き込み特性をサポートするインスタンスとストレージボリュームへの移行を検討してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- DB インスタンス ARN
- DiskQueueDepth メトリクス

Amazon RDS FreeStorageSpace

説明

RDS データベースインスタンスの FreeStorageSpace CloudWatch メトリクスが、運用上合理的なしきい値を下回ったかどうかを確認します。

チェック ID

`Cmsvnj8db2`

アラート条件

- 赤: FreeStorageSpace の合計容量の 10% 未満
- 黄: FreeStorageSpace は総容量の 10% ~ 20% です
- 緑: FreeStorageSpace は総容量の 20% を超えています

[Recommended Action] (推奨されるアクション)

Amazon RDS マネジメントコンソール、Amazon RDS API、または AWS コマンドラインインターフェイスを使用して、空きストレージが少なくなっている RDS データベースインスタンスのストレージスペースをスケールアップします。

[Report columns] (レポート列)

- ステータス
- リージョン
- DB インスタンス ARN

- FreeStorageSpace メトリクス (MB)
- DB インスタンス割り当てストレージ (MB)
- DB インスタンスストレージ使用率

Amazon RDS の口グ出力パラメータはテーブルに設定されます。

説明

log_output を TABLE に設定すると、log_output が FILE に設定されている場合よりも多くのストレージが使用されます。ストレージサイズの制限に達しないように、パラメーターを FILE に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> 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のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt023`

アラート条件

黄色: DB パラメータグループの log_output パラメータは TABLE に設定されています。

[Recommended Action] (推奨されるアクション)

DB パラメータグループの log_output パラメータ値を FILE に設定します。

その他のリソース

詳細については、「MySQL データベースログファイル」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS の innodb_default_row_format パラメータ設定は安全ではない

説明

DB インスタンスで既知の問題が発生しました: MySQL バージョン 8.0.26 よりも前のバージョンで、row_format を COMPACT または REDUNDANT に設定して作成されたテーブルは、インデックスが 767 バイトを超えるとアクセスできなくなり、回復できなくなります。

innodb_default_row_format パラメータ値を DYNAMIC に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用でき

ません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt036`

アラート条件

赤: DB パラメータグループの innodb_default_row_format パラメータの設定が安全ではありません。

[Recommended Action] (推奨されるアクション)

innodb_default_row_format パラメータを DYNAMIC に設定してください。

その他のリソース

MySQL バージョン 8.0.26 より前のバージョンで row_format を COMPACT または REDUNDANT に設定してテーブルを作成した場合、key prefix が 767 バイトより短いインデックスの作成は強制されません。データベースが再起動すると、これらのテーブルにアクセスしたり、それを復元したりすることはできません。

詳細については、MySQL ドキュメントウェブサイトの「MySQL 8.0.26 での変更点 (2021 年 7 月 20 日、一般提供開始)」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS innodb_flush_log_at_trx_commit パラメータが 1 ではありません

説明

DB インスタンスの innodb_flush_log_at_trx_commit パラメータの値は安全ではありません。このパラメータは、ディスクへのコミット操作の持続性を制御します。

innodb_flush_log_at_trx_commit パラメータを 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt030`

アラート条件

黄: DB パラメータグループの innodb_flush_log_at_trx_commit が 1 以外に設定されている。

[Recommended Action] (推奨されるアクション)

innodb_flush_log_at_trx_commit パラメータの値を 1 に設定します

その他のリソース

ログバッファが耐久ストレージに保存されると、データベーストランザクションは耐久性を持ちます。ただし、ディスクに保存するとパフォーマンスに影響します。innodb_flush_log_at_trx_commit パラメータに設定されている値によって、ログがディスクに書き込まれて保存される方法の動作が異なる場合があります。

- パラメータ値が 1 の場合、トランザクションがコミットされるたびにログがディスクに書き込まれ、保存されます。
- パラメータ値が 0 の場合、ログは 1 秒に 1 回ディスクに書き込まれて保存されます。
- パラメータ値が 2 の場合、ログはトランザクションがコミットされるたびに書き込まれ、1 秒に 1 回ディスクに保存されます。データは InnoDB メモリバッファから、同じくメモリ内にあるオペレーティングシステムのキャッシュに移動します。

> **Note**
>
> パラメータ値が 1 でない場合、InnoDB は ACID プロパティを保証しません。データベースがクラッシュすると、最後の 1 秒間の最近のトランザクションが失われる可能性があります。

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 1: Parameters related to performance」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS max_user_connections パラメータが低くなっています

説明

DB インスタンスは、各データベースアカウントの最大同時接続数の値が低くなっています。

max_user_connections パラメータを 5 より大きい数に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt034`

アラート条件

黄色: DB パラメータグループの max_user_connections の設定に誤りがあります。

[Recommended Action] (推奨されるアクション)

max_user_connections パラメータの値を 5 より大きい数にします。

その他のリソース

max_user_connections 設定は、MySQL ユーザーアカウントに許可される同時接続の最大数を制御します。この接続制限に達すると、バックアップ、パッチ、パラメータ変更などの Amazon RDS インスタンスの管理操作に障害が発生します。

詳細については、MySQL ドキュメント Web サイトの「アカウントリソース制限の設定」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS Multi-AZ

説明

単一のアベイラビリティーゾーン (AZ) にデプロイされた DB インスタンスをチェックします。

マルチ AZ 配置は、別のアベイラビリティーゾーン内のスタンバイインスタンスに同期的にレプリケートすることによってデータベースの可用性を向上させます。予定されたデータベースメンテナンスや、DB インスタンスまたはアベイラビリティーゾーンで障害が発生した際、Amazon RDS は自動的にスタンバイインスタンスにフェイルオーバーします。このフェイルオーバーにより、管理者の介入を必要とせずにデータベースオペレーションを迅速に再開できます。Amazon RDS は Microsoft SQL Server のマルチ AZ 配置をサポートしていないため、このチェックでは SQL Server インスタンスは調査されません。

チェック ID

`f2iK5R6Dep`

アラート条件

黄: DB インスタンスが 1 つのアベイラビリティーゾーンにデプロイされています。

[Recommended Action] (推奨されるアクション)

アプリケーションで高可用性が必要な場合は、DB インスタンスを変更してマルチ AZ 配置を有効にします。「高可用性 (マルチ AZ)」を参照してください。

その他のリソース

リージョンとアベイラビリティーゾーン

[Report columns] (レポート列)

- ステータス

- リージョン/AZ
- DB インスタンス
- VPC ID
- マルチ AZ

Amazon RDS が AWS Backup プランに含まれていない

説明

Amazon RDS DB インスタンスが AWS Backupのバックアッププランに含まれているかどうかを確認します。

AWS Backup はフルマネージド型のバックアップサービスであり、 AWS サービス間でデータのバックアップを簡単に一元化および自動化できます。

Amazon RDS DB インスタンスをバックアッププランに含めることは、規制遵守義務、ディザスタリカバリ、データ保護に関するビジネスポリシー、事業継続目標にとって重要です。

詳細については、「AWS Backup とは?」を参照してください。

> **Note**
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz159
```

ソース

```
AWS Config Managed Rule: rds-in-backup-plan
```

アラート条件

黄: Amazon RDS DB インスタンスは、 のバックアッププランに含まれていません AWS Backup。

[Recommended Action] (推奨されるアクション)

Amazon RDS DB インスタンスをバックアッププランに含めます AWS Backup。

詳細については「Amazon RDS Backup and Restore Using AWS Backup」を参照してください。

その他のリソース

バックアッププランへのリソースの割り当て

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon RDS リードレプリカは書き込み可能モードで開かれます。

説明

DB インスタンスには書き込み可能モードのリードレプリカがあり、クライアントからの更新が可能です。

リードレプリカが書き込み可能モードにならないように、read_only パラメータを TrueIfReplica に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt035`

アラート条件

黄色: DB パラメータグループはリードレプリカの書き込み可能モードを有効にします。

[Recommended Action] (推奨されるアクション)

read_only パラメータ値を TrueIfReplica に設定します。

その他のリソース

read_only パラメータは、クライアントからデータベースインスタンスへの書き込みアクセス許可を制御します。このパラメータのデフォルト値は TrueIfReplica.です。レプリカインスタンスの場合、TrueIfReplica は read_only 値を ON (1) に設定し、クライアントからの書き込みアクティビティをすべて無効にします。マスター/ライターインスタンスの場合、TrueIReplica は値を OFF (0) に設定し、クライアントからのインスタンスへの書き込みアクティビティを有効にします。リードレプリカを書き込み可能モードで開いた場合、このインスタンスに格納されているデータがプライマリインスタンスと異なることがあり、これがレプリケーションエラーの原因となります。

詳細については、MySQL ドキュメントサイトの「Best practices for configuring parameters for Amazon RDS for MySQL, part 2: Parameters related to replication」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース

- パラメータ名
- 推奨値
- 最終更新日時

Amazon RDS リソースの自動バックアップは無効になっています。

説明

DB リソースの自動バックアップは無効になっています。自動バックアップでは、お客様の DB インスタンスのポイントインタイムリカバリが可能になります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

```
c1qf5bt001
```

アラート条件

赤: Amazon RDS リソースでは自動バックアップが有効になっていません

[Recommended Action] (推奨されるアクション)

最大 14 日間の保存期間で自動バックアップを有効にします。

その他のリソース

自動バックアップでは、お客様の DB インスタンスのポイントインタイムリカバリが可能になります。自動バックアップをオンにすることをおすすめします。DB インスタンスの自動バックアップを有効にすると、Amazon RDS は希望するバックアップウィンドウに毎日自動的にデータの完全バックアップを実行します。バックアップは、DB インスタンスが更新されるとトランザクションログをキャプチャします。お客様の DB インスタンスのストレージサイズまで、バックアップストレージを追加料金なしでご利用いただけます。

詳細については、以下のリソースを参照してください。

- 自動バックアップの有効化
- Amazon RDS バックアップストレージコストとは

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS sync_binlog パラメータは無効になっています

説明

DB インスタンスでトランザクションのコミットが確認される前には、バイナリログのディスクへの同期は実行されません。

sync_binlog パラメータの値を 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt031`

アラート条件

黄色: DB パラメータグループの同期バイナリログ記録は無効になっています。

[Recommended Action] (推奨されるアクション)

sync_binlog パラメータを 1 に設定します。

その他のリソース

sync_binlog パラメータは、MySQL がバイナリログをディスクにプッシュする方法を制御します。このパラメータの値を 1 に設定すると、トランザクションがコミットされる前にバイナリログのディスクへの同期が有効になります。このパラメーターの値を 0 に設定すると、ディスクへのバイナリログ同期がオフになります。通常、MySQL サーバーはオペレーティングシステムに依存して、他のファイルと同様にバイナリログを定期的にディスクにプッシュします。sync_binlog パラメータ値を 0 に設定すると、パフォーマンスが向上します。ただし、停電やオペレーティングシステムのクラッシュが発生すると、サーバーはバイナリログと同期されていないコミット済みのトランザクションをすべて失います。

詳細については、「Best practices for configuring parameters for Amazon RDS for MySQL, part 2: Parameters related to replication」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

RDS DB クラスターでマルチ AZ レプリケーションが有効になっていない

説明

Amazon RDS DB クラスターでマルチ AZ レプリケーションが有効になっているかどうかを確認します。

マルチ AZ DB クラスターには、3 つの別々のアベイラビリティーゾーンに 1 つのライター DB インスタンスと 2 つのリーダー DB インスタンスがあります。マルチ AZ DB クラスターは、マルチ AZ 配置と比較して、高可用性、読み取りワークロードの容量の増加、および低レイテンシーを提供します。

詳細については、「マルチ AZ DB クラスターの作成」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz161
```

ソース

```
AWS Config Managed Rule: rds-cluster-multi-az-enabled
```

アラート条件

黄: Amazon RDS DB クラスターにはマルチ AZ レプリケーションが設定されていません

[Recommended Action] (推奨されるアクション)

Amazon RDS DB クラスターを作成するときに、マルチ AZ DB クラスターデプロイを有効にします。

詳細については、「マルチ AZ DB クラスターの作成」を参照してください。

その他のリソース

マルチ AZ DB クラスターのデプロイ

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

RDS マルチ AZ スタンバイインスタンスが有効になっていない

説明

Amazon RDS DB インスタンスにマルチ AZ スタンバイレプリカが設定されているかどうかを確認します。

Amazon RDS マルチ AZ は、異なるアベイラビリティーゾーンにあるスタンバイレプリカにデータを複製することで、データベースインスタンスの高可用性と耐久性を実現します。これにより、自動フェイルオーバーが可能になり、パフォーマンスが向上し、データの耐久性が向上します。マルチ AZ DB インスタンスのデプロイでは、Amazon RDS は、異なるアベイラビリティーゾーンで同期スタンバイレプリカを自動的にプロビジョンおよび維持します。プライマリ DB インスタンスは、アベイラビリティーゾーン間でスタンバイレプリカに同期的に複製され、データの冗長性を提供し、システムバックアップ中の遅延スパイクを最小限に抑えます。高可用性を備えた DB インスタンスを実行すると、計画されたシステムメンテナンス中の可用性が向上します。また、DB インスタンスの障害とアベイラビリティーゾーンの中断からデータベースを保護することを助けることもできます。

詳細については、「マルチ AZ DB インスタンスのデプロイ」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz156
```

ソース

```
AWS Config Managed Rule: rds-multi-az-support
```

アラート条件

黄: Amazon RDS DB インスタンスにマルチ AZ レプリカが設定されていません。

[Recommended Action] (推奨されるアクション)

Amazon RDS DB インスタンスを作成するときに、マルチ AZ 配置を有効にします。

このチェックは、 Trusted Advisor コンソールのビューから除外することはできません。

その他のリソース

マルチAZ DB インスタンスのデプロイ

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon RDS ReplicaLag

説明

RDS データベースインスタンスの ReplicaLag CloudWatch メトリクスが、過去 1 週間に運用上合理的なしきい値を超えたかどうかを確認します。

ReplicaLag メトリクスは、リードレプリカがプライマリインスタンスより遅れている秒数を測定します。リードレプリカに加えられた非同期更新が、プライマリデータベースインスタンスで行われている更新に追いつけないと、レプリケーションラグが発生します。プライマリインスタンスに障害が発生した場合、ReplicaLag が運用上妥当なしきい値を超えていると、リードレプリカからデータが失われる可能性があります。

チェック ID

`Cmsvnj8db1`

アラート条件

- 赤: ReplicaLag メトリクスが 1 週間に少なくとも 1 回は 60 秒を超えました。
- 黄: ReplicaLag メトリクスが 1 週間に少なくとも 1 回は 10 秒を超えました。
- 緑: ReplicaLag が 10 秒未満です。

[Recommended Action] (推奨されるアクション)

ReplicaLag が運用上の安全レベルを超えて増加する原因はいくつか考えられます。例えば、古いバックアップのレプリカインスタンスが最近交換または起動され、これらのレプリカがプライマリデータベースインスタンスとライブトランザクションに「追いつく」のにかなりの時間がかかることが原因である可能性があります。この ReplicaLag は、追いつきが発生するにつれて、時間の経過とともに減少する可能性があります。もう 1 つの例としては、プライマリデータベースインスタンスで達成できるトランザクション速度が、レプリケーションプロセスやレプリカインフラストラクチャで達成できる速度よりも速いことが挙げられます。この ReplicaLagは、レプリケーションがプライマリデータベースのパフォーマンスに追いついていないため、時間の経過とともに増加する可能性があります。最後に、1 日、1 か月などのさまざまな期間にわたってワークロードが集中し、その結果、ReplicaLag が遅くなることがあります。チームは、データベースの ReplicaLag が高くなる原因と考えられる根本原因を調査し、場合によってはデータベースインスタンスタイプやワークロードのその他の特性を変更して、レプリカ上のデータ継続性が要件と一致するようにする必要があります。

その他のリソース

- Amazon RDS for PostgreSQL でのリードレプリカの使用

- Amazon RDS での MySQL のレプリケーションの使用
- MySQL リードレプリカの使用

[Report columns] (レポート列)

- ステータス
- リージョン
- DB インスタンス ARN
- ReplicaLag メトリクス

Amazon RDS の synchronous_commit パラメータは無効になっています。

説明

synchronous_commit パラメータを無効にすると、データベースのクラッシュでデータが失われる可能性があります。データベースの耐久性が危険にさらされます。

synchronous_commit パラメータを有効にすることをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

c1qf5bt026

アラート条件

赤: DB パラメータグループでは synchronous_commit パラメータが無効になっています。

[Recommended Action] (推奨されるアクション)

DB パラメータグループの synchronous_commit パラメータを有効にします。

その他のリソース

synchronous_commit パラメータは、データベースサーバーがクライアントに成功通知を送信する前に先書き口グ(WAL) プロセスを完了することを定義します。WAL がトランザクションをディスクに保存する前にクライアントがコミットを承認するため、このコミットは非同期コミットと呼ばれます。synchronous_commit パラメータを無効にすると、トランザクションが失われ、DB インスタンスの耐久性が損なわれ、データベースがクラッシュしたときにデータが失われる可能性があります。

詳細については、「MySQL データベースログファイル」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- パラメータ名
- 推奨値
- 最終更新日時

Amazon Redshift クラスターの自動スナップショット

説明

自動スナップショットが Amazon Redshift クラスターに対して有効になっていることを確認します。

Amazon Redshift は、前回のスナップショット以降にクラスターに加えられた増分変更を追跡する、増分スナップショットを自動的に作成します。自動スナップショットは、スナップショットからクラスターを復元するために必要なすべてのデータを保持します。自動スナップショットを

無効にするには、保持期間を 0 に設定します。RA3 ノードタイプでは、自動スナップショットを無効にすることはできません。

AWS Config ルールの MinRetentionPeriod および MaxRetentionPeriod パラメータを使用して、必要な最小保持期間と最大保持期間を指定できます。

Amazon Redshift スナップショットとバックアップ

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz135`

ソース

`AWS Config Managed Rule: redshift-backup-enabled`

アラート条件

赤: Amazon Redshift で、希望する保持期間内に自動スナップショットが設定されていません。

[Recommended Action] (推奨されるアクション)

Amazon Redshift クラスターに対して自動スナップショットが有効になっていることを確認します。

詳細については、「コンソールを使用したスナップショットの管理」を参照してください。

その他のリソース

Amazon Redshift スナップショットとバックアップ

詳細については、「バックアップの使用」を参照してください。

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

削除された Amazon Route 53 ヘルスチェック

説明

削除されたヘルスチェックに関連付けられているリソースレコードセットをチェックします。

リソースレコードセットに関連付けられているヘルスチェックの削除を防止する機構は Route 53 にありません。関連付けられたリソースレコードセットを更新せずにヘルスチェックを削除すると、DNS フェイルオーバー設定の DNS クエリのルーティングは意図したとおりに機能しません。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`Cb877eB72b`

アラート条件

黄: リソースレコードセットが削除されたヘルスチェックに関連付けられています。

[Recommended Action] (推奨されるアクション)

新しいヘルスチェックを作成し、リソースレコードセットに関連付けます。「ヘルスチェックの作成、更新、削除」および「Adding Health Checks to Resource Record Sets」(リソースレコードセットへのヘルスチェックの追加) を参照してください。

その他のリソース

- Amazon Route 53 ヘルスチェックと DNS フェイルオーバー
- Amazon Route 53 のシンプルな設定でのヘルスチェックの動作

[Report columns] (レポート列)

- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名

- リソースレコードセットのタイプ
- リソースレコードセットの識別子

Amazon Route 53 フェイルオーバーリソースレコードセット

説明

設定ミスがある Amazon Route 53 フェイルオーバーリソースレコードセットをチェックします。

Amazon Route 53 のヘルスチェックでプライマリリソースが正常でないと判断されると、Amazon Route 53 はセカンダリのバックアップリソースレコードセットでクエリに応答します。フェイルオーバーが機能するには、正しく設定されたプライマリリソースレコードセットとセカンダリリソースレコードセットを作成する必要があります。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`b73EEdD790`

アラート条件

- 黄: プライマリフェイルオーバーリソースレコードセットには、対応するセカンダリリソースレコードセットがありません。
- 黄: セカンダリフェイルオーバーリソースレコードセットには、対応するプライマリリソースレコードセットがありません。
- 黄: 同じ名前のプライマリリソースレコードセットとセカンダリリソースレコードセットが同じヘルスチェックに関連付けられています。

[Recommended Action] (推奨されるアクション)

フェイルオーバーリソースセットがない場合は、対応するリソースレコードセットを作成します。「Creating Failover Resource Record Sets」(フェイルオーバーリソースレコードセットの作成) を参照してください。

リソースレコードセットが同じヘルスチェックに関連付けられている場合は、それぞれに個別のヘルスチェックを作成します。「ヘルスチェックの作成、更新、削除」を参照してください。

その他のリソース

Amazon Route 53 ヘルスチェックと DNS フェイルオーバー

[Report columns] (レポート列)

- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名
- リソースレコードセットのタイプ
- 理由

Amazon Route 53 高 TTL リソースレコードセット

説明

有効期限 (TTL) の値を小さくすることでメリットが生まれる可能性のあるリソースレコードセットをチェックします。

TTL は、リソースレコードセットが DNS リゾルバーによってキャッシュされる秒数です。長い TTL を指定すると、DNS リゾルバーは更新された DNS レコードのリクエストに時間がかかり、トラフィックの再ルーティングに不要な遅延が発生する可能性があります (たとえば、DNS フェイルオーバーがいずれかのエンドポイントの障害を検出して応答した場合) 。このチェックは、フェイルオーバーのポリシーを持つレコード、または関連付けられたヘルスチェックがあるレコードのみを調べます。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`C056F80cR3`

アラート条件

- 黄: ルーティングポリシーが [Failover] (フェイルオーバー) であるリソースレコードセットの TTL が 60 秒を超えています。
- 緑: リソースレコードにフェイルオーバーポリシーがないか、TTL が 60 未満のフェイルオーバーポリシーがあります。

[Recommended Action] (推奨されるアクション)

リストされたリソースレコードセットのために 60 秒の TTL 値を入力します。詳細については、「Working with Resource Record Sets」(リソースレコードセットの使用) を参照してください。

その他のリソース

Amazon Route 53 ヘルスチェックと DNS フェイルオーバー

[Report columns] (レポート列)

- ステータス
- ホストゾーン名
- ホストゾーン ID
- リソースレコードセット名
- リソースレコードセットのタイプ
- リソースレコードセット ID
- TTL

Amazon Route 53 ネームサーバー権限移譲

説明

ドメインレジストラまたは DNS が正しい Route 53 ネームサーバーを使用していない Amazon Route 53 ホストゾーンをチェックします。

ホストゾーンを作成する場合、Route 53 はホストゾーンに一連の 4 つのネームサーバーの移譲セットを割り当てます。これらのサーバーの名前は、ns-###.awsdns-##.com、.net、.org、および .co.uk です。ここで、### と ## は、一般的に別々の数を表します。Route 53 がドメインの DNS クエリをルーティングできるようにするには、レジストラのネームサーバー設定を更新して、レジストラが割り当てたネームサーバーを削除する必要があります。次に、Route 53 委任セットに 4 つのネームサーバーをすべて追加する必要があります。可用性を最大にするには、4 つの Route 53 ネームサーバーをすべて追加する必要があります。

AWS サービスによって作成されたホストゾーンは、チェック結果に表示されません。

チェック ID

`cF171Db240`

アラート条件

黄: ドメインのレジストラが委任セットの 4 つすべての Route 53 ネームサーバーを使用していないホストゾーン。

[Recommended Action] (推奨されるアクション)

レジストラまたはドメインの現在の DNS サービスでネームサーバーレコードを追加または更新し、Route 53 委任セットの 4 つすべてのネームサーバーを含めます。これらの値を見つける

には、「Getting the Name Servers for a Hosted Zone」(ホストゾーンのネームサーバーの取得) を参照してください。ネームサーバーレコードの追加または更新については、「Creating and Migrating Domains and Subdomains to Amazon Route 53」(ドメインおよびサブドメインの作成と Amazon Route 53 への移行) を参照してください。

その他のリソース

ホストゾーンの使用

[Report columns] (レポート列)

- ホストゾーン名
- ホストゾーン ID
- 使用されたネームサーバーの委任の数

Amazon Route 53 Resolver エンドポイントアベイラビリティーゾーンの冗長性

説明

サービス設定に、冗長性のために少なくとも 2 つのアベイラビリティーゾーン (AZ) で指定されている IP アドレスがあるかどうかを確認します。AZ は、他のゾーンの障害から隔離された独立した場所です。同一のリージョン内の複数のアベイラビリティーゾーンで IP アドレスを指定することにより、単一障害点からアプリケーションを保護できます。

チェック ID

`Chrv231ch1`

アラート条件

- 黄: IP アドレスは 1 つの AZ でのみ指定されています。
- 緑: IP アドレスは少なくとも 2 つの AZ で指定されています

[Recommended Action] (推奨されるアクション)

冗長性を確保するために、少なくとも 2 つのアベイラビリティーゾーンで IP アドレスを指定します。

その他のリソース

- 複数の Elastic Network Interface エンドポイントを常時使用できるようにする場合は、必要とするネットワークインターフェイス数の他に少なくとも 1 つ余分にインターフェイスを作成し、トラフィックが急増した場合にも処理できるよう追加の容量を確保しておくことをお勧め

します。また、追加のネットワークインターフェイスでメンテナンスやアップグレードなどのサービス作業を行っている間の可用性も確保できます。

- リゾルバーエンドポイントの高可用性

[Report columns] (レポート列)

- ステータス
- リージョン
- リソースARN
- AZ の数

Amazon S3 バケットロギング

説明

Amazon Simple Storage Service (Amazon S3) バケットのログ設定を確認します。

サーバーアクセスログが有効になっている場合、詳細なアクセスログは、選択したバケットに 1 時間ごとに配信されます。アクセスログには、リクエストのタイプ、リクエストで指定されたリソース、リクエストが処理された日時など、各リクエストの詳細が記録されます。デフォルトでは、バケットのログは有効になっていません。セキュリティ監査を実行する場合、またはユーザーと使用パターンについて詳しく知りたい場合は、ログを有効にする必要があります。

ログが最初に有効になっている場合、設定が自動的に検証されます。ただし、今後の変更により、ログが失敗する可能性があります。このチェックでは、明示的な Amazon S3 バケットのアクセス許可が検査されますが、バケットのアクセス許可を上書きする可能性のある関連付けられたバケットポリシーは検査されません。

チェック ID

`BueAdJ7NrP`

アラート条件

- 黄: バケットでサーバーアクセスのログ記録が有効になっていません。
- 黄: ターゲットバケットのアクセス許可にはルートアカウントが含まれていないため、 はルートアカウントを確認 Trusted Advisor できません。
- 赤: ターゲットバケットが存在しません。
- 赤: ターゲットバケットとソースバケットの所有者が異なります。

- 赤: ログ配信者には、ターゲットバケットに対する書き込み許可がありません。

[Recommended Action] (推奨されるアクション)

ほとんどのバケットでバケットログ記録を有効にします。「Enabling Logging Using the Console」(コンソールを使用してログ記録を有効にする) および「Enabling Logging Programmatically」(プログラムを使用してログ記録を有効にする) を参照してください。

ターゲットバケットのアクセス許可にルートアカウントが含まれておらず、ログ記録のステータス Trusted Advisor を確認する場合は、ルートアカウントを被付与者として追加します。「Editing Bucket Permissions」(バケット許可の編集) を参照してください。

ターゲットバケットが存在しない場合は、既存のバケットをターゲットとして選択するか、新しいバケットを作成して選択します。「Managing Bucket Logging」(バケットのログ記録の管理) を参照してください。

ターゲットとソースの所有者が異なる場合は、ターゲットバケットを、ソースバケットと同じ所有者を持つバケットに変更します。「Managing Bucket Logging」(バケットのログ記録の管理) を参照してください。

ターゲットに対する書き込み許可がログの配信者に付与されていない (書き込みが有効になっていない) 場合は、ログ配信グループにアップロード/削除許可を付与します。「Editing Bucket Permissions」(バケット許可の編集) を参照してください。

その他のリソース

- バケットの使用
- サーバーアクセスのログ記録
- サーバーアクセスログの形式
- ログファイルの削除

[Report columns] (レポート列)

- ステータス
- リージョン
- バケット名
- ターゲット名
- ターゲットが存在
- 同じ所有者

- 書き込み有効
- 理由

Amazon S3 バケットレプリケーションが有効になっていない

説明

Amazon S3 バケットで、クロスリージョンレプリケーション、同一リージョンレプリケーション、またはその両方に対してレプリケーションルールが有効になっているかどうかを確認します。

レプリケーションは、同じリージョンまたは異なる AWS リージョンのバケット間でオブジェクトを自動的に非同期コピーします。レプリケーションでは、新しく作成されたオブジェクトおよびオブジェクトの更新が、レプリケート元バケットからレプリケート先バケットにコピーされます。Amazon S3 バケットレプリケーションを使用すると、アプリケーションとデータストレージの耐障害性とコンプライアンスを向上させることができます。

詳細については、「オブジェクトのレプリケーション」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz119
```

ソース

```
AWS Config Managed Rule: s3-bucket-replication-enabled
```

アラート条件

黄: Amazon S3 バケットで、クロスリージョンレプリケーション、同一リージョンレプリケーション、またはその両方に対してレプリケーションルールが有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon S3 バケットレプリケーションルールをオンにして、アプリケーションとデータストレージの耐障害性とコンプライアンスを向上させます。

詳細については、「バックアップジョブと復旧ポイントの表示」と「レプリケーションの設定」を参照してください。

その他のリソース

チュートリアル: レプリケーションの設定例

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon S3 バケットバージョニング

説明

バージョニングが有効になっていないか、バージョニングが停止している Amazon Simple Storage Service バケットをチェックします。

バージョニングが有効であれば、意図しないユーザーアクションとアプリケーション障害の両方から簡単に復旧できます。バージョニングを使用すると、 バケットに保存されたオブジェクトのすべてのバージョンを保存、取得、復元することができます。ライフサイクルルールを使用してオブジェクトを Glacier ストレージクラスに自動的にアーカイブすることで、オブジェクトのすべてのバージョンとそれに関連するコストを管理できます。ルールを設定して、指定した期間後にオブジェクトのバージョンを削除することもできます。バケットのオブジェクトの削除や設定の変更に多要素認証 (MFA) を要求することもできます。

バージョン管理を有効にした後は、非アクティブ化できません。ただし、一時停止して、オブジェクトの新しいバージョンが作成されないようにすることができます。バージョニングを使用すると、オブジェクトの複数のバージョンのストレージ料金が発生するため、Amazon S3 のコストが増加する可能性があります。

チェック ID

R365s2Qddf

アラート条件

- 緑: バケットに対するバージョニングは有効になっています。
- 黄: バケットに対するバージョニングは有効になっていません。
- 黄: バケットのバージョニングが一時停止されています。

[Recommended Action] (推奨されるアクション)

誤って削除したり上書きしたりしないように、ほとんどのバケットでバケットのバージョニングを有効にします。「バージョニングの使用」および「Enabling Versioning Programmatically」(プログラムを使用してバージョニングを有効にする) を参照してください。

バケットのバージョニングが一時停止されている場合は、バージョニングを再度有効にすることを検討してください。バージョニングが停止されたバケット内のオブジェクトの操作については、「Managing Objects in a Versioning-Suspended Bucket」(バージョニングが停止されたバケット内のオブジェクトの管理) を参照してください。

バージョニングが有効または一時停止されている場合、特定のオブジェクトバージョンを期限切れとしてマークするか、不要なオブジェクトバージョンを完全に削除するライフサイクル設定ルールを定義できます。詳細については、「オブジェクトのライフサイクル管理」を参照してください。

MFA Delete では、バケットのバージョニングステータスが変更される場合、またはオブジェクトのバージョンが削除される場合に、追加の認証が必要です。ユーザーは、承認された認証デバイスから認証情報とコードを入力する必要があります。詳細については、「MFA Delete」を参照してください。

その他のリソース

バケットの使用

[Report columns] (レポート列)

- ステータス
- リージョン
- バケット名
- バージョニング
- MFA Delete 有効

Application、Network、Gateway Load Balancer が、複数のアベイラビリティーゾーンにまたがっていない

説明

Load Balancer (Application、Network、Gateway Load Balancer) が複数のアベイラビリティーゾーンにまたがるサブネットで構成されているかどうかを確認します。

AWS Config ルールの minAvailabilityZones パラメータで、必要な最小アベイラビリティーゾーンを指定できます。

詳細については、「Application Load Balancer のアベイラビリティーゾーン」、「アベイラビリティーゾーン- Network Load Balancer」、および「ゲートウェイロードバランサーを作成」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz169
```

ソース

```
AWS Config Managed Rule: elbv2-multiple-az
```

アラート条件

黄: 2 つ未満のアベイラビリティーゾーンのサブネットで構成された Application、Network、または Gateway Load Balancer。

[Recommended Action] (推奨されるアクション)

Application、Network、Gateway Load Balancer を複数のアベイラビリティーゾーンにまたがるサブネットで構成します。

その他のリソース

Application Load Balancer のアベイラビリティーゾーン

アベイラビリティーゾーン (Elastic Load Balancing)

ゲートウェイロードバランサーを作成

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

サブネットで利用可能な IP の自動スケーリング

説明

ターゲットサブネットで十分な IP が使用可能であることを確認します。使用可能な IP が十分にあると、Auto Scaling グループが最大サイズに達し、追加のインスタンスを起動する必要がある場合に役立ちます。

チェック ID

`Cjxm268ch1`

アラート条件

- 赤: ASG が作成できるインスタンスと IP アドレスの最大数が、設定したサブネットに残っている IP アドレスの数を超えています。
- 緑: ASG の残りの規模に対応できる十分な IP アドレスがあります。

[Recommended Action] (推奨されるアクション)

利用可能な IP アドレスの数を増やす

[Report columns] (レポート列)

- ステータス
- リージョン

- リソースARN
- 作成できるインスタンスの最大数
- 使用可能なインスタンス数

Auto Scaling Group ヘルスチェック

説明

Auto Scaling グループのヘルスチェック設定を調べます。

Auto Scaling グループに Elastic Load Balancing が使用されている場合は、Elastic Load Balancing ヘルスチェックを有効にすることをお勧めします。Elastic Load Balancing ヘルスチェックを使用しない場合、Auto Scaling は Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの状態にのみ作用します。Auto Scaling は、インスタンスで実行されているアプリケーションに対して動作しません。

チェック ID

`CL0G40CD08`

アラート条件

- 黄: Auto Scaling グループにはロードバランサーが関連付けられていますが、Elastic Load Balancing ヘルスチェックは有効になっていません。
- 黄: Auto Scaling グループにはロードバランサーが関連付けられていませんが、Elastic Load Balancing ヘルスチェックは有効になっています。

[Recommended Action] (推奨されるアクション)

Auto Scaling グループにロードバランサーが関連付けられているが、Elastic Load Balancing ヘルスチェックが有効になっていない場合は、「Auto Scaling グループに Elastic Load Balancing ヘルスチェックを追加する」を参照してください。

Elastic Load Balancing ヘルスチェックが有効になっているが、Auto Scaling グループにロードバランサーが関連付けられていない場合は、「Set Up an Auto-Scaled and Load-Balanced Application」(Auto Scaling および負荷分散アプリケーションのセットアップ) を参照してください。

その他のリソース

Amazon EC2 Auto Scaling ユーザーガイド

[Report columns] (レポート列)

- ステータス
- リージョン
- Auto Scaling グループ名
- 関連付けられている Load Balancer
- ヘルスチェック

Auto Scaling グループリソース

説明

起動設定、起動テンプレート、Auto Scaling グループに関連付けられたリソースの可用性をチェックします。

使用できないリソースをポイントする Auto Scaling グループは、新しい Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動できません。Auto Scaling が適切に設定されている場合、Amazon EC2 インスタンスの数は需要のスパイク時にシームレスに増加し、需要不足時には自動的に減少します。使用できないリソースを指す Auto Scaling グループと起動設定/起動テンプレートは、意図したとおりに動作しません。

チェック ID

`8CNsSllI5v`

アラート条件

- 赤: Auto Scaling グループは、削除されたロードバランサーに関連付けられています。
- 赤: 起動設定は、削除された Amazon マシンイメージ (AMI) に関連付けられています。
- 赤: 起動テンプレートは、削除された Amazon マシンイメージ (AMI) に関連付けられています。

[Recommended Action] (推奨されるアクション)

ロードバランサーが削除された場合は、新しいロードバランサーまたはターゲットグループを作成し、それを Auto Scaling グループに関連付けるか、ロードバランサーなしで新しい Auto Scaling グループを作成します。新しいロードバランサーを使用して新しい Auto Scaling グループを作成する方法については、「Set Up an Auto-Scaled and Load-Balanced Application」(Auto Scaling および負荷分散アプリケーションのセットアップ) を参照してください。ロードバランサーを使用せずに新しい Auto Scaling グループを作成する方法については、「Getting

Started With Auto Scaling Using the Console」(コンソールを使用した Auto Scaling の開始方法) の「Create Auto Scaling Group」(Auto Scaling グループの作成) を参照してください。

AMI が削除された場合は、有効な AMI を使用して新しい起動設定または起動テンプレートバージョンを作成し、Auto Scaling グループと関連付けます。新しい起動設定を作成する方法については、Amazon EC2 Auto Scaling ユーザーガイド」の「起動設定の作成」を参照してください。起動テンプレートの作成方法については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループの起動テンプレートを作成する」を参照してください。 Amazon EC2 Auto Scaling

> **Note**
>
> セキュリティ上の理由から、チェック結果には起動テンプレートの AWS Systems Manager パラメータを使用して参照されるリソースは含まれません。

起動テンプレートに Amazon マシンイメージ (AMI) ID を含む AWS Systems Manager パラメータが含まれている場合は、起動テンプレートを確認してパラメータが有効な AMI ID を参照しているか、 AWS Systems Manager パラメータストアで適切な変更を行います。詳細については、Amazon EC2 Auto Scaling ユーザーガイドIDs の代わりに AWS Systems Manager パラメータを使用する」を参照してください。

その他のリソース

- Troubleshooting Auto Scaling: Amazon EC2 AMIs (Auto Scaling のトラブルシューティング: Amazon EC2 AMI)
- Troubleshooting Auto Scaling: Load Balancer Configuration (Auto Scaling のトラブルシューティング: ロードバランサーの設定)
- Amazon EC2 Auto Scaling ユーザーガイド
- AMI ID の代わりに AWS Systems Manager パラメータを使用する IDs

[Report columns] (レポート列)

- ステータス
- リージョン
- Auto Scaling グループ名
- 起動タイプ
- リソースタイプ
- リソース名

AWS CloudHSM 単一の AZ で HSM インスタンスを実行するクラスター

説明

単一のアベイラビリティーゾーン (AZ) で HSM インスタンスを実行するクラスターをチェックします。このチェックは、クラスターに最新のバックアップがないリスクがある場合に警告します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`hc0dfs7601`

アラート条件

- 黄色: CloudHSM クラスターは、単一のアベイラビリティーゾーンですべての HSM インスタンスを 1 時間以上実行しています。
- 緑色: CloudHSM クラスターは、少なくとも 2 つの異なるアベイラビリティーゾーンにあるすべての HSM インスタンスを実行しています。

[Recommended Action] (推奨されるアクション)

異なるアベイラビリティーゾーンにあるクラスターのインスタンスを少なくとも 1 つ以上作成します。

その他のリソース

のベストプラクティス AWS CloudHSM

[Report columns] (レポート列)

- ステータス
- リージョン
- クラスター ID
- HSM インスタンス数

- 最終更新日時

AWS Direct Connect ロケーションの耐障害性

説明

オンプレミスを各 Direct Connect ゲートウェイまたは仮想プライベートゲートウェイに接続する AWS Direct Connect ために使用される の耐障害性をチェックします。

このチェックでは、Direct Connect ゲートウェイまたは仮想プライベートゲートウェイに、少なくとも 2 つの異なる Direct Connect ロケーションにまたがる仮想インターフェイスが設定されていない場合に警告します。ロケーションの耐障害性がないと、メンテナンス中の予期しないダウンタイム、ファイバーの切断、デバイスの障害、または完全なロケーション障害が発生する可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

> **Note**
>
> Direct Connect は、Direct Connect ゲートウェイを使用して Transit Gateway で実装されます。

チェック ID

`c1dfpnchv2`

アラート条件

赤: Direct Connect ゲートウェイまたは仮想プライベートゲートウェイは、単一の Direct Connect デバイスに 1 つ以上の仮想インターフェイスで設定されています。

黄: Direct Connect ゲートウェイまたは仮想プライベートゲートウェイは、1 つの Direct Connect ロケーション内の複数の Direct Connect デバイス間の仮想インターフェイスで設定されています。

緑: Direct Connect ゲートウェイまたは仮想プライベートゲートウェイは、2 つ以上の異なる Direct Connect ロケーションにまたがる仮想インターフェイスで設定されています。

[Recommended Action] (推奨されるアクション)

Direct Connect ロケーションレジリエンシーを構築するには、少なくとも 2 つの異なる Direct Connect ロケーションに接続するように Direct Connect ゲートウェイまたは仮想プライベートゲートウェイを設定できます。詳細については、AWS Direct Connect 「障害耐性に関する推奨事項」を参照してください。

その他のリソース

AWS Direct Connect 障害耐性に関する推奨事項

AWS Direct Connect フェイルオーバーテスト

[Report columns] (レポート列)

- ステータス
- リージョン
- 最終更新日時
- 障害耐性ステータス
- ロケーション
- 接続 ID
- ゲートウェイ ID

AWS Lambda デッドレターキューが設定されていない 関数

説明

AWS Lambda 関数にデッドレターキューが設定されているかどうかを確認します。

デッドレターキューは、失敗したイベントをキャプチャして分析 AWS Lambda し、それらのイベントを適切に処理する方法を提供する の機能です。コードによって例外が発生したり、タイムアウトになったり、メモリが不足したりして、Lambda 関数の非同期実行が失敗する可能性があります。デッドレターキューは、失敗した呼び出しからのメッセージを格納し、メッセージを処理して障害をトラブルシューティングする方法を提供します。

AWS Config ルールの dlqArns パラメータを使用して、チェックするデッドレターキューリソースを指定できます。

詳細については、「デッドレターキュー」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz182`

ソース

`AWS Config Managed Rule: lambda-dlq-check`

アラート条件

黄: AWS Lambda 関数にデッドレターキューが設定されていません。

[Recommended Action] (推奨されるアクション)

AWS Lambda 失敗したすべての非同期呼び出しのメッセージ処理を制御するように関数にデッドレターキューが設定されていることを確認します。

詳細については、「デッドレターキュー」を参照してください。

その他のリソース

- AWS Lambda デッドレターキューによる堅牢なサーバーレスアプリケーション設計

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS Lambda 失敗時のイベントの送信先

説明

失敗した呼び出しからのレコードを送信先にルーティングして、さらなる調査や処理を行うことができるように、アカウントの Lambda 関数に障害時のイベント送信先または非同期呼び出し用に設定されたデッドレターキュー (DLQ) があるかをチェックします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c1dfprch05`

アラート条件

- 黄色: 関数には障害時のイベントの送信先または DLQ が設定されていません。

[Recommended Action] (推奨されるアクション)

さらなるデバッグや処理を行えるように、Lambda 関数の障害時のイベント送信先または DLQ を設定して、失敗した呼び出しを、他の詳細とともに使用可能な送信先の AWS のサービスのいずれかに送信するようにしてください。

その他のリソース

- 非同期呼び出し
- AWS Lambda 失敗時のイベントの送信先

[Report columns] (レポート列)

- ステータス
- リージョン
- フラグが付けられたバージョンを持つ関数。
- 現在の非同期リクエストがドロップされた割合
- 当日の非同期リクエスト

- 非同期リクエストがドロップされた割合 (1 日あたりの平均)
- 非同期リクエスト (1 日あたりの平均)
- 最終更新日時

AWS Lambda VPC 対応関数 (マルチ AZ 冗長性なし)

説明

1 つのアベイラビリティーゾーンでサービスの中断に対して脆弱な VPC 対応 Lambda 関数の $LATEST バージョンを確認します。VPC 対応関数は、高可用性を実現するために複数のアベイラビリティーゾーンに接続することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`L4dfs2Q4C6`

アラート条件

黄: VPC 対応 Lambda 関数の $LATEST バージョンは、単一のアベイラビリティーゾーンのサブネットに接続されています。

[Recommended Action] (推奨されるアクション)

VPC にアクセスするために関数を設定する場合、高可用性を確保するために、複数のアベイラビリティーゾーンでサブネットを選択します。

その他のリソース

- VPC 内のリソースにアクセスするように Lambda 関数を設定する
- の耐障害性 AWS Lambda

[Report columns] (レポート列)

- ステータス

- リージョン
- 関数 ARN
- VPC ID
- 平均日次呼び出し
- 最終更新日時

AWS Outposts シングルラックデプロイ

説明

Outposts ラックのバランスをチェックします。これは、お客様が Outposts インスタンスを複数の Outposts ラックにデプロイするか、単一の Outpost ラックにデプロイするかを評価します。単一の Outposts ラックは、単一のラックに関連する問題 (環境障害など) に対して単一の障害点を作成します。これらのシナリオは、複数のラックに Outpost をデプロイすることで軽減できます。

チェック ID

`c243hjzrhn`

アラート条件

- 黄: Outpost が単一ラックにデプロイされています
- 緑: Outpost は複数のラックにデプロイされます。

[Recommended Action] (推奨されるアクション)

で本番ワークロードを実行している場合は AWS Outposts、次の回復力のあるアーキテクチャを使用するのがベストプラクティスです。1 つの AWS Outposts ラックで 1 つの障害点が作成されます。フェイルオーバーイベントに十分な容量を持つ別の AWS Outposts ラックをその場所に追加し、ラック間でワークロードを分散することを検討してください。

その他のリソース

障害モード 4: ラックまたはデータセンター

[Report columns] (レポート列)

- ステータス
- リソースARN
- AZ
- ラック数

- 最終更新日時

AWS Resilience Hub アプリケーションコンポーネントのチェック

説明

アプリケーションのアプリケーションコンポーネント (AppComponent) が回復不能かどうかを確認します。中断イベントが発生した場合に AppComponent が復旧しない場合、不明なデータ損失やシステムのダウンタイムが発生する可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

チェック ID

`RH23stmM04`

アラート条件

赤: AppComponent は回復できません。

[Recommended Action] (推奨されるアクション)

AppComponent が回復可能であることを確認するには、障害耐性に関する推奨事項を確認して実装し、新しい評価を実行します。障害耐性に関する推奨事項の確認の詳細については、「その他のリソース」を参照してください。

その他のリソース

障害耐性に関する推奨事項の確認

AWS Resilience Hub の概念

AWS Resilience Hub ユーザーガイド

[Report columns] (レポート列)

- ステータス
- リージョン
- アプリケーション名

- AppComponent 名
- 最終更新日時

AWS Resilience Hub ポリシー違反

説明

ポリシーで定義されている目標復旧時間 (RTO) と目標復旧時点 (RPO) を満たしていないアプリケーションを Resilience Hub でチェックします。このチェックでは、Resilience Hub でアプリケーションに設定した RTO と RPO をアプリケーションが満たしていない場合に警告が表示されます。

> **Note**
>
> > **Note**
> >
> > このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> > ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`RH23stmM02`

アラート条件

- 緑色: アプリケーションにはポリシーがあり、RTO と RPO の目標を満たしています。
- 黄色: アプリケーションはまだ評価されていません。
- 赤色: アプリケーションにはポリシーがありますが、RTO と RPO の目標を満たしていません。

[Recommended Action] (推奨されるアクション)

Resilience Hub コンソールにサインインし、レコメンデーションを確認して、アプリケーションが RTO と RPO を満たしていることを確認します。

その他のリソース

Resilience Hub の概念

[Report columns] (レポート列)

- ステータス
- リージョン
- アプリケーション名
- 最終更新日時

AWS Resilience Hub レジリエンススコア

説明

Resilience Hub でアプリケーションの評価が実行されたかどうかをチェックします。このチェックでは、耐障害性スコアが特定の値を下回っている場合に警告が表示されます。

> **Note**
>
> > **Note**
> >
> > このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> > ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`RH23stmM01`

アラート条件

- 緑色: アプリケーションの耐障害性スコアは 70 以上です。
- 黄色: アプリケーションの耐障害性スコアは 40～69 です。
- 黄色: アプリケーションはまだ評価されていません。
- 赤色: アプリケーションの耐障害性スコアは 40 未満です。

[Recommended Action] (推奨されるアクション)

Resilience Hub コンソールにサインインして、アプリケーションの評価を実行します。レコメンデーションを確認して耐障害性スコアを向上させてください。

その他のリソース

Resilience Hub の概念

[Report columns] (レポート列)

- ステータス
- リージョン
- アプリケーション名
- アプリケーション耐障害性スコア
- 最終更新日時

AWS Resilience Hub 評価期間

説明

最後にアプリケーション評価を実行してからどれくらいの時間が経過したかを確認します。このチェックでは、指定した日数の間アプリケーション評価を実行していない場合に警告を表示します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`RH23stmM03`

アラート条件

- 緑: 過去 30 日間にアプリケーション評価が実行されました。

- 黄色: アプリケーションは、評価過去 30 日間に実行されていません。

[Recommended Action] (推奨されるアクション)

Resilience Hub コンソールにサインインして、アプリケーションの評価を実行します。

その他のリソース

Resilience Hub の概念

[Report columns] (レポート列)

- ステータス
- リージョン
- アプリケーション名
- 最期に評価が実行されてからの日数
- 最期の評価を実行した時刻
- 最終更新日時

AWS Site-to-Site VPN に DOWN ステータスのトンネルが少なくとも 1 つある

説明

各 でアクティブなトンネルの数を確認します AWS Site-to-Site VPN。

1 つの VPN には、常に 2 つのトンネルが設定されている必要があります。これにより、AWS エンドポイントでのデバイスの障害や計画的なメンテナンスの場合に冗長性が得られます。一部のハードウェアでは、一度に 1 つのトンネルだけがアクティブになります。VPN にアクティブなトンネルがない場合、その VPN の料金が引き続き適用される場合があります。

詳細については、「AWS Site-to-Site VPN とは」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c18d2gz123

ソース

AWS Config Managed Rule: vpc-vpn-2-tunnels-up

アラート条件

黄: Site-to-Site VPN で少なくとも 1 つのトンネルが DOWN です。

[Recommended Action] (推奨されるアクション)

VPN 接続用に 2 つのトンネルが設定されていることを確認します。また、ハードウェアが対応している場合は、両方のトンネルがアクティブであることを確認してください。VPN 接続が不要になった場合には、料金の発生を回避するために、それを削除します。

詳細については、カスタマーゲートウェイデバイス、および AWS ナレッジセンターで利用できるコンテンツを参照してください。

その他のリソース

- AWS Site-to-Site VPN ユーザーガイド
- VPC への仮想プライベートゲートウェイの追加

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

信頼性に関する AWS Well-Architected のリスクの高い問題

説明

信頼性の柱で、ワークロードに関するリスクの高い問題 (HRI) をチェックします。このチェックは、お客様の AWS-Well Architected レビューに基づきます。チェック結果は、AWS Well-Architected でワークロード評価を完了したかどうかによって異なります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`Wxdfp4B1L4`

アラート条件

- 赤: AWS Well-Architected の信頼性の柱で、少なくとも 1 つのアクティブな高リスクの問題が特定されました。
- 緑: AWS Well-Architected の信頼性の柱でアクティブな高リスクの問題は検出されませんでした。

[Recommended Action] (推奨されるアクション)

AWS Well-Architected は、ワークロード評価中に高リスクの問題を検出しました。これらの問題は、リスクを軽減し、費用を節約する機会を提示します。AWS Well-Architected ツールにサインインして、回答を確認し、アクティブな問題を解決するためのアクションを実行します。

[Report columns] (レポート列)

- ステータス
- リージョン
- ワークロードの ARN
- ワークロード名
- レビュー担当者名
- ワークロードタイプ
- ワークロードの開始日
- ワークロードの最終変更日
- 信頼性について特定された HRI の数
- 信頼性について解決された HRI の数

- 信頼性について回答された質問の数
- 信頼性の柱の質問の総数
- 最終更新日時

Classic Load Balancer に複数のAZが設定されていない

説明

Classic Load Balancer が複数のアベイラビリティーゾーン (AZ) にまたがるかどうかをチェックします。

ロードバランサーは、受信アプリケーショントラフィックを複数のアベイラビリティーゾーンの複数の Amazon EC2 インスタンス間で分散します。デフォルトでは、ロードバランサーは、ロードバランサーに対して有効にするアベイラビリティーゾーン間で均等にトラフィックを分散します。1 つのアベイラビリティーゾーンで停止が発生した場合、ロードバランサーノードは、1 つ以上のアベイラビリティーゾーンにある正常な登録済みのインスタンスにリクエストを自動的に転送します。

AWS Config ルールの minAvailabilityZones パラメータを使用して、アベイラビリティーゾーンの最小数を調整できます。

詳細については、「What is a Classic Load Balancer?」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> 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のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、1 つ以上のリソースを Trusted Advisor 結果に含めるか、結果から除外できます。

チェック ID

```
c18d2gz154
```

ソース

```
AWS Config Managed Rule: clb-multiple-az
```

アラート条件

黄: Classic Load Balancer にはマルチ AZ が設定されていないか、指定された最小数の AZ を満たしていません。

[Recommended Action] (推奨されるアクション)

Classic Load Balancer に複数のアベイラビリティーゾーンが設定されていることを確認します。ロードバランサーを複数の AZ に分散させて、アプリケーションの高可用性を確保してください。

詳細については、「Tutorial: Create a Classic Load Balancer」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

CLB 接続ドレイン

説明

Connection Draining が有効になっていない Classic ロードバランサーをチェックします。

Connection Draining が有効になっていず、Classic Load Balancer から Amazon EC2 インスタンスを登録解除すると、Classic Load Balancer はそのインスタンスへのトラフィックのルーティングを停止し、接続を閉じます。Connection Draining が有効になっている場合、Classic Load Balancer は登録解除されたインスタンスへの新しいリクエストの送信を停止しますが、アクティブなリクエストを処理するために接続を開いたままにします。

チェック ID

`7qGXsKIUw`

アラート条件

- 黄: Classic ロードバランサーで Connection Draining が有効になっていません。
- 緑: Classic Load Balancer で Connection Draining が有効になっています。

[Recommended Action] (推奨されるアクション)

Classic Load Balancer の接続ドレイニングを有効にします。詳細については、「Connection Draining」および「Enable or Disable Connection Draining for Your Load Balancer」(ロードバランサーの Connection Draining を有効または無効にする) を参照してください。

その他のリソース

Elastic Load Balancing のコンセプト

[Report columns] (レポート列)

- ステータス
- リージョン
- ロードバランサー名
- 理由

ELB ターゲット不均衡

説明

Application Load Balancer (ALB)、Network Load Balancer (NLB)、Gateway Load Balancer (GWLB) のアベイラビリティーゾーン (AZs) 間のターゲットグループのターゲット分散をチェックします。

このチェックでは、以下は除外されます。

- 単一のアベイラビリティーゾーン (AZ) で設定されたロードバランサー。
- 入力量が最も多い AZ と少ない AZs 間のターゲット数の差が 1 以下のロードバランサー。
- AvailabilityZone 属性が「all」に設定されている IP ベースのターゲットを持つターゲットグループ。

チェック ID

b92b83d667

アラート条件

- 赤: 単一の AZ はロードバランサー容量の 66% 以上を表します。
- 黄: 単一の AZ はロードバランサー容量の 50% 以上を表します。
- 緑: AZsロードバランサー容量の 50% 以上を表していません。

[Recommended Action] (推奨されるアクション)

耐障害性を向上させるには、ターゲットグループが AZs 間で同じ数のターゲットを持っていることを確認してください。

その他のリソース

「Application Load Balancer のターゲットグループ」

Application Load Balancer ターゲットグループにターゲットを登録する

[Report columns] (レポート列)

- ステータス
- リージョン
- ロードバランサー名
- Load Balancerのタイプ
- ターゲットグループ ARN (ARN)
- AZs 間での登録済みターゲットの違い
- 最終更新日時

GWLB - エンドポイント AZ の独立性

説明

Gateway Load Balancer (GWLB) エンドポイントが、別のアベイラビリティーゾーン (AZ) からのルート送信先として設定されているかどうかを確認します。

Gateway Load Balancer エンドポイントは、検査のためにネットワークトラフィックを Gateway Load Balancer の背後にあるファイアウォールアプライアンスに転送します。各 Gateway Load Balancer エンドポイントは、指定された AZ 内で動作し、その AZ でのみ冗長性が構築されます。したがって、特定の AZ のすべてのリソースは、同じ AZ の Gateway Load Balancer エンドポイントを使用する必要があります。これにより、Gateway Load Balancer エンドポイントまたはその AZ の潜在的な停止が、別の AZ のリソースに影響を与えなくなります。

チェック ID

528d6f5ee7

アラート条件

- 黄: ある AZ のサブネットからのトラフィックは、別の AZ の Gateway Load Balancer エンドポイントを介してルーティングされています。

- 緑: 1 つの AZ のサブネットからのトラフィックは、同じ AZ の Gateway Load Balancer エンドポイントを介してルーティングされています。

[Recommended Action] (推奨されるアクション)

サブネットの AZ を確認し、同じ AZ の Gateway Load Balancer エンドポイントを介してトラフィックをルーティングするようにルートテーブルを設定します。

AZ に Gateway Load Balancer エンドポイントがない場合は、新しいエンドポイントを作成し、サブネットトラフィックをルーティングします。

異なる AZs のサブネット間で同じルートテーブルが関連付けられている場合は、Gateway Load Balancer エンドポイントと同じ AZ に存在するサブネットにこのルートテーブルを関連付けたままにします。他の AZ のサブネットの場合、別のルートテーブルをこの AZ の Gateway Load Balancer エンドポイントへのルートに関連付けることができます。

Amazon VPC のアーキテクチャ変更のメンテナンスウィンドウを選択するのがベストプラクティスです。

その他のリソース

- アベイラビリティーゾーンの独立性
- Gateway Load Balancer エンドポイントのルーティングを設定する
- AWS Well-Architected Tool - バルクヘッドアーキテクチャを使用して影響範囲を制限する

[Report columns] (レポート列)

- ステータス
- リージョン
- クロス AZ サブネット ID リスト
- Gateway Load Balancer エンドポイント ID
- Gateway Load Balancer エンドポイントサブネット ID
- VPC エンドポイントサブネット AZ
- 最終更新日時

ロードバランサーの最適化

説明

ロードバランサーの設定を確認します。

Elastic Load Balancing を使用するときに Amazon Elastic Compute Cloud (Amazon EC2) の耐障害性のレベルを高めるために、リージョン内の複数のアベイラビリティーゾーンで実行するインスタンスの数を同じにすることをお勧めします。設定されているロードバランサーでは料金が発生するため、コスト最適化チェックとしても機能します。

チェック ID

`iqdCTZKCUp`

アラート条件

- 黄: ロードバランサーは、1 つのアベイラビリティーゾーンで有効になっています。
- 黄: ロードバランサーは、アクティブなインスタンスのないアベイラビリティーゾーン用に有効になっています。
- 黄: ロードバランサーに登録されている Amazon EC2 インスタンスは、アベイラビリティーゾーン全体で不均等に分散されています。(使用中のアベイラビリティーゾーンの最大インスタンス数と最小インスタンス数の差は 1 を超えており、その差は最大数の 20% を超えています)。

[Recommended Action] (推奨されるアクション)

ロードバランサーが、少なくとも 2 つのアベイラビリティーゾーンにおいて、アクティブで正常なインスタンスをポイントしているようにします。詳細については、「Add Availability Zone」(アベイラビリティーゾーンの追加) を参照してください。

ロードバランサーが正常なインスタンスのないアベイラビリティーゾーン用に設定されている場合、またはアベイラビリティーゾーン全体でインスタンスの不均衡がある場合は、すべてのアベイラビリティーゾーンが必要かどうかを判断します。不要なアベイラビリティーゾーンを除外し、残りのアベイラビリティーゾーン全体でインスタンスが均等に分散されるようにします。詳細については、「Remove Availability Zone」(アベイラビリティーゾーンの削除) を参照してください。

その他のリソース

- アベイラビリティーゾーンとリージョン
- ロードバランサーの管理
- Elastic Load Balancing を評価する際のベストプラクティス

[Report columns] (レポート列)

- ステータス
- リージョン
- ロードバランサー名

- ゾーン数
- ゾーン a インスタンス
- ゾーン b インスタンス
- ゾーン c インスタンス
- ゾーン d インスタンス
- ゾーン e インスタンス
- ゾーン f インスタンス
- 理由

NAT ゲートウェイ AZ インディペンデンス

説明

NAT ゲートウェイの設定に、アベイラビリティーゾーン (AZ) インディペンデンスが使用されているかどうかを確認します。

NAT ゲートウェイを使用すると、プライベートサブネット内のリソースは、NAT ゲートウェイの IP アドレスを使用することでサブネット外のサービスに安全に接続でき、招待していないインバウンドトラフィックはすべて拒否されます。各 NAT ゲートウェイは指定されたアベイラビリティーゾーン (AZ) 内で動作し、その AZ 内のみで、冗長性を持って構築されています。そのため、特定の AZ にあるリソースは同一の AZ 内の NAT ゲートウェイを使用する必要があります。これにより、NAT ゲートウェイまたはその AZ が停止したとしても、別の AZ にあるリソースに影響が及ばないようになります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c1dfptbg10
```

アラート条件

- 赤: 1 つの AZ にあるサブネットからのトラフィックが、別の AZ の NATGW を経由してルーティングされています。
- 緑: 1 つの AZ にあるサブネットからのトラフィックが、同じ AZ の NATGW を経由してルーティングされています。

[Recommended Action] (推奨されるアクション)

サブネットの AZ を確認し、同じ AZ 内の NAT ゲートウェイ経由でトラフィックをルーティングします。

AZ に NATGW がない場合は、1 つ作成し、それを介してサブネットトラフィックをルーティングします。

異なる AZ のサブネットに同じルートテーブルが関連付けられている場合は、NAT ゲートウェイと同じ AZ にあるサブネットとこのルートテーブルとの関連付けを維持しておき、別の AZ のサブネットについては、そちらの AZ にある NAT ゲートウェイにルーティングして異なるルートテーブルを関連付けてください。

Amazon VPC のアーキテクチャを変更する場合は、メンテナンスウィンドウ内に実行することをお勧めします。

その他のリソース

- NAT ゲートウェイの作成方法
- さまざまな NAT ゲートウェイのユースケースに合わせてルーティングを設定する方法

[Report columns] (レポート列)

- ステータス
- リージョン
- NAT アベイラビリティゾーン
- NAT ID
- サブネットアベイラビリティーゾーン
- サブネット ID
- ルートテーブル ID
- NAT ARN
- 最終更新日時

Network Firewall エンドポイント AZ の独立性

説明

AWS Network Firewall エンドポイントが別のアベイラビリティーゾーン (AZ) からのルート送信先として設定されているかどうかを確認します。

Network Firewall エンドポイントは、検査のためにネットワークトラフィックを Network Firewall に転送します。各 Network Firewall エンドポイントは、指定された AZ 内で動作し、その AZ でのみ冗長性を使用して構築されます。特定の AZ のリソースは、同じ AZ の Network Firewall エンドポイントを使用する必要があります。これにより、Network Firewall エンドポイントまたはその AZ の潜在的な停止が、別の AZ のリソースに影響を与えなくなります。トラフィック検査のために別の AZ から発信されるネットワークトラフィックには、AZ 間のデータ転送料金が発生します。特定の AZ 内のすべてのリソースが同じ AZ の Network Firewall を使用して、AZ 間のデータ料金が発生しないようにすることがベストプラクティスです。

チェック ID

`7040ea389a`

アラート条件

- 黄: ある AZ のサブネットからのトラフィックは、別の AZ の Network Firewall エンドポイントを介してルーティングされています。
- 緑: 1 つの AZ のサブネットからのトラフィックは、同じ AZ の Network Firewall エンドポイントを介してルーティングされています。

[Recommended Action] (推奨されるアクション)

サブネットの AZ を確認し、同じ AZ の Network Firewall エンドポイントを介してトラフィックをルーティングします。

AZ に Network Firewall エンドポイントがない場合は、新しい Network Firewall を作成し、サブネットトラフィックをルーティングします。

異なる AZs の複数のサブネットに同じルートテーブルが関連付けられている場合は、Network Firewall エンドポイントと同じ AZ に存在するサブネットにこのルートテーブルを関連付けたままにします。他の AZs、別のルートテーブルをその AZ の Network Firewall エンドポイントへのルートに関連付けます。

Amazon VPC のアーキテクチャ変更のメンテナンスウィンドウを選択するのがベストプラクティスです。

その他のリソース

同じ 内のデータ転送 AWS リージョン

データ転送料金について

アベイラビリティーゾーンの独立性

ファイアウォールを実装するための大まかな手順

ファイアウォールの作成

AWS Well-Architected Tool - バルクヘッドアーキテクチャを使用して影響範囲を制限する

[Report columns] (レポート列)

- ステータス
- リージョン
- Network Firewall エンドポイント ID
- Network Firewall Arn
- Network Firewall エンドポイントサブネット
- Network Firewall エンドポイント AZ
- クロス AZ サブネットリスト
- 最終更新日時

Network Firewall マルチ AZ

説明

Network Firewall がファイアウォールエンドポイントに複数のアベイラビリティーゾーン (AZ) を使用するように設定されているかどうかを確認します。

AZ は、他のゾーンでの障害から隔離された個別の場所です。Network Firewall エンドポイントが 1 つの AZ にのみデプロイされている場合、単一障害点になり、トラフィック検査に Network Firewall を使用すると、他の AZs のワークロードが損なわれる可能性があります。ワークロードの可用性を向上させるために、同じリージョン内の複数の AZs に Network Firewall を設定するのがベストプラクティスです。

チェック ID

`c2vlfg0gqd`

アラート条件

- 黄: Network Firewall エンドポイントは 1 AZ にデプロイされます。
- 緑: Network Firewall エンドポイントは、少なくとも 2 つの AZs。

[Recommended Action] (推奨されるアクション)

Network Firewall が、本番ワークロード用に少なくとも 2 つの AZs で設定されていることを確認します。

その他のリソース

の VPC サブネット設定AWS Network Firewall

ファイアウォールの作成

アベイラビリティーゾーン

AWS Well-Architected Tool - ワークロードを複数の場所にデプロイする

共有サービス VPC 内のアプライアンス

[Report columns] (レポート列)

- ステータス
- リージョン
- Network Firewall Arn
- VPC Id
- Network Firewall サブネット
- Network Firewall サブネット AZs
- 最終更新日時

Network Load Balancer のクロスロードバランシング

説明

クロスゾーンロードバランシングが Network Load Balancer に対して有効になっているかどうかを確認します。

クロスゾーンロードバランシングは、異なるアベイラビリティーゾーンのインスタンス間で受信トラフィックを均等に分散させるのに役立ちます。これにより、ロードバランサーがすべてのト

ラフィックを同じアベイラビリティーゾーン内のインスタンスにルーティングし、トラフィックの分散が不均一になり、過負荷になるおそれを予防できます。また、この機能は、1 つのアベイラビリティーゾーンに障害が発生した場合に、他のアベイラビリティーゾーンの正常なインスタンスにトラフィックを自動的にルーティングするので、アプリケーションの信頼性にも役立ちます。

詳細については、「クロスゾーン負荷分散」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz105`

ソース

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

アラート条件

- 黄: Network Load Balancer でクロスゾーンロードバランシングが有効になっていません。

[Recommended Action] (推奨されるアクション)

クロスゾーンロードバランシングが Network Load Balancer に対して有効になっていることを確認します。

その他のリソース

クロスゾーン負荷分散 (Network Load Balancer)

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール

- 入力パラメータ
- 最終更新日時

NLB - プライベートサブネット内のインターネット向けリソース

説明

インターネット向け Network Load Balancer (NLB) にプライベートサブネットが設定されているかどうかを確認します。トラフィックを受信するには、インターネット向け Network Load Balancer (NLB) をパブリックサブネットで設定する必要があります。パブリックサブネットは、インターネットゲートウェイへの直接ルートを持つサブネットとして定義されます。サブネットがプライベートとして設定されている場合、アベイラビリティーゾーン (AZ) はトラフィックを受信しないため、可用性の問題が発生する可能性があります。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dfpnchv4`

アラート条件

赤: NLB は 1 つ以上のプライベートサブネットで設定されています

緑: インターネット向け NLB 用にプライベートサブネットが設定されていません

[Recommended Action] (推奨されるアクション)

インターネット向けロードバランサーで設定されたサブネットがパブリックであることを確認します。パブリックサブネットは、インターネットゲートウェイへの直接ルートを持つサブネットとして定義されます。次のいずれかのオプションを使用します。

- 新しいロードバランサーを作成し、インターネットゲートウェイへの直接ルートを持つ別のサブネットを選択します。

- 現在ロードバランサーにアタッチされているサブネットをプライベートからパブリックに変更します。これを行うには、ルートテーブルを変更し、インターネットゲートウェイを関連付けます。

その他のリソース

- ロードバランサーとリスナーを設定する
- VPC のサブネット
- ゲートウェイをルートテーブルに関連付ける

[Report columns] (レポート列)

- ステータス
- リージョン
- NLB Arn
- NLB の名前
- サブネット ID
- NLB スキーム
- サブネットタイプ
- 最終更新日時

NLB マルチ AZ

説明

Network Load Balancer が複数のアベイラビリティーゾーン (AZ) を使用するように設定されているかどうかを確認します。AZ は、他のゾーンの障害から隔離された独立した場所です。同じリージョンの複数の AZ にロードバランサーを設定すると、ワークロードの可用性が向上します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

c1dfprch09

アラート条件

黄色: 1 つの AZ に NLB があります。

緑: 2 つ以上の AZ に NLB があります。

[Recommended Action] (推奨されるアクション)

ロードバランサーが、少なくとも 2 つのアベイラビリティーゾーンで設定されているようにします。

その他のリソース

詳細については、次のドキュメントを参照してください。

- アベイラビリティーゾーンhttps://docs.aws.amazon.com/elasticloadbalancing/latest/network/network-load-balancers.html#availability-zones
- AWS Well-Architected - ワークロードを複数の場所にデプロイする
- リージョンとアベイラビリティーゾーン

[Report columns] (レポート列)

- ステータス
- リージョン
- AZ の数
- NLB ARN
- NLB の名前
- 最終更新日時

Incident Manager レプリケーションセット AWS リージョン 内の の数

説明

Incident Manager レプリケーションセットの設定で、リージョンのフェイルオーバーとレスポンスをサポートするために複数の AWS リージョン が使用されていることを確認します。CloudWatch アラームまたは EventBridge イベントによって作成されたインシデントの場合、Incident Manager はアラームまたはイベントルール AWS リージョン と同じ にインシデントを作成します。そのリージョンで Incident Manager が一時的に使用不能な場合、システムは、レ

プリケーションセット内にある別のリージョンにインシデントを作成しようとします。Incident Manager が使用不能で、レプリケーションセットに含まれるリージョンが 1 つだけの場合、システムはインシデントレコードの作成に失敗します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`cIdfp1js9r`

アラート条件

- 緑: レプリケーションセットには複数のリージョンが含まれています。
- 黄色: レプリケーションセットには 1 つのリージョンが含まれています。

[Recommended Action] (推奨されるアクション)

レプリケーションセットに 1 つ以上のリージョンを追加します。

その他のリソース

詳細については、「リージョン間のインシデント管理」を参照してください。

[Report columns] (レポート列)

- ステータス
- マルチリージョン
- レプリケーションセット
- 最終更新日時

シングル AZ アプリケーションチェック

説明

単一のアベイラビリティーゾーン (AZ) 経由でネットワークの送信トラフィックがルーティングされているかをチェックします。

AZ は口ケーションとして独立しており、他のゾーンの障害からは隔離されています。サービスを複数の AZ に分散させることで、AZ の障害が影響を及ぼす範囲を限定できます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dfptbg11`

アラート条件

- 黄色: 観測されるネットワークの送信パターンによっては、アプリケーションをデプロイできる AZ は 1 つのみです。これが当てはまり、またアプリケーションに高い可用性が必要な場合は、アプリケーションリソースをプロビジョニングし、複数のアベイラビリティーゾーンを利用するようにネットワークフローを実装することをお勧めします。

[Recommended Action] (推奨されるアクション)

アプリケーションで高い可用性が必要な場合は、可用性を高めるマルチ AZ アーキテクチャの実装を検討してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- VPC ID
- 最終更新日時

複数の AZ の VPC インターフェイスエンドポイントネットワークインターフェイス

説明

AWS PrivateLink VPC インターフェイスエンドポイントが複数のアベイラビリティーゾーン (AZ) を使用するように設定されているかどうかを確認します。AZ は、他のゾーンの障害から隔離さ

れた独立した場所です。これにより、同じ AWS リージョン内の AZs 間の低コストで低レイテンシーのネットワーク接続がサポートされます。インターフェイスエンドポイントの作成時に複数のアベイラビリティーゾーン内のサブネットを選択すると、単一障害点からアプリケーションを保護できます。

> **Note**
>
> 現在、このチェックにはインターフェースエンドポイントのみが含まれています。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c1dfprch10`

アラート条件

黄色: 単一の AZ に VPC エンドポイントがあります。

緑: 少なくとも 2 つの AZ に VPC エンドポイントがあります。

[Recommended Action] (推奨されるアクション)

VPC インターフェイスのエンドポイントが、少なくとも 2 つのアベイラビリティーゾーンで設定されているようにします。

その他のリソース

詳細については、次のドキュメントを参照してください。

- インターフェイス VPC エンドポイント AWS のサービス を使用して にアクセスする
- ネットワークインターフェイスのプライベート IP アドレス
- AWS PrivateLink の概念

- リージョンとアベイラビリティーゾーン

[Report columns] (レポート列)

- ステータス
- リージョン
- VPC エンドポイント ID
- はマルチ AZ
- 最終更新日時

VPN トンネルの冗長性

説明

Site-to-Site VPNs ごとにアクティブなトンネルの数を確認します。

1 つの VPN には、常に 2 つのトンネルが設定されている必要があります。これにより、 AWS エンドポイントでのデバイスの障害や計画的なメンテナンスの場合に冗長性が得られます。一部のハードウェアでは、一度に 1 つのトンネルだけがアクティブになります。VPN にアクティブなトンネルがない場合、その VPN の料金が引き続き適用される場合があります。詳細については、「AWS Site-to-Site VPN ユーザーガイド」を参照してください。

チェック ID

`S45wrEXrLz`

アラート条件

- 黄: VPN にはアクティブなトンネルが 1 つあります (これは一部のハードウェアでは正常です)。
- 黄: VPN にはアクティブなトンネルがありません。

[Recommended Action] (推奨されるアクション)

VPN 接続用に 2 つのトンネルが設定されていること、およびハードウェアがサポートしている場合は両方ともアクティブであることを確認してください。VPN 接続が不要になった場合には、料金の発生を回避するために、それを削除することができます。詳細については、「カスタマーゲートウェイデバイス」またはSite-to-Site VPN 接続の削除」を参照してください。

その他のリソース

- AWS Site-to-Site VPN ユーザーガイド
- ターゲットゲートウェイを作成する

[Report columns] (レポート列)

- ステータス
- リージョン
- VPN ID
- VPC
- 仮想プライベートゲートウェイ
- カスタマーゲートウェイ
- アクティブなトンネル
- 理由

ActiveMQ アベイラビリティーゾーンの冗長性

説明

Amazon MQ for ActiveMQ ブローカーが、複数のアベイラビリティーゾーンにあるアクティブ/スタンバイブローカーで高可用性を実現するように設定されていることを確認します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c1t3k8mqv1`

アラート条件

- 黄: Amazon MQ for ActiveMQ ブローカーが単一のアベイラビリティーゾーンに設定されています。

  緑: Amazon MQ for ActiveMQ ブローカーが少なくとも 2 つのアベイラビリティーゾーンに設定されています。

[Recommended Action] (推奨されるアクション)

アクティブ/スタンバイデプロイモードで新しいブローカーを作成します。

その他のリソース

- ActiveMQ ブローカーの作成

[Report columns] (レポート列)

- ステータス
- リージョン
- ActiveMQ ブローカー ID
- ブローカーエンジンタイプ
- デプロイモード
- 最終更新日時

RabbitMQ アベイラビリティーゾーンの冗長性

説明

Amazon MQ for RabbitMQ ブローカーが、複数のアベイラビリティーゾーンにあるクラスターで高可用性を実現するように設定されていることを確認します。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c1t3k8mqv2`

アラート条件

- 黄: Amazon MQ for RabbitMQ ブローカーが単一のアベイラビリティーゾーンに設定されています。

緑: Amazon MQ for RabbitMQ ブローカーが複数のアベイラビリティーゾーンに設定されています。

[Recommended Action] (推奨されるアクション)

クラスターデプロイモードで新しいブローカーを作成します。

その他のリソース

- RabbitMQ ブローカーの作成

[Report columns] (レポート列)

- ステータス
- リージョン
- RabbitMQ ブローカーID
- ブローカーエンジンタイプ
- デプロイモード
- 最終更新日時

サービス制限

サービス制限 (クォータとも呼ばれます) カテゴリについては、次のチェックを参照してください。

このカテゴリのすべてのチェックには、次の説明があります。

アラート条件

- 黄: 制限の 80% に達しました。
- 赤: 制限の 100% に達しました。
- Blue: 1 Trusted Advisor つ以上の の使用率または制限を取得できませんでした AWS リージョン。

[Recommended Action] (推奨されるアクション)

サービス制限を超えることが予想される場合は、Service Quotas コンソールから直接引き上げをリクエストしてください。Service Quotas がまだサービスをサポートしていない場合は、サポートセンターでサポートケースを開くことができます。

[Report columns] (レポート列)

- ステータス

- サービス
- リージョン
- 制限量
- 現在の使用状況

> **Note**
>
> - 値はスナップショットに基づいているため、現在の使用状況とは異なる場合があります。クォータおよび使用状況データは、変更が反映されるまでに最大 24 時間かかる場合があります。クォータが最近増加された場合、クォータを超える使用率が一時的に表示される場合があります。

チェック名

- Auto Scaling グループ
- Auto Scaling の起動設定
- CloudFormation スタック
- DynamoDB の読み込みキャパシティー
- DynamoDB 書き込みキャパシティー
- EBS アクティブなスナップショット
- EBS Cold HDD (sc1) ボリュームストレージ
- EBS 汎用 SSD (gp2) ボリュームストレージ
- EBS 汎用 SSD (gp3) ボリュームストレージ
- EBS マグネティック (スタンダードボリュームストレージ)
- EBS プロビジョンド IOPS SSD (io1) ボリューム集計 IOPS
- EBS プロビジョンド IOPS SSD (io1 ボリュームのストレージ)
- EBS プロビジョンド IOPS SSD (io2 ボリュームのストレージ)
- EBS スループット最適化 HDD (st1) ボリュームストレージ
- EC2 オンデマンドインスタンス
- EC2 リザーブドインスタンスのリース
- EC2-Classic Elastic IP アドレス

- EC2-VPC Elastic IP アドレス
- ELB Application Load Balancer
- ELB Classic Load Balancer
- ELB Network Load Balancer
- IAM グループ
- IAM インスタンスプロファイル
- IAM ポリシー
- IAM ロール
- IAM サーバー証明書
- IAM ユーザー
- Kinesis リージョンあたりのシャード
- Lambda コードストレージの使用状況
- RDS クラスターパラメータグループ
- RDS クラスターロール
- RDS クラスター
- RDS DB インスタンス
- RDS DB 手動スナップショット
- RDS DB パラメータグループ
- RDS DB セキュリティグループ
- RDS イベントサブスクリプション
- RDS セキュリティグループあたりの最大認証数
- RDS オプショングループ
- RDS マスターあたりのリードレプリカ
- RDS リザーブドインスタンス
- RDS サブネットグループ
- RDS サブネットグループあたりのサブネット
- RDS 合計ストレージクォータ
- Route 53 ホストゾーン
- Route 53 最大ヘルスチェック数

- Route 53 再利用可能な委託セット
- Route 53 トラフィックポリシー
- Route 53 トラフィックポリシーのインスタンス
- SES 日次送信クォータ
- VPC
- VPC インターネットゲートウェイ

Auto Scaling グループ

説明

Auto Scaling グループのクォータの 80% を超える使用状況を確認します。

チェック ID

`fW7HH0l7J9`

その他のリソース

Auto Scaling クォータ

Auto Scaling の起動設定

説明

Auto Scaling 起動設定クォータの 80% を超える使用状況を確認します。

チェック ID

`aW7HH0l7J9`

その他のリソース

Auto Scaling クォータ

CloudFormation スタック

説明

CloudFormation スタッククォータの 80% を超える使用状況を確認します。

チェック ID

gW7HH0l7J9

その他のリソース

AWS CloudFormation クォータ

DynamoDB の読み込みキャパシティー

説明

AWS アカウントあたりの読み込みで DynamoDB プロビジョニングされたスループット制限の 80% を超える使用状況をチェックします。

チェック ID

6gtQddfEw6

その他のリソース

DynamoDB クォータ

DynamoDB 書き込みキャパシティー

説明

AWS アカウントあたりの書き込みで DynamoDB プロビジョニングされたスループット制限の 80% を超える使用状況をチェックします。

チェック ID

c5ftjdfkMr

その他のリソース

DynamoDB クォータ

EBS アクティブなスナップショット

説明

EBS のアクティブなスナップショットクォータの 80% を超える使用状況を確認します。

チェック ID

eI7KK0l7J9

その他のリソース

Amazon EBS の制限事項

EBS Cold HDD (sc1) ボリュームストレージ

説明

EBS Cold HDD (sc1) ボリュームのストレージクォータの 80% を超える使用状況を確認します。

チェック ID

gH5CC0e3J9

その他のリソース

Amazon EBS の制限事項

EBS 汎用 SSD (gp2) ボリュームストレージ

説明

EBS 汎用 SSD (gp2) ボリュームストレージクォータの 80% を超える使用状況を確認します。

チェック ID

dH7RR0l6J9

その他のリソース

Amazon EBS の制限事項

EBS 汎用 SSD (gp3) ボリュームストレージ

説明

EBS 汎用 SSD (gp3) ボリュームストレージクォータの 80% を超える使用状況を確認します。

チェック ID

dH7RR0l6J3

その他のリソース

Amazon EBS の制限事項

EBS マグネティック (スタンダードボリュームストレージ)

説明

EBS マグネティック(スタンダード) ボリュームストレージクォータの 80% を超える使用状況を確認します。

チェック ID

cG7HH0l7J9

その他のリソース

Amazon EBS の制限事項

EBS プロビジョンド IOPS SSD (io1) ボリューム集計 IOPS

説明

EBS プロビジョンド IOPS SSD (io1) ボリュームの集計 IOPS クォータの 80% を超える使用状況をチェックします。

チェック ID

tV7YY0l7J9

その他のリソース

Amazon EBS の制限事項

EBS プロビジョンド IOPS SSD (io1 ボリュームのストレージ)

説明

EBS プロビジョンド IOPS SSD (io1) ボリュームのストレージクォータの 80% を超える使用状況を確認します。

チェック ID

gI7MM0l7J9

その他のリソース

Amazon EBS の制限事項

EBS プロビジョンド IOPS SSD (io2 ボリュームのストレージ)

説明

EBS プロビジョンド IOPS SSD (io2) ボリュームのストレージクォータの 80% を超える使用状況を確認します。

チェック ID

gI7MM0l7J2

その他のリソース

Amazon EBS の制限事項

EBS スループット最適化 HDD (st1) ボリュームストレージ

説明

EBS スループット最適化 HDD (st1) ボリュームストレージクォータの 80% を超える使用状況を確認します。

チェック ID

wH7DD0l3J9

その他のリソース

Amazon EBS の制限事項

EC2 オンデマンドインスタンス

説明

EC2 オンデマンドインスタンスのクォータの 80% を超える使用状況を確認します。

チェック ID

0Xc6LMYG8P

その他のリソース

Amazon EC2 のクォータ

EC2 リザーブドインスタンスのリース

説明

EC2 リザーブドインスタンスのリースクォータの 80% を超える使用状況を確認します。

チェック ID

`iH7PP0l7J9`

その他のリソース

Amazon EC2 のクォータ

EC2-Classic Elastic IP アドレス

説明

EC2-Classic Elastic IP アドレスクォータの 80% を超える使用状況を確認します。

チェック ID

`aW9HH0l8J6`

その他のリソース

Amazon EC2 のクォータ

EC2-VPC Elastic IP アドレス

説明

EC2-VPC Elastic IP アドレスクォータの 80% を超える使用状況を確認します。

チェック ID

`lN7RR0l7J9`

その他のリソース

VPC の Elastic IP クォータ

ELB Application Load Balancer

説明

ELB Application Load Balancer クォータの 80% を超える使用状況を確認します。

チェック ID

EM8b3yLRTr

その他のリソース

Elastic Load Balancing のクォータ

ELB Classic Load Balancer

説明

ELB Classic Load Balancer クォータの 80% を超える使用状況を確認します。

チェック ID

iK7000l7J9

その他のリソース

Elastic Load Balancing のクォータ

ELB Network Load Balancer

説明

ELB Network Load Balancer クォータの 80% を超える使用状況を確認します。

チェック ID

8wIqYSt25K

その他のリソース

Elastic Load Balancing のクォータ

IAM グループ

説明

IAM グループクォータの 80% を超える使用状況を確認します。

チェック ID

sU7XX0l7J9

その他のリソース

IAM クォータ

IAM インスタンスプロファイル

説明

IAM インスタンスプロファイルのクォータの 80% を超える使用状況を確認します。

チェック ID

n07SS0l7J9

その他のリソース

IAM クォータ

IAM ポリシー

説明

IAM ポリシークォータの 80% を超える使用状況を確認します。

チェック ID

pR7UU0l7J9

その他のリソース

IAM クォータ

IAM ロール

説明

IAM ロールクォータの 80% を超える使用状況を確認します。

チェック ID

oQ7TT0l7J9

その他のリソース

IAM クォータ

IAM サーバー証明書

説明

IAMサーバー証明書クォータの 80% を超える使用状況を確認します。

チェック ID

rT7WW0l7J9

その他のリソース

IAM クォータ

IAM ユーザー

説明

IAM ユーザークォータの 80% を超える使用状況を確認します。

チェック ID

qS7VV0l7J9

その他のリソース

IAM クォータ

Kinesis リージョンあたりのシャード

説明

Kinesis リージョンあたりのシャードクォータの 80% を超える使用状況を確認します。

チェック ID

bW7HH0l7J9

その他のリソース

Kinesis クォータ

Lambda コードストレージの使用状況

説明

アカウント制限の 80% を超えるコードストレージ使用状況がないかチェックします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c1dfprch07

アラート条件

- 黄: 制限の 80% に達しました。

[Recommended Action] (推奨されるアクション)

使用されていない Lambda 関数またはバージョンを特定して削除し、そのリージョンのアカウントのコードストレージを解放してください。追加のストレージが必要な場合は、サポートセンターでのサポートケースを作成してください。サービス制限を超えることが予想される場合は、Service Quotas コンソールから直接引き上げをリクエストしてください。Service Quotas が

まだサービスをサポートしていない場合は、サポートセンターでサポートケースを開くことができます。

その他のリソース

- Lambda コードストレージの使用状況

[Report columns] (レポート列)

- ステータス
- リージョン
- このリソースの修飾関数 ARN。
- 小数点以下 2 桁のメガバイト単位の関数コードストレージ使用状況。
- 関数内のバージョン数
- 最終更新日時

RDS クラスターパラメータグループ

説明

RDS クラスターパラメータグループクォータの 80% を超える使用状況を確認します。

チェック ID

`jtlIMO3qZM`

その他のリソース

Amazon RDS クォータ

RDS クラスターロール

説明

RDS クラスターロールクォータの 80% を超える使用状況を確認します。

チェック ID

`7fuccf1Mx7`

その他のリソース

Amazon RDS クォータ

RDS クラスター

説明

RDS クラスタークォータの 80% を超える使用状況を確認します。

チェック ID

gjqMBn6pjz

その他のリソース

Amazon RDS クォータ

RDS DB インスタンス

説明

RDS DB インスタンスクォータの 80% を超える使用状況を確認します。

チェック ID

XG0aXHpIEt

その他のリソース

Amazon RDS クォータ

RDS DB 手動スナップショット

説明

RDS DB 手動スナップショットクォータの 80% を超える使用状況を確認します。

チェック ID

dV84wpqRUs

その他のリソース

Amazon RDS クォータ

RDS DB パラメータグループ

説明

RDS DB パラメータグループクォータの 80% を超える使用状況を確認します。

チェック ID

`jEECYg2YVU`

その他のリソース

Amazon RDS クォータ

RDS DB セキュリティグループ

説明

RDS DB セキュリティグループクォータの 80% を超える使用状況を確認します。

チェック ID

`gfZAn3W7wl`

その他のリソース

Amazon RDS クォータ

RDS イベントサブスクリプション

説明

RDS イベントサブスクリプションクォータの 80% を超える使用状況を確認します。

チェック ID

`keAhfbH5yb`

その他のリソース

Amazon RDS クォータ

RDS セキュリティグループあたりの最大認証数

説明

RDS セキュリティグループクォータあたりの最大認証数の 80% を超える使用状況を確認します。

チェック ID

dBkuNCvqn5

その他のリソース

Amazon RDS クォータ

RDS オプショングループ

説明

RDS オプショングループクォータの 80% を超える使用状況を確認します。

チェック ID

3Njm0DJQO9

その他のリソース

Amazon RDS クォータ

RDS マスターあたりのリードレプリカ

説明

マスタークォータごとに RDS リードレプリカの 80% を超える使用状況を確認します。

チェック ID

pYW8UkYz2w

その他のリソース

Amazon RDS クォータ

RDS リザーブドインスタンス

説明

RDS リザーブドインスタンスクォータの 80% を超える使用状況を確認します。

チェック ID

UUDv0a5r34

その他のリソース

Amazon RDS クォータ

RDS サブネットグループ

説明

RDS サブネットグループクォータの 80% を超える使用状況を確認します。

チェック ID

dYWBaXaaMM

その他のリソース

Amazon RDS クォータ

RDS サブネットグループあたりのサブネット

説明

RDS のサブネットグループクォータあたりのサブネット の 80% を超える使用状況を確認します。

チェック ID

jEhCtdJK0Y

その他のリソース

Amazon RDS クォータ

RDS 合計ストレージクォータ

説明

RDS 合計ストレージクォータの 80% を超える使用状況を確認します。

チェック ID

`P1jhKWEmLa`

その他のリソース

Amazon RDS クォータ

Route 53 ホストゾーン

説明

アカウントあたりの Route 53 ホストゾーンのクォータの 80% を超える使用状況を確認します。

チェック ID

`dx3xfcdfMr`

その他のリソース

Route 53 のクォータ

Route 53 最大ヘルスチェック数

説明

アカウントあたりの Route 53 ヘルスチェック数クォータの 80% を超える使用状況を確認します。

チェック ID

`ru4xfcdfMr`

その他のリソース

Route 53 のクォータ

Route 53 再利用可能な委託セット

説明

アカウントあたりの Route 53 再利用可能な委託セットクォータの 80% を超える使用状況を確認します。

チェック ID

`ty3xfcdfMr`

その他のリソース

Route 53 のクォータ

Route 53 トラフィックポリシー

説明

アカウントあたりの Route 53 トラフィックポリシークォータの 80% を超える使用状況を確認します。

チェック ID

`dx3xfbjfMr`

その他のリソース

Route 53 のクォータ

Route 53 トラフィックポリシーのインスタンス

説明

アカウントあたりの Route 53 トラフィックポリシーインスタンスクォータの 80% を超える使用状況を確認します。

チェック ID

`dx8afcdfMr`

その他のリソース

Route 53 のクォータ

SES 日次送信クォータ

説明

Amazon SES 日次送信クォータの 80% を超える使用状況を確認します。

チェック ID

hJ7NN0l7J9

その他のリソース

Amazon SES のクォータ

VPC

説明

VPC クォータの 80% を超える使用状況を確認します。

チェック ID

jL7PP0l7J9

その他のリソース

VPC クォータ

VPC インターネットゲートウェイ

説明

VPC インターネットゲートウェイクォータの 80% を超える使用状況を確認します。

チェック ID

kM7QQ0l7J9

その他のリソース

VPC クォータ

運用上の優秀性

運用上の優秀性のカテゴリに次のチェックを使用できます。

チェック名

- Amazon API Gateway が実行ログを記録しない
- X-Ray トレースが有効になっていない Amazon API Gateway の REST API
- Amazon CloudFront のアクセスログの設定
- Amazon CloudWatch アラームアクションが無効になっている
- によって管理されていない Amazon EC2 インスタンス AWS Systems Manager
- タグの不変性が無効になっている Amazon ECR リポジトリ
- Container Insights が無効の Amazon ECS クラスター
- Amazon ECS タスクのログ記録が有効になっていない
- CloudWatch のログ記録が設定されていない Amazon OpenSearch Service
- 異種のパラメータグループを持つクラスター内の Amazon RDS DB インスタンス
- Amazon RDS 拡張モニタリングは無効になっています
- Amazon RDS Performance Insights は無効になっています
- Amazon RDS の track_counts パラメータは無効になっています
- Amazon Redshift クラスター監査ログ
- Amazon S3 アクセスログの有効化
- Amazon S3 でイベント通知が有効になっていない
- Amazon SNS トピックがメッセージ配信ステータスのログを記録しない
- フローログがない Amazon VPC
- アクセスログが有効になっていない Application Load Balancer および Classic Load Balancer
- AWS CloudFormation スタック通知
- AWS CloudTrail S3 バケット内のオブジェクトのデータイベントのログ記録
- AWS CodeBuild プロジェクトのログ記録
- AWS CodeDeploy 自動ロールバックとモニターの有効化
- AWS CodeDeploy Lambda はall-at-onceデプロイ設定を使用しています
- AWS Elastic Beanstalk 拡張ヘルスレポートが設定されていない
- AWS Elastic Beanstalk マネージドプラットフォームの更新が無効になっている
- AWS Fargate プラットフォームバージョンが最新ではない
- AWS Systems Manager 非準拠ステータスのステートマネージャーの関連付け

- CloudTrail 証跡が、Amazon CloudWatch Logs で設定されていない
- ロードバランサーの Elastic Load Balancing 削除保護が有効になっていない
- RDS DB クラスター削除保護チェック
- RDS DB インスタンスのマイナーバージョン自動アップグレードチェック

Amazon API Gateway が実行ログを記録しない

説明

Amazon API Gateway で CloudWatch Logs が該当するログ記録レベルでオンになっているかどうかを確認します。

Amazon API Gateway の REST API メソッドまたは WebSocket API ルートの CloudWatch ログ記録を有効にして、API が受信したリクエストの実行ログを CloudWatch Logs に収集します。実行ログに含まれる情報は、API に関連する問題の特定やトラブルシューティングに役立ちます。

ルールの loggingLevel パラメータでログ記録レベル (ERROR、INFO) ID を指定できます AWS Config 。

Amazon API Gateway の CloudWatch ログ記録の詳細については、REST API または WebSocket API ドキュメントを参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz125
```

ソース

```
AWS Config Managed Rule: api-gw-execution-logging-enabled
```

アラート条件

黄: 実行ログを収集する CloudWatch ログ記録の設定が、Amazon API Gateway に該当するログ記録レベルで有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon API Gateway REST API または WebSocket API における実行ログの CloudWatch ログ記録を適切なログ記録レベル (ERROR、INFO) で有効にします。

詳細については、「フローログの作成」を参照してください。

その他のリソース

- API Gateway での CloudWatch による REST API のログの設定
- WebSocket API のログ記録の設定

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

X-Ray トレースが有効になっていない Amazon API Gateway の REST API

説明

Amazon API Gateway REST APIs AWS X-Ray トレースが有効になっているかどうかを確認します。

REST API の X-Ray トレースを有効にして、API Gateway がトレース情報を含む API 呼び出しリクエストをサンプリングできるようにします。これにより、API Gateway REST API を介してダウンストリームサービスに移動するリクエスト AWS X-Ray を で追跡 APIs および分析できます。

詳細については、「X-Ray を使用した REST API へのユーザーリクエストのトレース」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz126`

ソース

`AWS Config Managed Rule: api-gw-xray-enabled`

アラート条件

黄: API Gateway の REST API で X-Ray トレースが有効になっていません。

[Recommended Action] (推奨されるアクション)

API Gateway の REST API で X-Ray トレースを有効にします。

詳細については、「API Gateway REST API AWS X-Ray でのセットアップ APIs」を参照してください。

その他のリソース

- X-Ray を使用した REST API へのユーザーリクエストのトレース
- とは AWS X-Ray

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon CloudFront のアクセスログの設定

説明

Amazon CloudFront ディストリビューションが、Amazon S3 サーバーアクセスログから情報をキャプチャするように設定されているかどうかを確認します。Amazon S3 サーバーのアクセスログには、CloudFront が受信するすべてのユーザーリクエストに関する詳細情報が含まれています。

AWS Config ルールの Amazon S3 S3BucketName バケットの名前を調整できます。

詳細については、「標準ログ (アクセスログ) の設定および使用」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz110
```

ソース

```
AWS Config Managed Rule: cloudfront-accesslogs-enabled
```

アラート条件

黄: Amazon CloudFront のアクセスログが有効になっていません。

[Recommended Action] (推奨されるアクション)

CloudFront が受信するすべてのユーザーリクエストに関する詳細情報を取得できるように、CloudFront のアクセスログ記録を有効にしてください。

ディストリビューションを作成または更新するとき、標準ログをオンにできます。

詳細については、「ディストリビューションを作成または更新する場合に指定する値」を参照してください。

その他のリソース

- ディストリビューションを作成または更新する場合に指定する値
- 標準ログ (アクセスログ) の設定および使用

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon CloudWatch アラームアクションが無効になっている

説明

Amazon CloudWatch のアラームアクションが無効状態であるかどうかを確認します。

を使用して AWS CLI 、アラームのアクション機能を有効または無効にできます。または、 AWS SDK を使用してアクション機能をプログラムで無効化または有効化できます。アラームアクション機能がオフになっている場合、CloudWatch はどの状態 (OK、INSUFFICIENT_DATA、ALARM) の定義済みアクションでも実行しません。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz109
```

ソース

```
AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check
```

アラート条件

黄: Amazon CloudWatch のアラームアクションが有効になっていません。どのアラーム状態でもアクションが実行されません。

[Recommended Action] (推奨されるアクション)

テスト目的など、アクションを無効にする正当な理由がない限り、CloudWatch アラームのアクションを有効にしてください。

CloudWatch アラームが必要なくなった場合は、不要なコストの発生を抑えるため削除してください。

詳細については、 AWS CLI 「 コマンドリファレンス」のenable-alarm-actions」および AWS 「 SDK for Go API リファレンス」の「func (*CloudWatch) EnableAlarmActions」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

によって管理されていない Amazon EC2 インスタンス AWS Systems Manager

説明

アカウント内の Amazon EC2 インスタンスが によって管理されているかどうかを確認します AWS Systems Manager。

Systems Manager は、Amazon EC2 インスタンスと OS 設定の現在の状態を把握し、制御するのに役立ちます。Systems Manager を使用すると、インスタンスのフリートに関するソフトウェア設定とインベントリ情報 (インスタンスにインストールされているソフトウェアを含む) を収集できます。これにより、詳細なシステム設定、OS パッチレベル、アプリケーション設定、デプロイに関するその他の詳細を追跡することができます。

詳細については、「Systems Manager の EC2 インスタンスのセットアップ」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz145`

ソース

`AWS Config Managed Rule: ec2-instance-managed-by-systems-manager`

アラート条件

黄: Amazon EC2 インスタンスが Systems Manager によって管理されていません。

[Recommended Action] (推奨されるアクション)

Amazon EC2 インスタンス が Systems Manager によって管理されるように設定します。

このチェックは、 Trusted Advisor コンソールのビューから除外することはできません。

詳細については、「Systems Manager で EC2 インスタンスがマネージドノードとして表示されない、または 「接続が失われました」というステータスが表示されるのはなぜですか?」を参照してください。

その他のリソース

Systems Manager の EC2 インスタンスのセットアップ

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ

- 最終更新日時

タグの不変性が無効になっている Amazon ECR リポジトリ

説明

プライベート Amazon ECR リポジトリでイメージタグの不変性が有効になっているかどうかを確認します。

プライベート Amazon ECR リポジトリのイメージタグの不変性を有効にして、イメージタグが上書きされるのを防ぎます。これにより、イメージを追跡して一意に識別する信頼できるメカニズムとして、説明タグを使用できます。例えば、イメージタグの不変性がオンになっている場合、ユーザーはイメージタグを使用して、デプロイされたイメージバージョンと、そのイメージを生成したビルドを確実に関連付けることができます。

詳細については、「イメージタグの変更可能性」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz129
```

ソース

```
AWS Config Managed Rule: ecr-private-tag-immutability-enabled
```

アラート条件

黄: Amazon ECR プライベートリポジトリでタグの不変性が有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon ECR プライベートリポジトリでイメージタグの不変性を有効にしてください。

詳細については、「イメージタグの変更可能性」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Container Insights が無効の Amazon ECS クラスター

説明

Amazon ECS クラスターで Amazon CloudWatch Container Insights が有効になっているかどうかを確認します。

CloudWatch Container Insights は、コンテナ化されたアプリケーションとマイクロサービスのメトリクスとログを収集、集約、要約します。このメトリクスには、CPU、メモリ、ディスク、ネットワークなどのリソース使用率が含まれます。

詳細については、「Amazon ECS CloudWatch コンテナインサイト」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz173
```

ソース

```
AWS Config Managed Rule: ecs-container-insights-enabled
```

アラート条件

黄: Amazon ECS クラスターで Container Insights が有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon ECS クラスターで CloudWatch Container Insights を有効にしてください。

詳細については、「Container Insights の使用」を参照してください。

その他のリソース

Amazon ECS CloudWatch コンテナインサイト

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon ECS タスクの口グ記録が有効になっていない

説明

アクティブな Amazon ECS タスク定義に、口グ設定がセットアップされているかどうかを確認します。

Amazon ECS タスク定義の口グ設定を確認することで、コンテナによって生成された口グが適切に設定され、保存されていることを確認することができます。これにより、より迅速に問題を特定してトラブルシューティングすることができ、パフォーマンスを最適化して、コンプライアンス要件を満たすことができます。

デフォルトでは、コンテナをローカルに実行した場合、キャプチャされる口グは通常インタラクティブターミナルにコマンド出力を表示します。awslogs ドライバーは、これらの口グを Docker から Amazon CloudWatch Logs に渡します。

詳細については、「awslogs 口グドライバーを使用する」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz175`

ソース

`AWS Config Managed Rule: ecs-task-definition-log-configuration`

アラート条件

黄: Amazon ECS のタスク定義にログ設定がありません。

[Recommended Action] (推奨されるアクション)

CloudWatch Logs または別のログ記録ドライバーにログ情報を送信するために、コンテナ定義でログドライバー設定を指定することを検討してください。

詳細については、「LogConfiguration」を参照してください。

その他のリソース

CloudWatch Logs または別のログ記録ドライバーにログ情報を送信するために、コンテナ定義でログドライバー設定を指定することを検討してください。

詳細については、「タスク定義の例」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ

- 最終更新日時

CloudWatch のログ記録が設定されていない Amazon OpenSearch Service

説明

Amazon OpenSearch Service ドメインが、Amazon CloudWatch Logs にログを送信するように設定されているかどうかを確認します。

ログのモニタリングは、OpenSearch Service の信頼性、可用性、パフォーマンスを維持する上で非常に重要です。

検索スローログ、インデックス作成スローログ、およびエラーログは、ワークロードのパフォーマンスや安定性の問題をトラブルシューティングするのに役立ちます。これらのログを有効にしてデータをキャプチャする必要があります。

AWS Config ルールの logTypes パラメータを使用して、フィルタリングするログタイプ (エラー、検索、インデックス) を指定できます。

詳細については、「Amazon OpenSearch Service ドメインのモニタリング」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz184
```

ソース

```
AWS Config Managed Rule: opensearch-logs-to-cloudwatch
```

アラート条件

黄: Amazon OpenSearch Service に Amazon CloudWatch Logs による口グ設定がありません

[Recommended Action] (推奨されるアクション)

CloudWatch Logs にログを発行するように OpenSearch Service ドメインを設定してください。

詳細については、「ログ発行を有効にする (コンソール)」を参照してください。

その他のリソース

- Amazon CloudWatch を用いた OpenSearch クラスターメトリクスのモニタリング

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

異種のパラメータグループを持つクラスター内の Amazon RDS DB インスタンス

説明

DB クラスター内のすべての DB インスタンスが同じ DB パラメータグループを使用することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。

DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt010`

アラート条件

黄色: DB クラスターには、異種のパラメータグループを持つ DB インスタンスがあります。

[Recommended Action] (推奨されるアクション)

DB インスタンスを、DB クラスター内のライターインスタンスに関連付けられた DB パラメータグループに、関連付けます。

その他のリソース

DB クラスター内の DB インスタンスが異なる DB パラメータグループを使用している場合、フェイルオーバー時に動作が一貫しなかったり、DB クラスター内の DB インスタンス間の互換性の問題が発生したりする可能性があります。

詳細については、「パラメータグループの操作」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS 拡張モニタリングは無効になっています

説明

データベースリソースでは拡張モニタリングが有効になっていません。拡張モニタリングにより、モニタリングとトラブルシューティングのためのリアルタイムのオペレーティングシステムメトリクスが提供されます。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt004`

アラート条件

黄色: Amazon RDS リソースでは拡張モニタリングが有効になっていません。

[Recommended Action] (推奨されるアクション)

Enhanced monitoring] を有効にします。

その他のリソース

Amazon RDS 拡張モニタリングにより、DB インスタンスの状態を可視化しやすくします。拡張モニタリングを有効にすることをお勧めします。DB インスタンスで拡張モニタリングオプションを有効にすると、重要なオペレーティングシステムメトリクスとプロセス情報が収集されます。

詳細については、「拡張モニタリングを使用した OS メトリクスのモニタリング」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS Performance Insights は無効になっています

説明

Amazon RDS Performance Insights では、DB インスタンスの負荷をモニタリングし、データベースパフォーマンスの問題の分析と解決をサポートします。Performance Insights を有効にすることをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

c1qf5bt012

アラート条件

黄色: Amazon RDS リソースでは Performance Insights が有効になっていません。

[Recommended Action] (推奨されるアクション)

Performance Insights をオンにします。

その他のリソース

Performance Insights では、アプリケーションのパフォーマンスに影響を与えない軽量なデータ収集方法を使用しています。Performance Insights は、データベースの負荷を迅速に評価することができます。

詳細については、「Amazon RDS での Performance Insights を使用したDB 負荷のモニタリング」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- 推奨値
- エンジン名
- 最終更新日時

Amazon RDS の track_counts パラメータは無効になっています

説明

track_counts パラメータが無効の場合、データベースはデータベースアクティビティ統計を収集しません。自動バキュームでは、これらの統計が正しく機能する必要があります。

track_counts パラメータを 1 に設定することをお勧めします。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

> **Note**
>
> DB インスタンスまたは DB クラスターが停止すると、 で Amazon RDS の推奨事項を Trusted Advisor 3 ~ 5 日間表示できます。5 日後、レコメンデーションは では使用できません Trusted Advisor。推奨事項を表示するには、Amazon RDS コンソールを開いて [推奨事項] を選択します。
> DB インスタンスまたは DB クラスターを削除すると、それらのインスタンスまたはクラスターに関連付けられたレコメンデーションは、 Trusted Advisor または Amazon RDS マネジメントコンソールでは使用できません。

チェック ID

`c1qf5bt027`

アラート条件

黄色: DB パラメータグループの track_counts パラメータは無効になっています。

[Recommended Action] (推奨されるアクション)

track_counts パラメーターを 1 に設定します。

その他のリソース

track_counts パラメータが無効の場合、データベースアクティビティ統計の収集が無効になります。自動バキュームデーモンは、自動バキューム処理と自動分析の対象となるテーブルを識別するために、収集した統計情報を必要とします。

詳細については、PostgreSQL のドキュメント Web サイトで「PostgreSQL のランタイム統計」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース

- パラメータ値
- 推奨値
- 最終更新日時

Amazon Redshift クラスター監査ログ

説明

Amazon Redshift クラスターでデータベース監査ログが有効になっているかどうかを確認します。Amazon Redshift は、データベースの接続とユーザーアクティビティに関する情報を記録します。

AWS Config ルールの bucketNames パラメータで、一致するログ記録 Amazon S3 バケット名を指定できます。

詳細については、「データベース監査ログ作成」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz134
```

ソース

```
AWS Config Managed Rule: redshift-audit-logging-enabled
```

アラート条件

黄: Amazon Redshift クラスターのデータベース監査ログが無効になっています

[Recommended Action] (推奨されるアクション)

Amazon Redshift クラスターのログ記録とモニタリングを有効化してください。

詳細については、「コンソールを使用して監査を設定する」を参照してください。

その他のリソース

Amazon Redshift でのログ作成とモニタリング

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon S3 アクセスログの有効化

説明

Amazon Simple Storage Service バケットのログ記録設定を確認します。

サーバーアクセスログ記録を有効にすると、指定した Amazon S3 バケットに詳細なアクセスログが 1 時間ごとに提供されます。アクセスログには、タイプ、指定されたリソース、処理日時などのリクエストの詳細が含まれます。デフォルトでは、ログは無効化されています。お客様は、セキュリティ監査を実行したり、ユーザーの行動と使用パターンを分析したりするために、アクセスログを有効にする必要があります。

ログ記録が最初にアクティブ化されると、設定は自動的に検証されます。ただし、今後の変更により、ログが失敗する可能性があります。現在、このチェックでは Amazon S3 バケットの書き込みアクセス許可は調べられません。

チェック ID

`c1fd6b96l4`

アラート条件

- 黄: バケットでサーバーアクセスのログ記録が有効になっていません。
- 黄: ターゲットバケットの許可にルートアカウントが含まれていないため、 Trusted Advisor は確認できません。
- 赤: ターゲットバケットが存在しません。

- 赤: ターゲットバケットとソースバケットの所有者が異なります。
- 緑: バケットでサーバーアクセスのログ記録が有効になっていて、ターゲットが存在し、ターゲットに書き込むアクセス許可が存在する

[Recommended Action] (推奨されるアクション)

関連するすべての Amazon S3 バケットのサーバーアクセスログ記録を有効にします。サーバーアクセスログは、バケットのアクセスパターンを理解し、疑わしいアクティビティを調査するために使用できる監査証跡を提供します。該当するすべてのバケットでログ記録を有効にすると、Amazon S3 環境全体のアクセスイベントの可視性が向上します。「Enabling Logging Using the Console」(コンソールを使用してログ記録を有効にする) および「Enabling Logging Programmatically」(プログラムを使用してログ記録を有効にする) を参照してください。

ターゲットバケットの許可にルートアカウントが含まれておらず、 Trusted Advisor にログ記録ステータスを確認させる場合は、ルートアカウントを被付与者として追加します。「Editing Bucket Permissions」(バケット許可の編集) を参照してください。

ターゲットバケットが存在しない場合は、既存のバケットをターゲットとして選択するか、新しいバケットを作成して選択します。「Managing Bucket Logging」(バケットのログ記録の管理) を参照してください。

ターゲットとソースの所有者が異なる場合は、ターゲットバケットを、ソースバケットと同じ所有者を持つバケットに変更します。「Managing Bucket Logging」(バケットのログ記録の管理) を参照してください。

その他のリソース

バケットの使用

サーバーアクセスのログ記録

サーバーアクセスログ形式

ログファイルの削除

[Report columns] (レポート列)

- ステータス
- リージョン
- リソースARN
- バケット名

- ターゲット名
- ターゲットが存在
- 同じ所有者
- 書き込み有効
- 理由
- 最終更新日時

Amazon S3 でイベント通知が有効になっていない

説明

Amazon S3 イベント通知が有効になっているかどうか、目的の送信先またはタイプで正しく設定されているかどうかを確認します。

Amazon S3 イベント通知機能では、S3 バケットで特定のイベントが発生したときに通知を送信します。Amazon S3 はAmazon SQSキュー、Amazon SNS トピック、および AWS Lambda 関数に通知メッセージを送信できます。

AWS Config ルールの destinationArn パラメータと eventTypes パラメータを使用して、目的の宛先とイベントタイプを指定できます。 eventTypes

詳細については、「Amazon S3 イベント通知」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

```
c18d2gz163
```

ソース

```
AWS Config Managed Rule: s3-event-notifications-enabled
```

アラート条件

黄: Amazon S3 でイベント通知が有効になっていないか、目的の送信先またはタイプが設定されていません。

[Recommended Action] (推奨されるアクション)

オブジェクトイベントとバケットイベントに対して Amazon S3 イベント通知を設定します。

詳細については、「Amazon S3 コンソールを使用したイベント通知の有効化と設定」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

Amazon SNS トピックがメッセージ配信ステータスのログを記録しない

説明

Amazon SNS トピックでメッセージ配信ステータスのログ記録が有効になっているかどうかを確認します。

メッセージ配信ステータスのログを記録する Amazon SNS トピックを設定して、運用上のインサイトをより的確に把握できるようにします。例えば、メッセージ配信ログ記録でメッセージが特定の Amazon SNS エンドポイントに配信されたかどうかを検証します。また、エンドポイントから送信された応答を識別するのにも役立ちます。

詳細については、「メッセージの配信ステータスの Amazon SNS アプリケーション属性を使用する」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

`c18d2gz121`

ソース

`AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled`

アラート条件

黄: Amazon SNS トピックのメッセージ配信ステータスログ記録が有効になっていません。

[Recommended Action] (推奨されるアクション)

SNS トピックのメッセージ配信ステータスログ記録を有効にしてください。

詳細については、「AWS Management Console を使用した配信ステータスのログ記録を設定する」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

フローログがない Amazon VPC

説明

Amazon Virtual Private Cloud フローログが VPC に対して作成されているかどうかを確認します。

AWS Config ルールの trafficType パラメータを使用してトラフィックタイプを指定できます。

詳細については、「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz122
```

ソース

```
AWS Config Managed Rule: vpc-flow-logs-enabled
```

アラート条件

黄: VPC に Amazon VPC フローログがありません。

[Recommended Action] (推奨されるアクション)

VPC ごとに VPC フローログを作成してください。

詳細については、「フローログの作成」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

アクセスログが有効になっていない Application Load Balancer および Classic Load Balancer

説明

Application Load Balancer と Classic Load Balancer でアクセスログ記録が有効になっているかどうかを確認します。

Elastic Load Balancing は、ロードバランサーに送信されるリクエストに関する詳細情報をキャプチャしたアクセスログを提供します。各ログには、リクエストを受け取った時刻、クライアントの IP アドレス、レイテンシー、リクエストのパス、サーバーレスポンスなどの情報が含まれます。これらのアクセスログを使用して、トラフィックパターンを分析し、問題のトラブルシューティングを行えます。

アクセスログの作成は、Elastic Load Balancing のオプション機能であり、デフォルトでは無効化されています。ロードバランサーのアクセスログの作成を有効にすると、Elastic Load Balancing はログをキャプチャし、そのログを指定した Amazon S3 バケット内に保存します。

AWS Config ルールの Amazon S3s3BucketNames バケットを指定できます。

詳細については、「Application Load Balancer のアクセスログ」または「Access logs for your Classic Load Balancer」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> Business、Enterprise On-Ramp、または Enterprise Support のお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz167
```

ソース

```
AWS Config Managed Rule: elb-logging-enabled
```

アラート条件

黄: Application Load Balancer または Classic Load Balancer に対して、アクセスログ機能が有効になっていません。

[Recommended Action] (推奨されるアクション)

Application Load Balancer および Classic Load Balancer のアクセスログを有効にしてください。

詳細については、「Application Load Balancer のアクセスログを有効にする」または「Enable access logs for your Classic Load Balancer」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CloudFormation スタック通知

説明

イベントが発生したときに、すべての AWS CloudFormation スタックが Amazon SNS を使用して通知を受信するかどうかを確認します。

AWS Config ルールのパラメータを使用して、特定の Amazon SNS トピック ARNs を検索するようにこのチェックを設定できます。

詳細については、AWS CloudFormation「スタックオプションの設定」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外できます。

チェック ID

c18d2gz111

ソース

AWS Config Managed Rule: cloudformation-stack-notification-check

アラート条件

黄: スタックの Amazon SNS イベント通知はオンになっていません。 AWS CloudFormation

[Recommended Action] (推奨されるアクション)

イベントが発生したときに AWS CloudFormation 、スタックが Amazon SNS を使用して通知を受信していることを確認します。

スタックイベントをモニタリングすることで、 AWS 環境を変更する可能性のある不正なアクションに迅速に対応できます。

その他のリソース

AWS CloudFormation スタックが ROLLBACK_IN_PROGRESS ステータスになったときにメールアラートを受信するにはどうすればよいですか?

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CloudTrail S3 バケット内のオブジェクトのデータイベントの口グ記録

説明

少なくとも 1 つの AWS CloudTrail 証跡がすべての Amazon S3 バケットの Amazon S3 データイベントを口グに記録するかどうかを確認します。

詳細については、「AWS CloudTrailを使用した Amazon S3 API コールの口グ記録」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz166`

ソース

`AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled`

アラート条件

Amazon S3 バケットの黄： AWS CloudTrail イベントログ記録が設定されていません

[Recommended Action] (推奨されるアクション)

Amazon S3 バケットとオブジェクトの CloudTrail イベントログ記録を有効にして、ターゲットバケットへのアクセスリクエストを追跡してください。

詳細については、S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CodeBuild プロジェクトのログ記録

説明

AWS CodeBuild プロジェクト環境がログ記録を使用しているかどうかを確認します。ログ記録オプションは、Amazon CloudWatch Logs 内のログ、指定した Amazon S3 バケットでビルドされたログ、またはその両方のログとすることができます。CodeBuild プロジェクトでログ記録を有効にすると、デバッグや監査など、いくつかのメリットが得られます。

AWS Config ルールで sAmazon S3cloudWatchGroupNamesグループの名前を指定できます。CloudWatch s3BucketNames

詳細については、「 のモニタリング AWS CodeBuild」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz113
```

ソース

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

アラート条件

黄: AWS CodeBuild プロジェクトのログ記録が有効になっていません。

[Recommended Action] (推奨されるアクション)

AWS CodeBuild プロジェクトでログ記録が有効になっていることを確認します。このチェックは、 AWS Trusted Advisor コンソールのビューから除外することはできません。

詳細については、「ログインとモニタリング AWS CodeBuild」を参照してください。

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CodeDeploy 自動ロールバックとモニターの有効化

説明

デプロイグループに、アラームがアタッチされた自動デプロイロールバックとデプロイモニタリングが設定されているかどうかを確認します。デプロイ中に問題が発生した場合、自動的にロールバックされ、アプリケーションは安定した状態を維持します。

詳細については、「Redeploy and roll back a deployment with CodeDeploy」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz114
```

ソース

```
AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled
```

アラート条件

黄: AWS CodeDeploy 自動デプロイのロールバックとデプロイのモニタリングは有効になっていません。

[Recommended Action] (推奨されるアクション)

デプロイが失敗した場合、または指定した監視しきい値に達した場合、自動的にロールバックするように、デプロイグループまたはデプロイを設定してください。

デプロイプロセス中に CPU 使用率、メモリ使用量、ネットワークトラフィックなど、さまざまなメトリクスを監視できるようにアラームを設定します。これらのメトリクスのいずれかが特定のしきい値を超えると、アラームが起動し、デプロイが停止またはロールバックされます。

デプロイグループの自動ロールバックとアラームの設定については、「Configure advanced options for a deployment group」を参照してください。

その他のリソース

What is CodeDeploy?

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS CodeDeploy Lambda はall-at-onceデプロイ設定を使用しています

説明

AWS Lambda コンピューティングプラットフォームの AWS CodeDeploy デプロイグループがall-at-onceデプロイ設定を使用しているかどうかを確認します。

CodeDeploy で Lambda 関数のデプロイが失敗するリスクを減らすには、すべてのトラフィックが元の Lambda 関数から最新の関数に一度に移行されるデフォルトオプションの代わりに、Canary デプロイまたは線形デプロイの設定を使用するのがベストプラクティスです。

詳細については、「Lambda 関数のバージョン」と「デプロイ設定」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz115`

ソース

`AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-disabled`

アラート条件

黄： AWS CodeDeploy Lambda デプロイでは、all-at-onceデプロイ設定を使用して、すべてのトラフィックを更新された Lambda 関数に一度にシフトします。

[Recommended Action] (推奨されるアクション)

Lambda コンピューティングプラットフォームに対して、CodeDeploy デプロイグループの Canary デプロイ設定または線形デプロイ設定を使用してください。

その他のリソース

Deployment configuration

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS Elastic Beanstalk 拡張ヘルスレポートが設定されていない

説明

拡張ヘルスレポート用に AWS Elastic Beanstalk 環境が設定されているかどうかを確認します。

Elastic Beanstalk の拡張ヘルスレポートでは、CPU 使用率、メモリ使用量、ネットワークトラフィック、およびインスタンス数やロードバランサーのステータスといったインフラストラクチャの健全性に関する情報など、詳細なパフォーマンスメトリクスを提供します。

詳細については、「拡張ヘルスレポートおよびモニタリング」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz108
```

ソース

```
AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled
```

アラート条件

黄: Elastic Beanstalk 環境が拡張ヘルスレポートを作成するように設定されていません。

[Recommended Action] (推奨されるアクション)

Elastic Beanstalk 環境が拡張ヘルスレポートを作成できるように設定されているかどうかを確認してください。

詳細については、「Elastic Beanstalk コンソールを使用した拡張ヘルスレポートの有効化」を参照してください。

その他のリソース

- Elastic Beanstalk の拡張ヘルスレポートの有効化

- 拡張ヘルスレポートおよびモニタリング

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS Elastic Beanstalk マネージドプラットフォームの更新が無効になっている

説明

Elastic Beanstalk 環境と設定テンプレートでマネージドプラットフォームの更新が有効になっているかどうかを確認します。

AWS Elastic Beanstalk は、プラットフォームの更新を定期的にリリースして、修正、ソフトウェアの更新、新機能を提供します。マネージドプラットフォーム更新により、Elastic Beanstalk で新しいパッチやマイナープラットフォームバージョンのプラットフォーム更新を自動的に実行することができます。

AWS Config ルールの UpdateLevel パラメータで、必要な更新レベルを指定できます。

詳細については、「Elastic Beanstalk 環境のプラットフォームバージョンの更新」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

c18d2gz177

ソース

AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled

アラート条件

黄: AWS Elastic Beanstalk マネージドプラットフォームの更新は、マイナーレベルやパッチレベルなど、まったく設定されていません。

[Recommended Action] (推奨されるアクション)

Elastic Beanstalk 環境でマネージドプラットフォーム更新を有効にするか、マネージドプラットフォーム更新をマイナーレベルまたは更新レベルで設定してください。

詳細については、「マネージドプラットフォーム更新」を参照してください。

その他のリソース

- Elastic Beanstalk の拡張ヘルスレポートの有効化
- 拡張ヘルスレポートおよびモニタリング

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS Fargate プラットフォームバージョンが最新ではない

説明

Amazon ECS が最新の AWS Fargateプラットフォームバージョンを実行しているかどうかを確認します。Fargate プラットフォームバージョンでは、Fargate タスクインフラストラクチャの特定のランタイム環境を参照することができます。これは、カーネルとコンテナのランタイムバージョンの組み合わせです。新しいプラットフォームのバージョンは、ランタイム環境の進化に伴ってリリースされます。例えば、カーネルやオペレーティングシステムの更新、新機能、バグ修正、セキュリティ更新があったときにリリースされます。

詳細については、「Fargate タスクのメンテナンス」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz174
```

ソース

```
AWS Config Managed Rule: ecs-fargate-latest-platform-version
```

アラート条件

黄: Amazon ECS が Fargate プラットフォームの最新バージョンで実行されていません。

[Recommended Action] (推奨されるアクション)

最新の Fargate プラットフォームバージョンに更新してください。

詳細については、「Fargate タスクのメンテナンス」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

AWS Systems Manager 非準拠ステータスのステートマネージャーの関連付け

説明

インスタンスで AWS Systems Manager 関連付けを実行した後、関連付けコンプライアンスのステータスが COMPLIANT または NON_COMPLIANT かどうかを確認します。

の一機能であるステートマネージャーは AWS Systems Manager、マネージドノードやその他の AWS リソースを定義した状態に保つプロセスを自動化する、安全でスケーラブルな設定管理サービスです。ステートマネージャーの関連付けは、 AWS リソースに割り当てる設定です。設定ではリソース上で維持したい状態を定義するため、Amazon EC2 インスタンス間の設定ドリフトの回避など、目標を達成するのに役立ちます。

詳細については、「AWS Systems Manager State Manager」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz147`

ソース

`AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check`

アラート条件

黄: AWS Systems Manager 関連付けコンプライアンスのステータスは NON_COMPLIANT です。

[Recommended Action] (推奨されるアクション)

State Manager の関連付けステータスを検証し、必要なアクションを実行してステータスを COMPLIANT に戻してください。

詳細については、「About State Manager」を参照してください。

その他のリソース

AWS Systems Manager ステートマネージャー

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

CloudTrail 証跡が、Amazon CloudWatch Logs で設定されていない

説明

CloudWatch Logs にログを送信するように AWS CloudTrail 証跡が設定されているかどうかを確認します。

CloudWatch Logs を使用して CloudTrail ログファイルを監視し、 AWS CloudTrailで重要なイベントがキャプチャされたら自動応答が開始されるようにします。

詳細については、「Amazon CloudWatch Logs による CloudTrail ログファイルをモニタリングする」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz164
```

ソース

```
AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled
```

アラート条件

黄: CloudWatch Logs 統合では設定 AWS CloudTrail されていません。

[Recommended Action] (推奨されるアクション)

CloudWatch Logs にログイベントを送信するように CloudTrail 証跡を設定してください。

詳細については、「CloudTrail イベントの CloudWatch アラームの作成: 例」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

ロードバランサーの Elastic Load Balancing 削除保護が有効になっていない

説明

ロードバランサーの削除保護が有効になっているかどうかを確認します。

Elastic Load Balancing は、Application Load Balancer、Network Load Balancer、Gateway Load Balancer の削除保護をサポートします。ロードバランサーが誤って削除されるのを防ぐために、削除保護を有効にします。ロードバランサーを作成すると、デフォルトで削除保護はオフになります。ロードバランサーが本番環境の一部である場合は、削除保護を有効にすることを検討してください。

アクセスログの作成は、Elastic Load Balancing のオプション機能であり、デフォルトでは無効化されています。ロードバランサーのアクセスログの作成を有効にすると、Elastic Load Balancing はログをキャプチャし、そのログを指定した Amazon S3 バケット内に保存します。

詳細については、「Application Load Balancer の削除保護」、「Network Load Balancer の削除保護」、または「Gateway Load Balancer の削除保護」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。

ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

`c18d2gz168`

ソース

`AWS Config Managed Rule: elb-deletion-protection-enabled`

アラート条件

黄: ロードバランサーの削除保護が有効になっていません。

[Recommended Action] (推奨されるアクション)

Application Load Balancer、Network Load Balancer、Gateway Load Balancer の削除保護を有効にしてください。

詳細については、「Application Load Balancer の削除保護」、「Network Load Balancer の削除保護」、または「Gateway Load Balancer の削除保護」を参照してください。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

RDS DB クラスター削除保護チェック

説明

Amazon RDS DB クラスターの削除保護が有効になっているかどうかを確認します。

クラスターの削除保護を設定すると、どのユーザーもデータベースを削除できません。

削除保護は、すべての AWS リージョンの Amazon Aurora および RDS for MySQL、RDS for MariaDB、RDS for Oracle、RDS for PostgreSQL、および RDS for SQL Server データベースインスタンスで使用できます。

詳細については、「Aurora クラスターの削除保護」を参照してください。

チェック ID

`c18d2gz160`

ソース

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

アラート条件

黄: 削除保護が有効になっていない Amazon RDS DB クラスターがあります。

[Recommended Action] (推奨されるアクション)

Amazon RDS DB クラスターを作成するときに、削除保護を有効にしてください。

削除保護が有効になっていないクラスターのみ削除できます。削除保護を有効にすると、保護レイヤーがさらに強化され、データベースインスタンスが偶発的または意図的に削除されることによるデータ損失を回避できます。削除保護は、規制コンプライアンス要件への対応やビジネスの継続性を確保することにも役立ちます。

詳細については、「Aurora クラスターの削除保護」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

その他のリソース

Aurora クラスターの削除保護

[Report columns] (レポート列)

- ステータス

- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

RDS DB インスタンスのマイナーバージョン自動アップグレードチェック

説明

Amazon RDS DB インスタンスにマイナーバージョン自動アップグレードが設定されているかどうかを確認します。

Amazon RDS インスタンスのマイナーバージョン自動アップグレードを有効にして、データベースが常に安全で安定した最新バージョンを実行していることを確認します。マイナーアップグレードでは、セキュリティ更新、バグ修正、パフォーマンスの向上が提供され、既存のアプリケーションとの互換性が維持されます。

詳細については、「DB インスタンスのエンジンバージョンのアップグレード」を参照してください。

> **Note**
>
> このチェックの結果は、1 日に数回自動的に更新され、更新リクエストは許可されません。変更が表示されるまでに数時間かかる場合があります。
> ビジネス、エンタープライズ On-Ramp、またはエンタープライズサポートのお客様は、BatchUpdateRecommendationResourceExclusion API を使用して、 Trusted Advisor 結果に 1 つ以上のリソースを含めるか除外することができます。

チェック ID

```
c18d2gz155
```

ソース

```
AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled
```

アラート条件

黄: RDS DB インスタンスのマイナーバージョン自動アップグレードが有効になっていません。

[Recommended Action] (推奨されるアクション)

Amazon RDS DB インスタンスを作成するときに、マイナーバージョン自動アップグレードを有効にしてください。

マイナーバージョンアップグレードを有効にすると、マイナーエンジンバージョンの自動アップグレードより低い DB エンジンのマイナーバージョンを実行中のデータベースバージョンは、自動的にアップグレードされます。

[Report columns] (レポート列)

- ステータス
- リージョン
- リソース
- AWS Config ルール
- 入力パラメータ
- 最終更新日時

の変更ログ AWS Trusted Advisor

Trusted Advisor チェックに対する最近の変更については、次のトピックを参照してください。

> **Note**
>
> Trusted Advisor コンソールまたは AWS サポート API を使用する場合、削除されたチェックはチェック結果に表示されません。 AWS サポート API オペレーションやコードでチェック ID を指定するなど、削除されたチェックのいずれかを使用する場合は、API コールエラーを避けるためにこれらのチェックを削除する必要があります。

使用できるチェックの詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しいチェック: Amazon RDS 継続的バックアップが有効になっていない

Trusted Advisor は、2024 年 12 月 23 日に次のチェックを追加しました。

チェック名	チェックカテゴリ	チェック ID
Amazon RDS 継続的バックアップが有効になっていない	耐障害性	44fde09ab5

Amazon RDS インスタンスが Amazon RDS を使用した自動バックアップまたは の継続的バックアップで有効になっているかどうかを確認します AWS Backup。継続的なバックアップにより、予期しないデータ損失のリスクが軽減され、point-in-timeリカバリが可能になります。

詳細については、「Amazon RDS 継続的バックアップが有効になっていない」を参照してください。

新しいチェック: AWS CloudTrail 管理イベントのログ記録

Trusted Advisor は、2024 年 12 月 23 日に次のチェックを追加しました。

チェック名	チェックカテゴリ	チェック ID
AWS CloudTrail 管理イベントのログ記録	セキュリティ	c25hn9x03v

の使用を確認します AWS CloudTrail。

詳細については、「AWS CloudTrail 管理イベントのログ記録」を参照してください。

Auto Scaling グループのリソースチェックを更新しました

Trusted Advisor は、2024 年 12 月 23 日に次のチェックを更新しました。

チェック名	チェックカテゴリ	チェック ID
Auto Scaling グループリソース	耐障害性	8CNsSllI5v

このチェックの説明が更新され、起動設定と起動テンプレートが追加されました。

新しいアラート基準が追加されRed: A launch template is associated with a deleted Amazon Machine Image (AMI).ました。

詳細については、「Auto Scaling グループリソース」を参照してください。

IAM Access Analyzer の外部アクセスチェックを更新しました

Trusted Advisor は、2024 年 12 月 23 日に次のチェックを更新しました。

チェック名	チェックカテゴリ	チェック ID
IAM Access Analyzer の外部アクセス	セキュリティ	07602fcad6

このチェックの説明が更新され、アカウントレベルで IAM アクセスが分析されることを示します。詳細については、「IAM Access Analyzer の外部アクセス」を参照してください。

1 つの新しいチェックを追加

Trusted Advisor は、2024 年 11 月 22 日に 1 つの新しいチェックを追加しました。

- 8604e947f2 - Application Load Balancer セキュリティグループ

3 つのチェックを更新

Trusted Advisor は 2024 年 11 月 7 日に 3 つのチェックを更新しました。

- b92b83d667 - ELB ターゲット不均衡
- 8CNsSlll5v - Auto Scaling グループのリソース
- wuy7G1zxql - Amazon EC2 アベイラビリティーゾーンバランス

4 つのチェックを追加

Trusted Advisor は、2024 年 10 月 11 日に 4 つの新しいチェックを追加しました。

- 07602fcad6 - IAM Access Analyzer - 外部アクセス
- 528d6f5ee7 - GWLB - エンドポイント AZ

- c2vlfg0jp6 - 非アクティブな VPC インターフェイスエンドポイント
- c2vlfg0k35 - 非アクティブな Gateway Load Balancer エンドポイント

3 つのチェックを更新

Trusted Advisor は 2024 年 10 月 2 日に 3 つのチェックを更新しました。

- ID 7040ea389a がコスト最適化の柱から耐障害性の柱に移動されたことを確認する
- チェック ID 7DAFEmoDos を更新
- チェック ID Cmsvnj8db2 を更新しました

9 つの新しいチェックを追加

Trusted Advisor は、2024 年 8 月 23 日に 9 件の新しいチェックを追加しました。

- c2vlfg0p86 - [IAM] - SAML 2.0 ID プロバイダー
- 7040ea389a - Network Firewall エンドポイントのクロス AZ データ転送
- c2vlfg0bfw - 低使用率の Network Firewall
- c2vlfg0gqd - Network Firewall マルチ AZ
- c2vlfg0p1w - Application Load Balancer ターゲットグループの暗号化プロトコル
- c2vlfg022t - [NAT ゲートウェイ] - 使用率の低いリソース
- c243hjzrhn - AWS Outposts シングルラックデプロイ
- b92b83d667 - ELB ターゲット不均衡
- 90046ff5b5 - MSK の可用性は 2 ゾーンに制限されています

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

1 つのセキュリティチェックを更新し、1 つのセキュリティチェックを追加

Trusted Advisor は、2024 年 8 月 22 日に 1 件のオペレーショナルエクセレンスチェックを更新しました。

- c1fd6b96l4

Trusted Advisor 2024 年 8 月 22 日に に 1 つのセキュリティチェックが追加されました。

- c2vlfg0f4h

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

6 セキュリティチェックを更新

Trusted Advisor は 2024 年 8 月 20 日に 6 セキュリティチェックを更新しました。

- nNauJisYIT
- c9D319e7sG
- a2sEc6lLx
- HCP4007jGY
- 1iG5NDGVre
- Yw2K9puPzl

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

1 つの耐障害性チェックを更新

Trusted Advisor は、2024 年 8 月 12 日に 1 つの耐障害性チェックと 1 つのセキュリティを更新しました。

- VPN トンネルの冗長性
- Amazon RDS エンジンのマイナーバージョンアップグレードが必須です。

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

9 つのチェックを更新

Trusted Advisor は、2024 年 7 月 21 日に 9 件のチェックを更新しました。

- 7qGXsKIUw
- ZRxQlPsb6c
- N425c450f2
- 7DAFEmoDos

- Pfx0RwqBli
- H7IgTzjTYb
- C056F80cR3
- Yw2K9puPzl
- xSqX82fQu

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

5 つのチェックを削除し、1 つのチェックを追加

Trusted Advisor 2024 年 5 月 15 日に 3 つの耐障害性チェック、1 つのパフォーマンスチェック、および 1 つのセキュリティチェックを廃止しました。

- IAM の使用
- ELB クロスゾーン負荷分散
- 利用率が高すぎる Amazon EBS マグネティックボリューム
- EC2 セキュリティグループルールの増大
- EC2 セキュリティグループルールの増大

Trusted Advisor は、2024 年 5 月 15 日に 1 つの新しいセキュリティチェックを追加しました。

- Amazon S3 サーバーアクセスログの有効化

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

耐障害性チェックを削除

Trusted Advisor 2024 年 4 月 25 日に 3 つの耐障害性チェックが廃止されました。

- AWS Direct Connect 接続冗長性
- AWS Direct Connect ロケーションの冗長性
- AWS Direct Connect 仮想インターフェイスの冗長性

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しい耐障害性チェック

Trusted Advisor 2024 年 2 月 29 日に 1 つの耐障害性チェックが追加されました。

- NLB - プライベートサブネット内のインターネット向けリソース

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

耐障害性とセキュリティチェックの更新

Trusted Advisor 2024 年 3 月 28 日に 1 つの新しい耐障害性チェックを追加し、1 つの既存の耐障害性と 1 つのセキュリティチェックを修正しました。

- AWS Resilience Hub アプリケーションコンポーネントのチェックを追加
- マルチ AZ 冗長化を使用しない AWS Lambda VPC 対応関数の更新
- 非推奨ランタイムを使用した AWS Lambda 関数の更新

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しい耐障害性チェック

Trusted Advisor 2024 年 1 月 31 日に 1 つの耐障害性チェックが追加されました。

- AWS Direct Connect ロケーションの耐障害性

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

耐障害性チェックの更新

Trusted Advisor 2024 年 1 月 8 日に 1 件の耐障害性チェックを修正しました。

- Amazon RDS innodb_flush_log_at_trx_commit パラメータが 1 ではありません

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

更新済みのセキュリティチェック

Trusted Advisor 2023 年 12 月 21 日に修正 1 セキュリティチェック：

- AWS Lambda 非推奨ランタイムを使用する関数

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しいセキュリティチェックとパフォーマンスチェック

Trusted Advisor は、2023 年 12 月 20 日に 2 つの新しいセキュリティチェックと 2 つの新しいパフォーマンスチェックを追加しました。

- 転送中のデータの暗号化を使用しない Amazon EFS クライアント
- 読み取りワークロードのプロビジョニングが不十分な Amazon Aurora DB クラスター
- システム容量のプロビジョニングが不十分な Amazon RDS インスタンス
- Ubuntu LTS を使用した Amazon EC2 インスタンスの標準サポートの終了

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しいセキュリティチェック

Trusted Advisor は、2023 年 12 月 15 日に 1 つの新しいセキュリティチェックを追加しました。

- S3 バケットを直接指定する Amazon Route 53 の CNAME レコードの不一致

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しい耐障害性チェックとコスト最適化チェック

Trusted Advisor は、2023 年 12 月 7 日に 2 つの新しい耐障害性チェックと 1 つの新しいコスト最適化チェックを追加しました。

- Amazon DocumentDB シングル AZ クラスター
- Amazon S3 で不完全なマルチパートアップロードを中止するための設定
- ブロックモードの Amazon ECS AWS Logs ドライバー

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しい耐障害性チェック

Trusted Advisor は、2023 年 11 月 17 日に 3 つの新しい耐障害性チェックを追加しました。

- ALB マルチ AZ
- NLB マルチ AZ
- 複数の AZ の VPC インターフェイスエンドポイントネットワークインターフェイス

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

Amazon RDS の新しいチェック

Trusted Advisor は、2023 年 11 月 15 日に Amazon RDS の新しいチェックを 37 件追加しました。

詳細については、「AWS Trusted Advisor チェックリファレンス」を参照してください。

新しい AWS Trusted Advisor API

AWS Trusted Advisor では、Trusted Advisor のベストプラクティスチェック、レコメンデーション、優先レコメンデーションにプログラムでアクセスできる新しい APIs が導入されました。Trusted Advisor APIsを使用すると、任意の運用ツールとプログラムで統合 Trusted Advisor して、ワークロードを大規模に自動化および最適化できます。Business、Enterprise On-Ramp、または Enterprise Support のお客様が利用できる新しい APIs は、お客様のアカウントまたは支払者アカウント内のすべての連結アカウントの Trusted Advisor レコメンデーションへのアクセスを提供します。管理アカウントまたは委任管理者アカウントにアクセスできる Enterprise Support のお客様は、さらに、組織全体で優先順位の高い推奨事項をプログラムで取得できます。

新しい Trusted Advisor APIsは、 AWS サポート API (SAPI) を通じて以前に提供された 3 つの機能を置き換えます。SAPI では、今後もケースやその他のサポート情報を提供していきます。

Trusted Advisor APIsは、米国東部 (オハイオ) 、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、アジアパシフィック (ソウル) 、アジアパシフィック (シドニー) 、欧州 (アイルランド) の各リージョンで一般利用可能です。

詳細については、AWS Trusted Advisor API ページをご覧ください。

Trusted Advisor 削除のチェック

Trusted Advisor は、2023 年 11 月 9 日に次のチェックを削除しました。

チェック名	チェックカテゴリ	チェック ID
EBS ボリュームを EC2 インスタンスに接続する必要がある	セキュリティ	Hs4Ma3G119
S3 バケットでは、サーバー側の暗号化を有効にする必要があります	セキュリティ	Hs4Ma3G167
CloudFront ディストリビューションでは、オリジンアクセスアイデンティティを有効にする必要があります	セキュリティ	Hs4Ma3G195

AWS Config チェックの への統合 Trusted Advisor

Trusted Advisor は、2023 年 10 月 30 AWS Config 日に によって提供される 64 の新しいチェックを追加しました。

詳細については、「による AWS Trusted Advisor チェックの表示 AWS Config」を参照してください。

新しい耐障害性チェック

Trusted Advisor は、2023 年 10 月 12 日に次のチェックを追加しました。

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver エンドポイントアベイラビリティーゾーンの冗長性
- サブネットで利用可能な IP の自動スケーリング
- Amazon MSK ブローカーがホストするパーティションの数が多すぎる

詳細については、耐障害性 カテゴリを参照してください。

新しいサービス制限のチェック

Trusted Advisor は、2023 年 8 月 17 日に次のチェックを追加しました。

- Lambda コードストレージの使用状況

詳細については、サービス制限 カテゴリを参照してください。

新しい耐障害性チェック

Trusted Advisor は、2023 年 8 月 3 日に次のチェックを追加しました。

- AWS Lambda 失敗時のイベントの送信先

詳細については、耐障害性 カテゴリを参照してください。

新しい耐障害性チェックとパフォーマンスチェック

Trusted Advisor は、2023 年 6 月 1 日に次のチェックを追加しました。

- Amazon EFS マウントターゲット冗長性なし
- Amazon EFS スループットモードの最適化
- ActiveMQ アベイラビリティーゾーンの冗長性
- RabbitMQ アベイラビリティーゾーンの冗長性

詳細については、耐障害性 カテゴリと パフォーマンス カテゴリを参照してください。

新しい耐障害性チェック

Trusted Advisor は、2023 年 5 月 16 日に次のチェックを追加しました。

- NAT ゲートウェイ AZ インディペンデンス
- シングル AZ アプリケーションチェック

詳細については、耐障害性 カテゴリを参照してください。

新しい耐障害性チェック

Trusted Advisor は、2023 年 4 月 27 日に次のチェックを追加しました。

- Incident Manager レプリケーションセット AWS リージョン 内の の数
- AWS Resilience Hub 評価期間

詳細については、耐障害性 カテゴリを参照してください。

Amazon ECS 耐障害性チェックでのリージョン拡張

Trusted Advisor は、2023 年 4 月 27 日に次のチェックを追加のリージョンに拡張しました。Trusted Advisor チェックは、Amazon ECS が一般公開されているすべてのリージョンで利用可能になりました。

- 単一の AZ を使用した Amazon ECS サービス
- Amazon ECS マルチ AZ 配置戦略

拡張されたリージョンには、アフリカ (ケープタウン)、アジアパシフィック (香港)、アジアパシフィック (ハイデラバード)、アジアパシフィック (ジャカルタ)、アジアパシフィック (メルボルン)、欧州 (ミラノ)、欧州 (スペイン)、欧州 (チューリッヒ)、中東 (バーレーン)、および中東 (UAE) が含まれます。

新しい耐障害性チェック

Trusted Advisor 2023 年 3 月 30 日に で次のチェックが追加されました。

- 単一の AZ を使用した Amazon ECS サービス
- Amazon ECS マルチ AZ 配置戦略

詳細については、耐障害性 カテゴリを参照してください。

新しい耐障害性チェック

Trusted Advisor では、2022 年 12 月 15 日に次のチェックが追加されました。

- AWS CloudHSM 単一の AZ で HSM インスタンスを実行する クラスター

- Amazon ElastiCache マルチ AZ クラスター
- Amazon MemoryDB マルチ AZ クラスター

、ElastiCache AWS CloudHSM、MemoryDB クラスターの結果 Trusted Advisor を で受け取るには、アベイラビリティーゾーンにクラスターが必要です。詳細については、次のドキュメントを参照してください。

- AWS CloudHSM ユーザーガイド
- Amazon MemoryDB デベロッパーガイド

Trusted Advisor は、2022 年 12 月 15 日に次のチェック情報を更新しました。

- AWS Resilience Hub ポリシー違反 — アプリケーション名がアプリケーション名に更新されました
- AWS Resilience Hub レジリエンススコア – アプリケーション名とアプリケーションのレジリエンススコアがアプリケーション名とアプリケーションのレジリエンススコアに更新されました

詳細については、耐障害性 カテゴリを参照してください。

と Trusted Advisor の統合の更新 AWS Security Hub

Trusted Advisor は、2022 年 11 月 17 日に次の更新を行いました。

Security Hub または AWS Config の を無効にした場合 AWS リージョン、 は 7～9 AWS リージョン 日以内にそのコントロール検出結果を削除する Trusted Advisor ようになりました。以前は、Security Hub データを削除する期間は 90 日 Trusted Advisor でした。

詳細については、トラブルシューティング トピックの次のセクションを参照してください。

- Security Hub またはリージョン AWS Config で をオフにした
- コントロールは Security Hub にアーカイブされていますが、 に結果が表示されます Trusted Advisor

AWS Resilience Hubの新しい耐障害性チェック

Trusted Advisor は、2022 年 11 月 17 日に次のチェックを追加しました。

- AWS Resilience Hub ポリシー違反
- AWS Resilience Hub レジリエンススコア

これらのチェックを使用すると、アプリケーションの最新のレジリエンスポリシーステータスとレジリエンススコアを表示できます。Resilience Hub では、アプリケーションのレジリエンシーと可用性を一元的に定義、追跡、管理できます。

Resilience Hub アプリケーションの結果 Trusted Advisor を で受け取るには、アプリケーションをデプロイ AWS し、Resilience Hub を使用してアプリケーションの障害耐性体制を追跡する必要があります。詳細については、AWS Resilience Hub ユーザーガイドをご参照ください。

ElastiCache クラスターと MemoryDB クラスターの結果 Trusted Advisor を で受け取るには、アベイラビリティーゾーンにクラスターが必要です。詳細については、次のドキュメントを参照してください。

Amazon MemoryDB デベロッパーガイド

詳細については、耐障害性 カテゴリを参照してください。

Trusted Advisor コンソールの更新

Trusted Advisor 2022 年 11 月 16 日に に次の変更が追加されました。

コンソールの Trusted Advisor ダッシュボードが Trusted Advisor レコメンデーションになりました。[Trusted Advisor Recommendations] ページには、チェック結果と、 AWS アカウントの各カテゴリで利用できるチェックが引き続き表示されます。

この名前の変更により、 Trusted Advisor コンソールのみが更新されます。コンソール Trusted Advisor と サポート API の Trusted Advisor オペレーションは、通常どおり引き続き使用できます。

詳細については、「Trusted Advisor Recommendations の開始方法」を参照してください。

Amazon EC2 の新しいチェック

Trusted Advisor は、2022 年 9 月 1 日に次のチェックを追加しました。

- Microsoft Windows Server を使用した Amazon EC2 インスタンスのサポートの終了

詳細については、セキュリティ カテゴリを参照してください。

Security Hub チェックを Trusted Advisorに追加しました

2022 年 6 月 23 日現在、 は 2022 年 4 月 7 日まで利用可能な Security Hub コントロール Trusted Advisor のみをサポートしています。このリリースでは、カテゴリ: 復旧 > 回復力のコントロールを除き、 AWS Foundational Security Best Practices セキュリティ標準のすべてのコントロールがサポートされています。詳細については、「での AWS Security Hub コントロールの表示 AWS Trusted Advisor」を参照してください。

サポートされるコントロールのリストについては、AWS Security Hub ユーザーガイドの「AWS Foundational Security Best Practices controls」を参照してください。

からのチェックの追加 AWS Compute Optimizer

Trusted Advisor は、2022 年 5 月 4 日に次のチェックを追加しました。

チェック名	チェックカテゴリ	チェック ID
Amazon EBS の過剰プロビジョニングボリューム	コストの最適化	COr6dfpM03
Amazon EBS のプロビジョニング不足ボリューム	パフォーマンス	COr6dfpM04
AWS Lambda メモリサイズの過剰プロビジョニングされた関数	コストの最適化	COr6dfpM05
AWS Lambda メモリサイズのプロビジョニング不足関数	パフォーマンス	COr6dfpM06

これらのチェックが Lambda および Amazon EBS リソースからデータを受信できるように、Compute Optimizer AWS アカウント の をオプトインする必要があります。詳細については、「チェック AWS Compute Optimizer に Trusted Advisor オプトインする」を参照してください。

公開アクセスキーチェックの更新

Trusted Advisor は、2022 年 4 月 25 日に次のチェックを更新しました。

チェック名	チェックカテゴリ	チェック ID
露出したアクセスキー	セキュリティ	12Fnkpl8Y5

Trusted Advisor でこのチェックが自動的に更新されるようになりました。このチェックは、 Trusted Advisor コンソールまたは AWS サポート API から手動で更新することはできません。アプリケーションまたはコードが のこのチェックを更新する場合は AWS アカウント、更新してこのチェックを更新しないことをお勧めします。作成されていない場合は、`InvalidParameterValue` エラーが発生します。

この更新の前に除外したアクセスキーは除外されなくなり、影響を受けるリソースとして表示されます。チェック結果からアクセスキーを除外することはできません。詳細については、「露出したアクセスキー」を参照してください。

> **Note**
>
> 2022 年 4 月 25 AWS アカウント 日以降に を作成した場合、公開アクセスキーのチェック結果には、公開されていないアクセスキーであっても、最初は灰色のアイコン ( ) が表示されます。これは、 Trusted Advisor がチェックへの変更を識別していないことを意味します。
> がリスクのあるリソース Trusted Advisor を識別すると、ステータスはアクション推奨アイコン () に変わります
> 。
> リソースを修正または削除すると、チェック結果にチェックマークアイコン ( ) が表示されます。

AWS Direct Connectの更新したチェック項目

Trusted Advisor は、2022 年 3 月 29 日に次のチェックを更新しました。

チェック名	チェックカテゴリ	チェック ID
AWS Direct Connect 接続冗長性	耐障害性	0t121N1Ty3
AWS Direct Connect ロケーションの冗長性	耐障害性	8M012Ph3U5
AWS Direct Connect 仮想インターフェイスの冗長性	耐障害性	4g3Nt5M1Th

- [Region] (リージョン) 列の値には、フルネームではなく AWS リージョン コードが表示されるようになりました。例えば、米国東部 (バージニア北部) のリソースは、us-east-1 値となります。
- [Time Stamp] (タイムスタンプ) 列の値は、2022-03-30T01:02:27.000Z などの RFC 3339 形式で表示されるようになりました。
- 問題が検出されていないリソースが、チェックテーブルに表示されるようになりました。これらのリソースには、横にチェックマークアイコン (✓) が表示されます。

  以前は、調査を Trusted Advisor 推奨するリソースのみがテーブルに表示されていました。これらのリソースには、横に警告アイコン (⚠) が表示されています。

AWS Security HubAWS Trusted Advisor コンソールに追加されたコントロール

AWS Trusted Advisor は、2022 年 1 月 18 日にセキュリティカテゴリに 111 個の Security Hub コントロールを追加しました。

Security Hub コントロールの検出結果は、 AWS Foundational Security Best Practices セキュリティ標準から確認できます。この統合には、[Recover] (回復) > [Resilience] (耐障害性) のカテゴリを使用しているのコントロールは含まれていません。

この機能の詳細については、「での AWS Security Hub コントロールの表示 AWS Trusted Advisor」を参照してください。

Amazon EC2 および AWS Well-Architected の新しいチェック機能

Trusted Advisor は、2021 年 12 月 20 日に次のチェックを追加しました。

- Amazon EC2 インスタンスの統合 (Microsoft SQL Server 向け)
- 過剰にプロビジョニングされた Amazon EC2 インスタンス (Microsoft SQL サーバー向け)
- Microsoft SQL Server を使用した Amazon EC2 インスタンスのサポートの終了
- コスト最適化に関する AWS Well-Architected のリスクの高い問題
- パフォーマンスに関する AWS Well-Architected のリスクの高い問題
- セキュリティに関する AWS Well-Architected のリスクの高い問題
- 信頼性に関する AWS Well-Architected のリスクの高い問題

詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。

Amazon OpenSearch Service のチェック名を更新しました

Trusted Advisor は、2021 年 9 月 8 日にAmazon OpenSearch Service Reserved Instance Optimizationチェックの名前を更新しました。

チェックの推奨事項、カテゴリ、および ID は同じです。

チェック名	チェックカテゴリ	チェック ID
Amazon OpenSearch Service リザーブドインスタンス最適化	コストの最適化	`7ujm6yhn5t`

> **Note**
>
> Amazon CloudWatch メトリクス Trusted Advisor に を使用する場合、このチェックのメトリクス名も更新されます。詳細については、「AWS Trusted Advisor メトリクスをモニタリングする Amazon CloudWatch アラームを作成する」を参照してください。

Amazon Elastic Block Store ボリュームストレージに追加されたチェック

Trusted Advisor では、2021 年 6 月 8 日に次のチェックが追加されました。

チェック名	チェックカテゴリ	チェック ID
EBS 汎用 SSD (gp3) ボリュームストレージ	サービス制限	dH7RR0l6J3
EBS プロビジョンド IOPS SSD (io2 ボリュームのストレージ)	サービス制限	gI7MM0l7J2

のチェックを追加 AWS Lambda

Trusted Advisor は、2021 年 3 月 8 日に次のチェックを追加しました。

チェック名	チェックカテゴリ	チェック ID
AWS Lambda 過剰なタイムアウトがある関数	コストの最適化	L4dfs2Q3C3
AWS Lambda エラー率の高い関数	コストの最適化	L4dfs2Q3C2
AWS Lambda 非推奨ランタイムを使用する関数	セキュリティ	L4dfs2Q4C5
AWS Lambda マルチ AZ 冗長化を使用しない VPC 対応関数	耐障害性	L4dfs2Q4C6

Lambda でこれらのチェックを使用する方法の詳細については、「 AWS Lambda デベロッパーガイド」の「レコメンデーションを表示する AWS Trusted Advisor ワークフローの例」を参照してください。

Trusted Advisor 削除のチェック

Trusted Advisor は、2021 年 3 月 8 AWS GovCloud (US) Region 日に の次のチェックを削除しました。

チェック名	チェックカテゴリ	チェック ID
EC2 Elastic IP アドレス	サービス制限	aW9HH0l8J6

Amazon Elastic Block Store の更新されたチェック

Trusted Advisor は、2021 年 3 月 5 日に以下のチェックのために Amazon EBS ボリュームの単位をギビバイト (GiB) からテビバイト (TiB) に更新しました。

> **Note**
>
> Amazon CloudWatch メトリクス Trusted Advisor に を使用する場合、これら 5 つのチェックのメトリクス名も更新されます。詳細については、「AWS Trusted Advisor メトリクスをモニタリングする Amazon CloudWatch アラームを作成する」を参照してください。

チェック名	チェックカテゴリ	チェック ID	ServiceLimit の更新された CloudWatch メトリクス
EBS Cold HDD (sc1) ボリュームストレージ	サービス制限	gH5CC0e3J9	Cold HDD (sc1) ボリュームストレージ (TiB)
EBS 汎用 SSD (gp2) ボリュームストレージ	サービス制限	dH7RR0l6J9	汎用 SSD (gp2) ボリュームストレージ (TiB)
EBS マグネティック (スタンダードボリュームストレージ)	サービス制限	cG7HH0l7J9	マグネティック (スタンダードボリュームストレージ) (TiB)

チェック名	チェックカテゴリ	チェック ID	ServiceLimit の更新された CloudWatch メトリクス
EBS プロビジョンド IOPS SSD (io1 ボリュームのストレージ)	サービス制限	gI7MM0l7J9	プロビジョンド IOPS (SSD) ストレージ (TiB)
EBS スループット最適化 HDD (st1) ボリュームストレージ	サービス制限	wH7DD0l3J9	スループット最適化 HDD (st1) ボリュームストレージ (TiB)

Trusted Advisor 削除のチェック

> **Note**
>
> Trusted Advisor は、2020 年 11 月 18 日に次のチェックを削除しました。

2020 年 11 月 18 日に削除されたチェック	チェックカテゴリ	チェック ID
EC2 Windows インスタンス用の EC2Config サービス	耐障害性	V77iOLlBqz
EC2 Windows インスタンス用の ENA ドライバーバージョン	耐障害性	TyfdMXG69d
EC2 Windows インスタンス用の NVMe ドライバーバージョン	耐障害性	yHAGQJV9K5
EC2 Windows インスタンス用の PV ドライバーバージョン	耐障害性	Wnwm9Il5bG
EBS アクティブボリューム	サービス制限	fH7LL0l7J9

Amazon Elastic Block Store では、プロビジョニングできるボリュームの数に制限がなくなりました。

AWS Systems Manager Distributor またはその他のサードパーティー製ツールを使用するか、Windows 管理インストルメンテーション (WMI) のドライバー情報を返す独自のスクリプトを記述することによって Amazon EC2 インスタンスを監視してインスタンスが最新であることを確認できます。

Trusted Advisor 削除のチェック

Trusted Advisor は、2020 年 2 月 18 日に次のチェックを削除しました。

チェック名	チェックカテゴリ	チェック ID
サービスの制限	パフォーマンス	eW7HH0l7J9

AWS サポート Slack のアプリ

AWS サポート アプリを使用して、Slack で AWS サポートケースを管理できます。チームメンバーをチャットチャネルに招待し、ケースの更新に応答し、サポートエージェントと直接チャットします。 AWS サポート アプリを使用して、Slack でサポートケースをすばやく管理します。

AWS サポート アプリを使用して、次の操作を行います。

- Slack チャンネルでサポートケースを作成、更新、検索、解決する
- ファイルをサポートケースに添付する
- Service Quotas でクォータの引き上げをリクエストする
- Slack チャンネルから退出することなく、サポートケースの詳細をチームに共有する
- サポートエージェントとのライブチャットセッションを開始する

AWS サポート アプリでサポートケースを作成、更新、または解決すると、ケースも で更新されます AWS Support Center Console。サポートケースを個別に管理するために、サポートセンターコンソールにサインインする必要はありません。

> **メモ**
>
> - サポートケースの応答時間は、ケースを Slack から作成したか、サポートセンターコンソールから作成したかに関係なく同一です。
> - アカウントと請求サポート、サービスクォータの引き上げ、テクニカルサポートのサポートケースを作成できます。

トピック

- Slack でのサポートケースの検索
- Slack でのサポートケースの解決
- Slack でのサポートケースの再オープン
- サービスクォータの引き上げリクエスト
- AWS サポート アプリからの Slack チャンネル設定の削除
- AWS サポート アプリからの Slack ワークスペース設定の削除
- AWS サポート Slack コマンドのアプリ
- AWS サポート アプリのコレスポンデンスを AWS Support Center Consoleに表示する
- を使用した Slack リソースでの AWS サポート アプリの作成 AWS CloudFormation

前提条件

Slack で AWS サポート アプリを使用するには、次の要件を満たす必要があります。

- ビジネスプラン、エンタープライズ On-Ramp、エンタープライズサポートプランを利用している。ご自身のサポートプランは、 AWS Support Center Console またはサポートプランのページでご確認いただけます。詳細については、AWS サポート 「計画の比較」を参照してください。
- ご自身の組織の Slack ワークスペースとチャンネルを用意する必要があります。Slack ワークスペースの管理者であるか、またはその Slack ワークスペースにアプリを追加する許可を得ている必要があります。詳細については、Slack ヘルプセンターを参照してください。
- 必要なアクセス許可を持つ AWS Identity and Access Management (IAM) ユーザーまたはロール AWS アカウント として にサインインします。詳細については、「AWS サポート アプリウィジェットへのアクセスの管理」を参照してください。
- 自分の代わりにアクションを実行する、必要なアクセス許可を持つ IAM ロールを作成する必要があります。 AWS サポート アプリはこのロールを使用して、さまざまな サービスへの API コールを行います。詳細については、「AWS サポート アプリへのアクセスの管理」を参照してください。

トピック

- AWS サポート アプリウィジェットへのアクセスの管理
- AWS サポート アプリへのアクセスの管理

AWS サポート アプリウィジェットへのアクセスの管理

AWS Identity and Access Management (IAM) ポリシーをアタッチして、 で AWS サポート アプリウィジェットを設定するアクセス許可を IAM ユーザーに付与できます AWS Support Center Console。

ポリシーを IAM エンティティにアタッチする方法の詳細については、「IAM ユーザーガイド」の「IAM ID アクセス許可の追加 (コンソール)」を参照してください。

> **Note**
>
> のルートユーザーとしてサインインすることもできますが AWS アカウント、これはお勧めしません。ルートユーザーアクセスの詳細については、「IAM ユーザーガイド」の「ルートユーザーの認証情報を保護し、日常的なタスクには使用しない」を参照してください。

IAM ポリシーの例

次のポリシーは、IAM ユーザーやグループなどのエンティティにアタッチできます。このポリシーを使うと、サポートセンターコンソールで Slack ワークスペースを承認したり、Slack チャンネルを設定したりできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
```

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

AWS サポート アプリを Slack に接続するために必要な許可

AWS サポート アプリには、API オペレーションに直接対応しないアクセス許可のみのアクションが含まれています。これらのアクションは、「サービス認可リファレンス」の「〔アクセス許可のみ〕」で示されています。

AWS サポート アプリは、次の API アクションを使用して Slack に接続し、パブリック Slack チャネルを に一覧表示します AWS Support Center Console。

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

これらの API アクションは、コードで呼び出すためのものではないため、したがって、これらの API アクションは AWS CLI および AWS SDKs に含まれません。

AWS サポート アプリへのアクセスの管理

AWS サポート アプリウィジェットへのアクセス許可を取得したら、 (IAM) AWS Identity and Access Management ロールも作成する必要があります。このロールは、 AWS サポート API や Service Quotas など AWS のサービス 、他の からアクションを実行します。

続いて、このロールに IAM ポリシーをアタッチし、これらのアクションを実行するために必要なアクセス許可を、このロールに付与します。このロールは、サポートセンターコンソールで Slack チャンネル設定を作成する際に選択します。

Slack チャンネルのユーザーは、IAM ロールに付与したのと同じアクセス許可を有しています。例えば、サポートケースへの読み取り専用アクセスが指定されている場合、Slack チャンネルのユーザーは、サポートケースの表示はできますが更新はできません。

> **Important**
>
> サポートエージェントとのライブチャットをリクエストし、ライブチャットチャネルの設定として新しいプライベートチャネルを選択すると、 AWS サポート アプリは別の Slack チャ

ネルを作成します。この Slack チャンネルは、ケースを作成したりチャットを開始したりしたチャンネルと同じアクセス許可を有しています。
IAM ロールまたは IAM ポリシーを変更すると、変更は設定した Slack チャネルと、 AWS サポート アプリが作成する新しいライブチャット Slack チャネルに適用されます。

IAM ロールとポリシーを作成するときは、以下の手順に従います。

トピック

AWS 管理ポリシーを使用するか、カスタマー管理ポリシーを作成する

ロールのアクセス許可を付与するには、 AWS 管理ポリシーまたはカスタマー管理ポリシーのいずれかを使用できます。

> **Tip**
> ポリシーを手動で作成しない場合は、代わりに AWS 管理ポリシーを使用して、この手順をスキップすることをお勧めします。管理ポリシーには、 AWS サポート アプリに必要なアクセス許可が自動的に付与されます。ユーザーがポリシーを手動で更新する必要はありません。詳細については、「AWS Slack の AWS サポート アプリの マネージドポリシー」を参照してください。

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。この手順では、IAM コンソールの JSON ポリシーエディタを使用します。

AWS サポート アプリのカスタマー管理ポリシーを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで、ポリシー を選択してください。
3. [ポリシーの作成] を選択します。
4. [JSON] タブを選択します。

5. JSON を入力し、エディタでデフォルトの JSON を置き換えます。ポリシーの例を利用できます。
6. [Next: Tags] (次へ: タグ) を選択します。
7. (オプション) キーバリューペアとしてのタグを使用して、メタデータをポリシーに追加することができます。
8. [次へ: レビュー] を選択します。
9. [Review policy] (ポリシーの確認) ページで、名前 (*AWSSupportAppRolePolicy* など) と説明 (任意) を入力します。
10. [Summary] (概要) ページで、そのポリシーで付与されているアクセス許可を確認し、[Create policy] (ポリシーの作成) を選択します。

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

IAM ポリシーの例

IAM ロールには、以下のポリシーの例をアタッチできます。このポリシーにより、ロールは AWS サポート アプリに必要なすべてのアクションに対する完全なアクセス許可を持つことができます。このロールを使って Slack チャンネルを設定すると、チャンネル内のすべてのユーザーに同じアクセス許可が付与されます。

> **Note**
>
> AWS 管理ポリシーのリストについては、「」を参照してくださいAWS Slack の AWS サポート アプリの マネージドポリシー。

ポリシーを更新して、 AWS サポート アプリからアクセス許可を削除できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
```

```
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

各アクションの説明については、「サービス認可リファレンス」の以下のトピックを参照してください。

- AWS サポート のアクション、リソース、条件キー
- 「Service Quotas のアクション、リソース、および条件キー」
- のアクション、リソース、および条件キー AWS Identity and Access Management

IAM ロールを作成する

このポリシーを作成したら、IAM ロールを作成し、そのロールにポリシーをアタッチする必要があります。このロールは、サポートセンターコンソールで Slack チャンネル設定を作成するときに選択します。

AWS サポート アプリのロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。

3. [Select trusted entity] (信頼されたエンティティを選択) で、[AWS のサービス] を選択します。
4. [AWS サポート アプリケーション] を選択します。
5. [Next: Permissions] (次へ: アクセス許可) を選択します。
6. ポリシー名を入力します。 AWS 管理ポリシーを選択するか、 など、作成したカスタマー管理ポリシーを選択できます*AWSSupportAppRolePolicy*。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. [Role name] (ロール名) に、*AWSSupportAppRole* など、名前を入力します。
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。これで、サポートセンターコンソールで Slack チャンネルを設定する際に、このロールを選択できるようになりました。「Slack チャンネルの設定」を参照してください。

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

トラブルシューティング

AWS サポート アプリへのアクセスを管理するには、以下のトピックを参照してください。

目次

Slack チャンネルで特定のユーザーが特定のアクションを行うことを制限したい

デフォルトでは、Slack チャンネルのユーザーには、作成する IAM ロールにアタッチする IAM ポリシーで指定したものと同じアクセス許可が付与されます。つまり、 または AWS アカウント IAM ユーザーがあるかどうかにかかわらず、チャネル内のすべてのユーザーがサポートケースへの読み取りまたは書き込みアクセス権を持ちます。

推奨されるベストプラクティスを以下に示します：

- AWS サポート アプリでプライベート Slack チャネルを設定する
- チャンネルには、サポートケースにアクセスする必要のあるユーザーのみを招待します。
- AWS サポート アプリへの必要最小限のアクセス許可を有した IAM ポリシーを使用します。「AWS Slack の AWS サポート アプリの マネージドポリシー」を参照してください。

Slack チャンネルを設定しても、作成した IAM ロールが表示されない

IAM ロールが AWS サポート アプリリストの IAM ロールに表示されない場合は、そのロールに信頼されたエンティティとして AWS サポート アプリがないか、ロールが削除されたことを意味します。既存のロールを更新するか、新しいロールを作成します。「IAM ロールを作成する」を参照してください。

IAM ロールにアクセス許可が付与されていない

Slack チャンネル用に作成する IAM ロールには、求められているアクションを実行するためのアクセス許可が必要です。例えば、Slack のユーザーがサポートケースを作成できるようにしたいときは、ロールに `support:CreateCase` のアクセス許可が必要です。 AWS サポート アプリは、これらのアクションを実行するためにこのロールを引き受けます。

AWS サポート アプリからアクセス許可の欠落に関するエラーが表示された場合は、ロールにアタッチされたポリシーに必要なアクセス許可があることを確認します。

前述の「IAM ポリシーの例」を参照してください。

Slack のエラーで、IAM ロールが有効でないと表示される

チャンネルの設定に適したロールを選択していることを確認してください。

ロールを確認するには

1. https://console.aws.amazon.com/support/app#/config ページで にサインイン AWS Support Center Console します。
2. AWS サポート アプリで設定したチャネルを選択します。
3. [Permissions] (アクセス許可) セクションで、選択した IAM ロールの名前を見つけます。
    - ロールを変更するには、[Edit] (編集) をクリックし、別のロールを選択して [Save] (保存) を選択します。

- ロールまたはロールにアタッチしたポリシーを更新するときは、IAM コンソールにサインインします。

AWS サポート アプリは、Service Quotas の IAM ロールがないと言います

Service Quotas でクォータの引き上げをリクエストするときは、アカウントに AWSServiceRoleForServiceQuotas ロールが必要です。リソースの欠落に関するエラーが発生したときは、以下のいずれかの手順を実行します。

- クォータの引き上げをリクエストするときは、Service Quotas のコンソールを使用します。リクエストが成功すると、Service Quotas が自動的にロールを作成します。次に、 AWS サポート アプリを使用して、Slack でクォータの引き上げをリクエストできます。詳細については、「Requesting a quota increase」(クォータ引き上げのリクエスト) を参照してください。
- ロールにアタッチされた IAM ポリシーを更新します。これにより、Service Quotas へのアクセス許可がロールに付与されます。の次のセクションIAM ポリシーの例では、 AWS サポート アプリが Service Quotas ロールを作成できるようにします。

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

チャネル用に設定した IAM ロールを削除する場合は、手動でロールを作成するか、IAM ポリシーを更新して、 AWS サポート アプリがロールを作成できるようにする必要があります。

Slack ワークスペースを承認する

ワークスペースを承認し、そのワークスペースへのアクセス許可を AWS サポート アプリに付与したら、 の AWS Identity and Access Management (IAM) ロールが必要です AWS アカウント。 AWS サポート アプリはこのロールを使用して、 AWS サポートおよび Service Quotas から API オペレーションを呼び出します。例えば、 AWS サポート アプリは ロールを使用して CreateCaseオペレーションを呼び出し、Slack でサポートケースを作成します。

メモ

- Slack チャンネルは IAM ロールからアクセス許可を継承します。つまり、Slack チャンネルのユーザーは誰でも、このロールにアタッチされた IAM ポリシーで指定されているものと同じアクセス許可を利用できるということです。

  例えば、IAM ポリシーがサポートケースの完全な読み取りと書き込みをこのロールに許可している場合は、Slack チャンネルにいる誰もがサポートケースを作成、更新、解決できます。IAM ポリシーでロールに許可されているのが読み取り専用のアクセス許可である場合、Slack チャンネルのユーザーはサポートケースの読み取りのみが許可されます。
- Slack ワークスペースとチャンネルは、サポートオペレーションの管理に必要なものを追加することが推奨されます。また、プライベートチャンネルを設定し、必要なユーザーのみを招待することが推奨されます。

Slack ワークスペースはそれぞれ、 AWS アカウントのために使用するものを承認する必要があります。複数の がある場合は AWS アカウント、各アカウントにサインインし、次の手順を繰り返してワークスペースを承認する必要があります。アカウントが AWS Organizations の組織に属しており、複数のアカウントを承認する必要があるときは、複数のアカウントを承認に進んでください。

の Slack ワークスペースを承認するには AWS アカウント

1. AWS Support Center Console にサインインし、[Slack configuration] (Slack の設定) を選択します。
2. [Getting started] (開始方法) のページで [Authorize workspace] (ワークスペースを承認) を選択します。
3. Slack にまだサインインしていない場合は、[Sign in to your workspace] (ワークスペースにサインイン) ページでワークスペース名を入力し、[Continue] (続行) をクリックします。
4. [AWS サポート が your-workspace-name Slack へのアクセス許可をリクエスト中] ページで、[許可] を選択します。

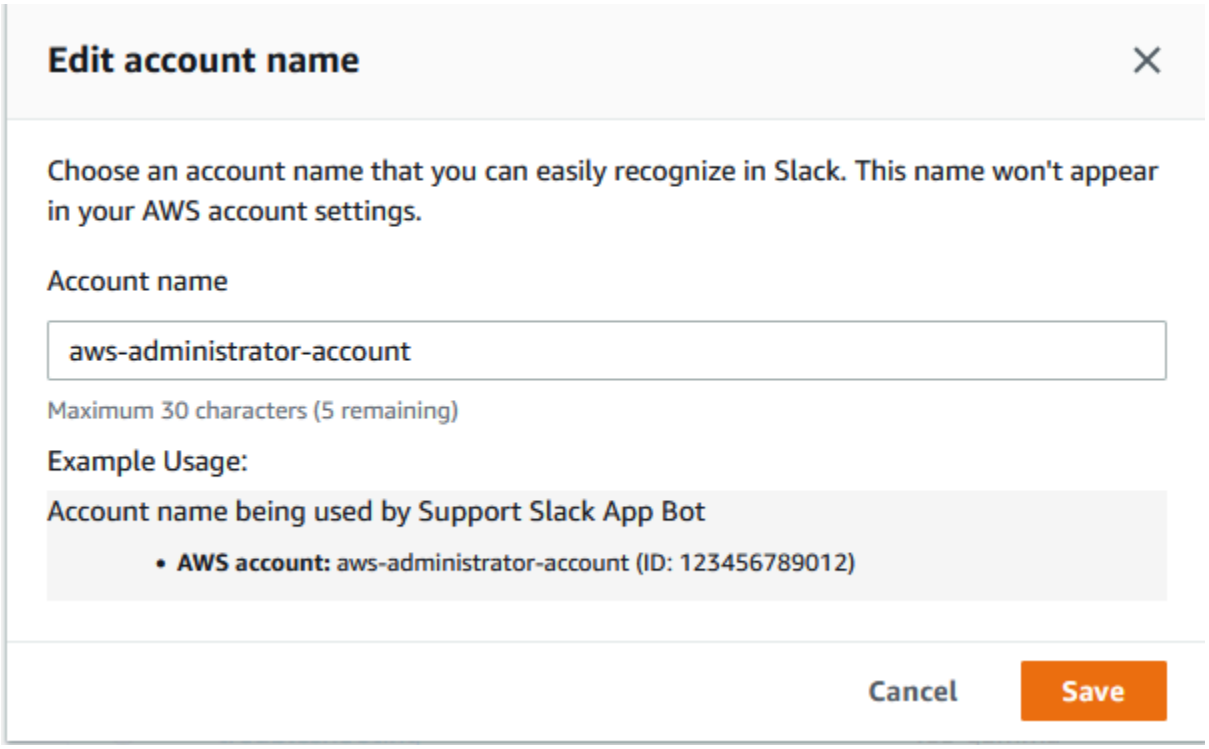
   Note

   Slack にワークスペースへのアクセスを許可できない場合は、Slack 管理者からワークスペースに AWS サポート アプリを追加するためのアクセス許可があることを確認してください。「前提条件」を参照してください。

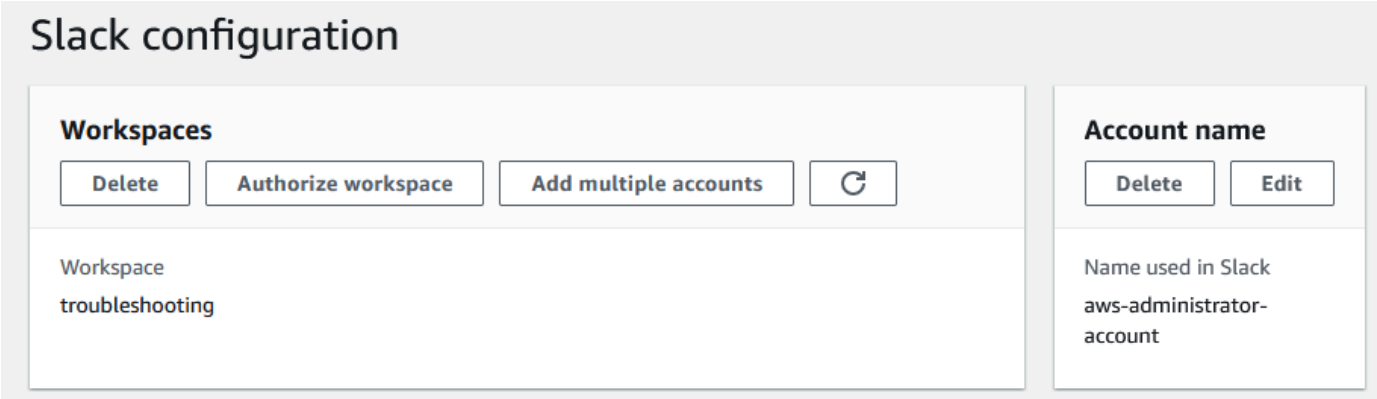
[Slack configuration] (Slack の設定) ページで、ワークスペース名が [Workspaces] (ワークスペース) に表示されます。

5. (オプション) さらにワークスペースを追加するときは、[Authorize workspace] (ワークスペースを承認) を選択し、3～4 の手順を繰り返します。アカウントには最大 5 つまでワークスペースを追加できます。
6. (オプション) デフォルトでは、 AWS アカウント ID 番号は Slack チャネルのアカウント名として表示されます。この値を変更するときは、[Account name] (アカウント名) で [Edit] (編集) をクリックし、アカウント名を入力して [Save] (保存) をクリックします。

> **Tip**
>
> アカウント名には、ご自分やご自分のチームが容易に認識できる名前を使用してください。 AWS サポート アプリはこの名前を使用して、Slack チャネル内のアカウントを識別します。この名前はいつでも変更できます。



ワークスペースとアカウント名は、[Slack configuration] (Slack の設定) のページに表示されます。



複数のアカウントを承認

複数の AWS アカウント に Slack ワークスペースの使用を許可するには、 AWS CloudFormationまたは Terraform を使用して AWS サポート アプリリソースを作成します。

Slack チャンネルの設定

Slack ワークスペースを承認すると、 AWS サポート アプリを使用するように Slack チャンネルを設定することができます。

AWS サポート アプリを招待して追加するチャネルは、ケースを作成および検索し、ケース通知を受信できる場所です。このチャンネルには、新しく作成または解決されたケース、追加されたコレスポンデンス、共有されたケースの詳細など、ケースの最新情報が表示されます。

Slack チャンネルは IAM ロールからアクセス許可を継承します。つまり、Slack チャンネルのユーザーは誰でも、このロールにアタッチされた IAM ポリシーで指定されているものと同じアクセス許可を利用できるということです。

例えば、IAM ポリシーがサポートケースの完全な読み取りと書き込みをこのロールに許可している場合は、Slack チャンネルにいる誰もがサポートケースを作成、更新、解決できます。IAM ポリシーでロールに許可されているのが読み取り専用のアクセス許可である場合、Slack チャンネルのユーザーはサポートケースの読み取りのみが許可されます。

1 つのアカウントには最大 20 チャンネルまで追加できます。Slack チャンネルは、最大 100 の AWS アカウントを持つことができます。言い換えれば、同じ Slack チャンネルを AWS サポート アプリに追加できるアカウントは100 個まで、ということです。追加するアカウントは、組織のサポートケースの管理に必要な数のみにすることが推奨されます。それによりチャンネルで受け取る通知の数が減り、チームの中断時間を減らすことができます。

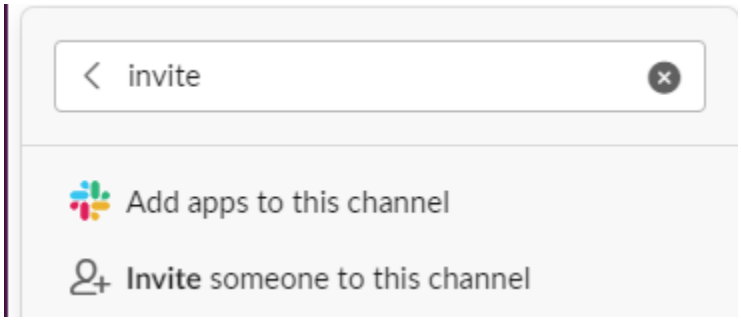
各 は、 AWS サポート アプリで個別に Slack チャネルを設定 AWS アカウント する必要があります。これにより、 AWS サポート アプリはそのサポートケースにアクセスできます AWS アカウント。組織 AWS アカウント 内の別の が既にその Slack チャネルに AWS サポート アプリを招待している場合は、ステップ 3 に進みます。

> **Note**
>
> Slack Connect 内のチャンネルや、複数のワークスペースで共有するチャンネルを設定できます。ただし、 AWS サポート アプリを使用 AWS アカウント できるのは、 の共有チャネルを設定した最初のワークスペースのみです。別のワークスペースに同じ Slack チャネルを設定しようとすると、 AWS サポート アプリはエラーメッセージを返します。

Slack チャンネルを設定する

1. Slack アプリケーションから、 AWS サポート アプリで使用する Slack チャネルを選択します。
2. アプリをチャネル AWS サポート に招待するには、次のステップを実行します。

   a. [+] をクリックして `invite` を入力し、画面が表示されたら、[Add apps to this channel] (アプリをこのチャンネルに追加) を選択します。

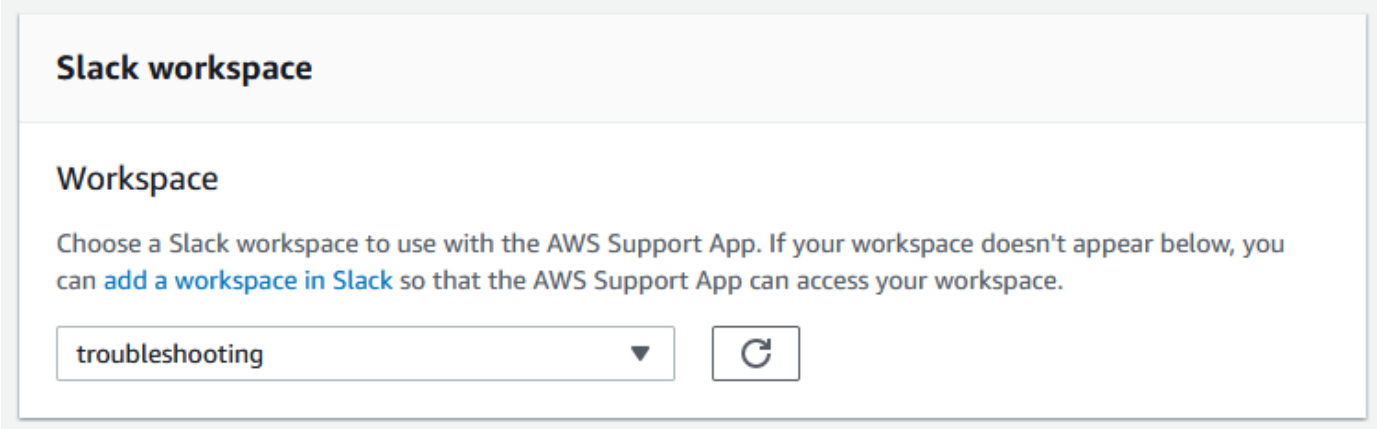
   b. アプリケーションを検索するには、[アプリケーションを channelName に追加] の [AWS サポート アプリケーション] を入力します。

   c. [AWS サポート アプリケーション] の横にある [追加] を選択します。

3. サポートセンターコンソールにサインインし、[Slack configuration] (Slack の設定) を選択します。

4. [Add channel] (チャンネルの追加) を選択します。
5. [Add channel] (チャンネルの追加) ページの[Workspace] (ワークスペース) で、すでに認証されているワークスペース名を選択します。ワークスペース名がリストに表示されない場合は、更新アイコンをクリックします。

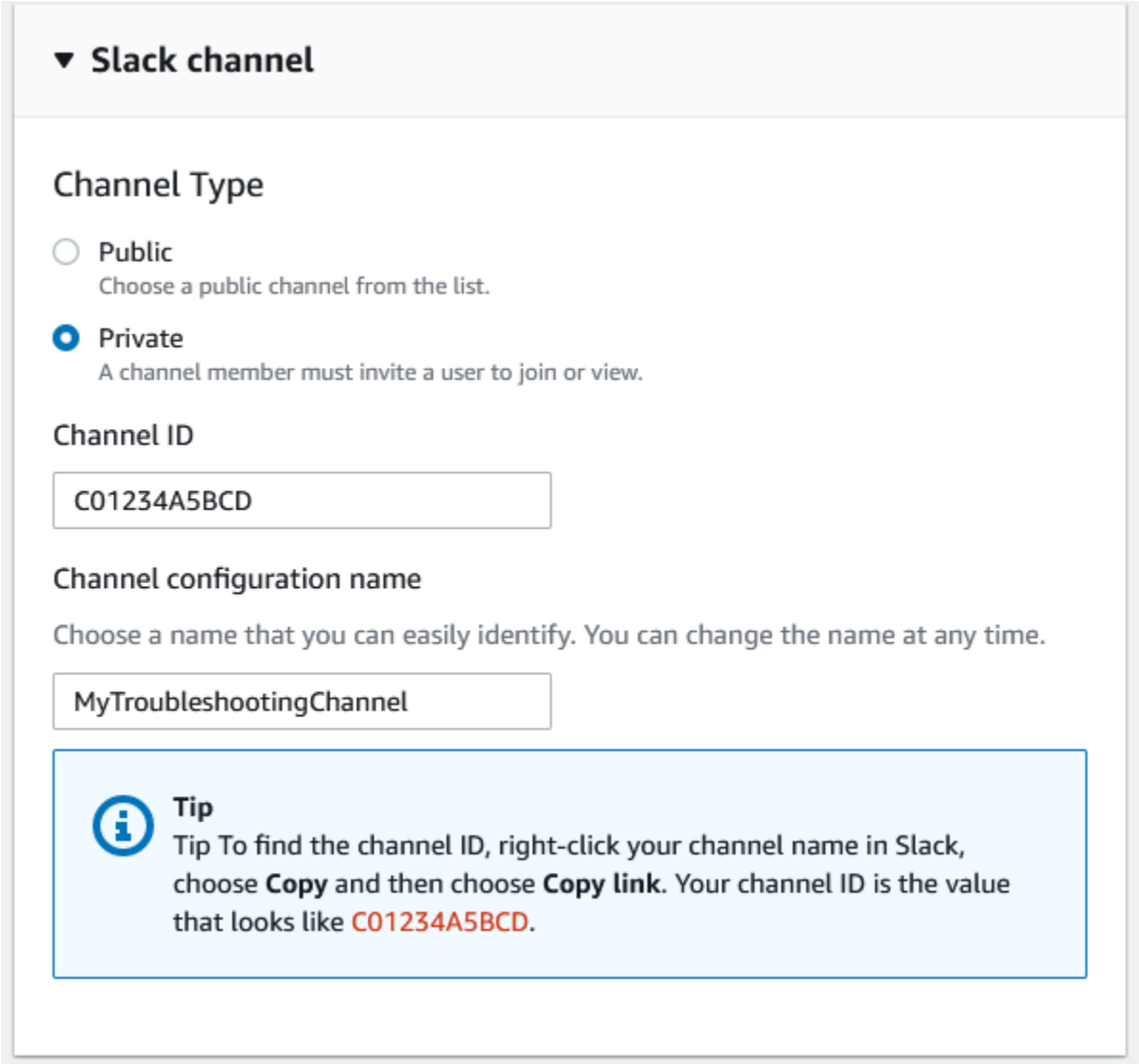


6. [Slack channel] (Slack チャンネル) の [Channel type] (チャンネルタイプ) で、次のいずれかを選択します。
   - [Public] (パブリック) – [Public channel] (パブリックチャンネル) で、 AWS サポート アプリに招待した Slack チャンネルを選択します (ステップ 2)。チャンネルがリストに表示されていない場合は、更新アイコンをクリックし、再度試します。
   - プライベート – チャネル ID に、 AWS サポート アプリを招待した Slack チャネルの ID または URL を入力します。

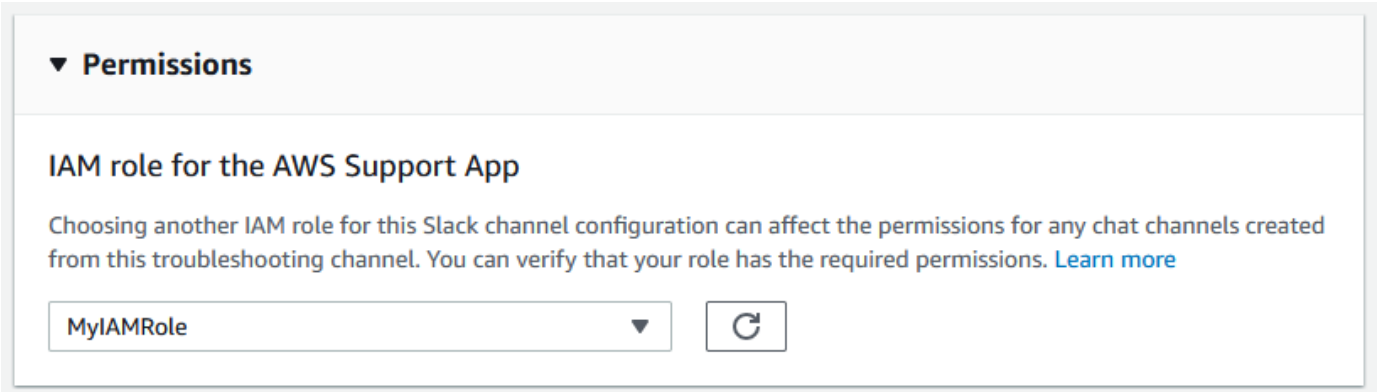
     > **Tip**
     >
     > チャンネル ID を見つけるには、Slack で、チャンネル名のコンテキストメニューを (右クリックで) 開き、[Copy] (コピー)、[Copy link] (リンクをコピー) の順に選択します。チャンネル ID は、*C01234A5BCD* (例) のような値で表示されます。

7. 「チャネル設定名」に、 AWS サポート アプリの Slack チャネル設定を簡単に識別できる名前を入力します。この名前は にのみ表示 AWS アカウント され、Slack には表示されません。チャンネル設定の名前は後で変更できます。

   Slack チャンネルのタイプは、次のような見た目になります。



8. アクセス許可で、Slack の AWS サポート アプリの IAM ロールで、 AWS サポート アプリ用に作成したロールを選択します。信頼されたエンティティとして AWS サポート アプリを持つロールのみがリストに表示されます。



> **Note**
>
> まだロールを作成していない、またはリストに自分のロールが表示されない場合は、「AWS サポート アプリへのアクセスの管理」を参照してください。

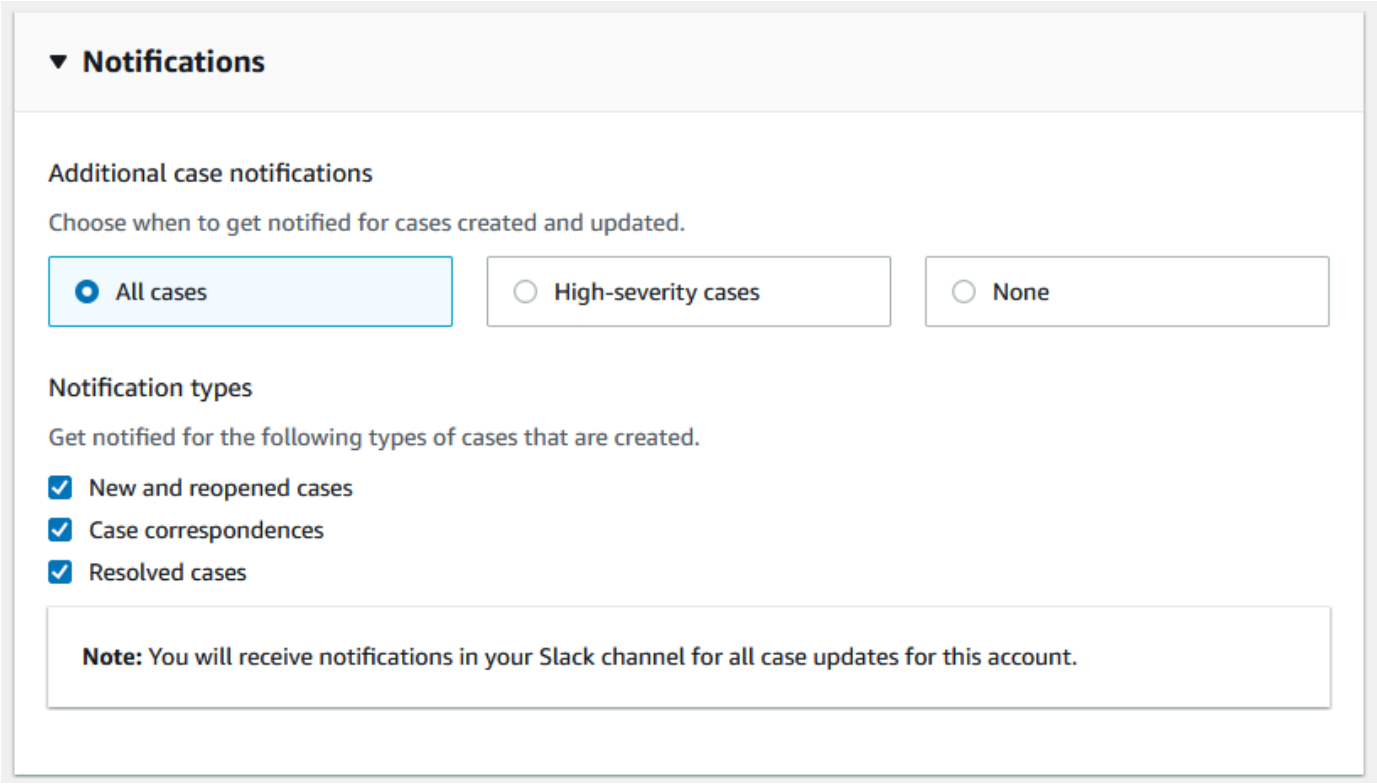
9. [Notifications] (通知) で、ケースの通知を受け取る方法を指定します。

   - [All cases] (すべてのケース) – すべてのケースの更新通知を受け取ります。
   - [High-severity cases] (重要度の高いケース) — 本番システム以上に影響するケースのみ、通知を受け取ります。詳細については、「緊急度の選択」を参照してください。
   - [None] (なし) — ケースの更新に関する通知は受け取りません。

10. (オプション) [All cases] (すべてのケース) または [High-severity cases] (重要度の高いケース) を選択した場合、次のオプションうち 1 つ以上を選択する必要があります。

    - 新規のケースと再オープンしたケース
    - ケースのコレスポンデンス
    - 解決したケース

    次のチャンネルは、Slack におけるすべてのケース更新のケース通知を受け取ります。



11. 設定を確認し、[Add channel] (チャンネルを追加) を選択します。チャンネルが [Slack configuration] (Slack の設定) ページに表示されます。

Slack チャンネルの設定を更新する

Slack チャンネルを設定したら、後でそれらを更新して、IAM ロールやケース通知を変更できます。

Slack チャンネルの設定を更新するには

1. サポートセンターコンソールにサインインし、[Slack configuration] (Slack の設定) を選択します。
2. [Channels] (チャンネル) で、希望するチャンネル設定を選択します。
3. ***[channelName]*** ページでは、次のタスクを実行できます。
   - チャンネル設定の名前を更新するときは、[Rename] (名前の変更) を選択します。この名前は にのみ表示 AWS アカウント され、Slack には表示されません。
   - 削除を選択して、 AWS サポート アプリからチャネル設定を削除します。「AWS サポートアプリからの Slack チャンネル設定の削除」を参照してください。
   - ブラウザで Slack チャンネルを開くときは、[Open in Slack] (Slack で開く) を選択します。
   - IAM ロールまたは通知を変更するときは、[Edit] (編集) を選択します。

Slack チャンネルでのサポートケースの作成

Slack ワークスペースを認可して Slack チャンネルを追加すると、Slack チャンネルでサポートケースを作成できます。

Slack でサポートケースを作成するには

1. Slack チャンネルで、次のコマンドを入力します。

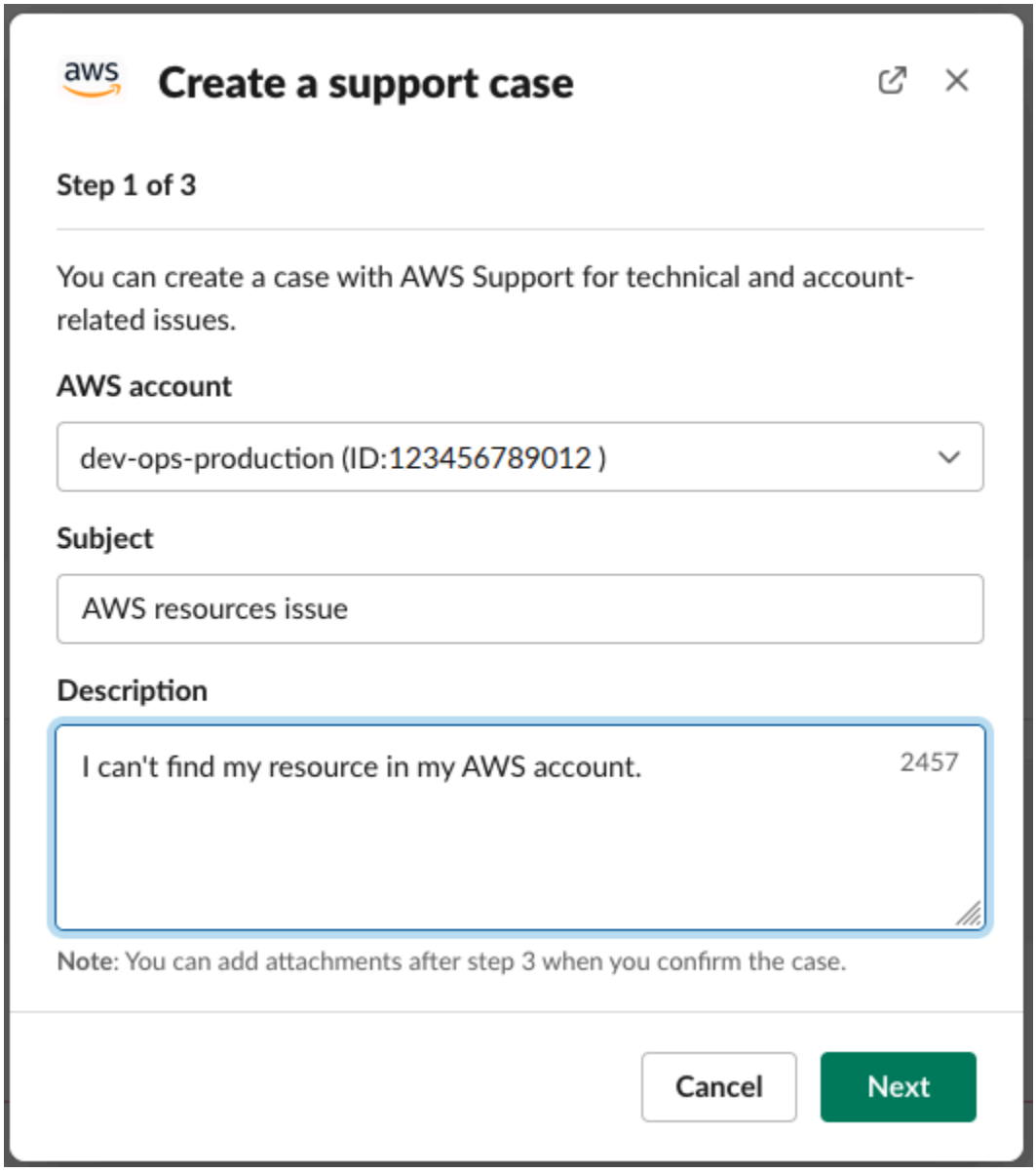
   ```
   /awssupport create
   ```

2. [Create a support case] (サポートケースを作成) ダイアログボックスで、以下を行います。

   a. この Slack チャンネルで複数のアカウントを設定した場合は、[AWS アカウント] で、アカウント ID を選択します。アカウント名を作成した場合は、この値はアカウント ID の横に表示されます。詳細については、「Slack ワークスペースを承認する」を参照してください。

   b. [Subject] (件名) にサポートケースのタイトルを入力します。

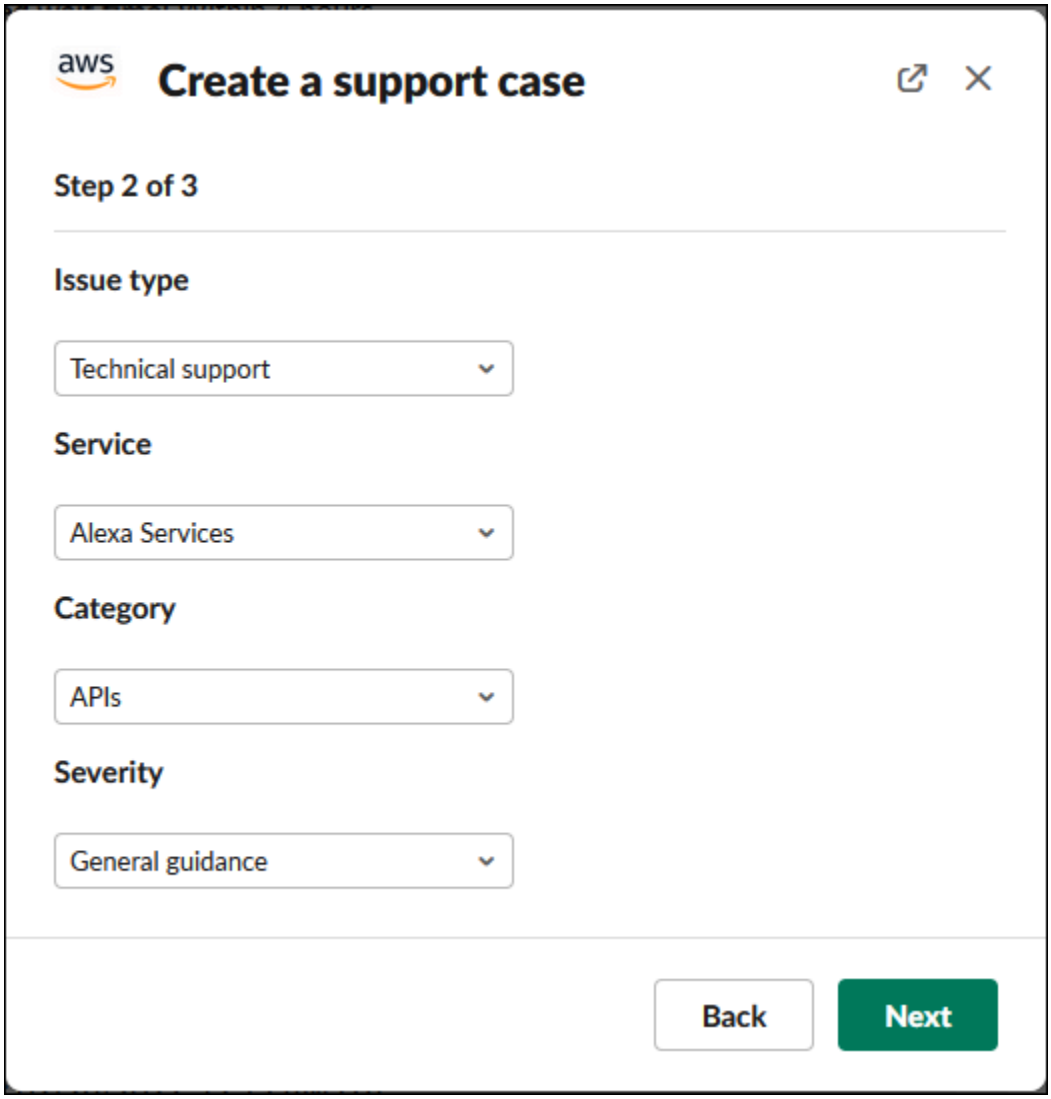
   c. [Case description] (ケースの説明) に、サポートケースの説明を入力します。の使用方法 AWS のサービス や、試したトラブルシューティング手順などの詳細を入力します。



3. [Next (次へ)] を選択します。
4. [Create a support case] (サポートケースを作成) ダイアログボックスで、以下のオプションを指定します。

   a. [Issue type] (問題のタイプ) を選択します。
   b. [Service] (サービス) を選択します。
   c. [Category] (カテゴリ) を選択します。
   d. [Severity] (重要度) を選択します。
   e. ケースの詳細を確認したら、[Next] (次へ) を選択します。

      次の例は、Alexa サービスのテクニカルサポートケースを示しています。

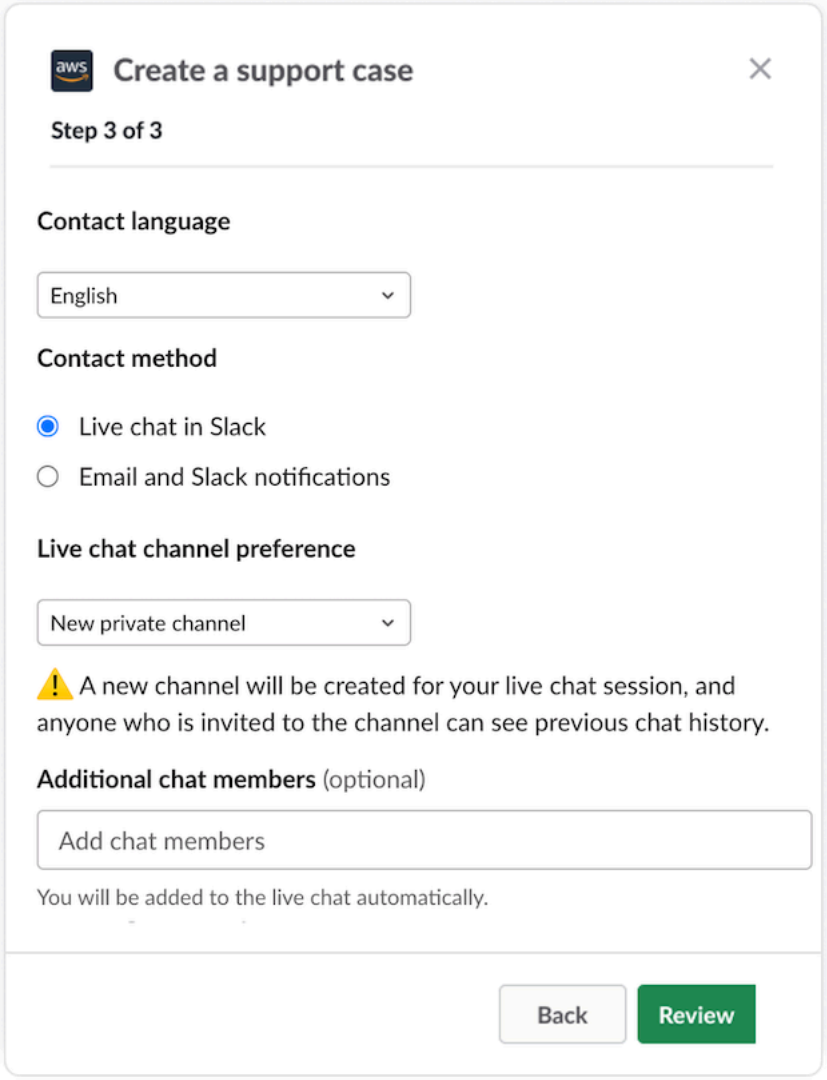


5. [Contact language] (連絡用言語) で、サポートケースの使用する言語を選択します。

> **Note**
>
> Slack でのアカウントおよび請求に関するライブチャットでは、日本語のサポートは利用できません。

6. [Contact method] (連絡方法) で、[Email and Slack notifications] (E メールと Slack 通知) または [Live chat in Slack] (Slack でのライブチャット) を選択します。

   次の例は、Slack でライブチャットを選択する方法を示しています。



a. [Slack でのライブチャット] を選択した場合は、[ライブチャットのチャンネル設定] として [新しいプライベートチャンネル] または [現在のチャンネル] を選択します。新しいプライベートチャネルでは、 AWS サポート エージェントとチャットするための別のプライベートチャネルが作成され、現在のチャネルでは AWS サポート 、エージェントとチャットするための現在のチャネルのスレッドが使用されます。

b. (オプション) [Live chat in Slack] (Slack でのライブチャット) を選択した場合は、他の Slack メンバーの名前を入力できます。新しいプライベートチャネルの場合、 AWS サポート アプリはユーザーと選択したメンバーを新しいチャネルに自動的に追加します。現在のチャネルの場合、 AWS サポート エージェントが参加すると、 AWS サポート アプリはチャットスレッド内のユーザーと選択したメンバーに自動的にタグ付けします。

> **Important**
>
> - 追加するチャットメンバーは、サポートケースの詳細とチャット履歴にアクセスさせたいメンバーのみにすることをお勧めします。
> - 既存のサポートケースで新しいライブチャットセッションを開始すると、 AWS サポート アプリは以前のライブチャットで使用されたのと同じチャットチャネルまたはスレッドを使用します。 AWS サポート アプリは、以前に使用されたものと同じライブチャットチャネル設定も使用します。
> - [現在のチャンネル] オプションは、プライベートチャンネルからチャットがリクエストされた場合にのみ使用できます。このオプションは、チャンネルメンバー全員にチャットへのアクセスを許可する場合のみにすることをお勧めします。

7. (オプション) [Additional contacts to notify] (通知する追加連絡先) に、このサポートケースに関する更新を受け取る E メールアドレスを入力します。最大 10 件のアドレスを追加できます。
8. [Review] (レビュー) を選択します。
9. Slack チャンネルで、ケースの詳細を確認します。以下の操作を行うことができます。
   - ケースの詳細を変更するときは、[Edit] (編集) を選択します。
   - ファイルをケースに追加します。そのためには、以下の手順を実行します。
     a. [Attach file] (ファイルを添付) を選択し、Slack の [+] をクリックし、[Your computer] (お使いのコンピュータ) を選択します。
     b. ファイルに移動して、選択します。
     c. [Upload a file] (ファイルのアップロード) ダイアログボックスで、`@awssupport` を入力し、メッセージ送信の  をクリックします。

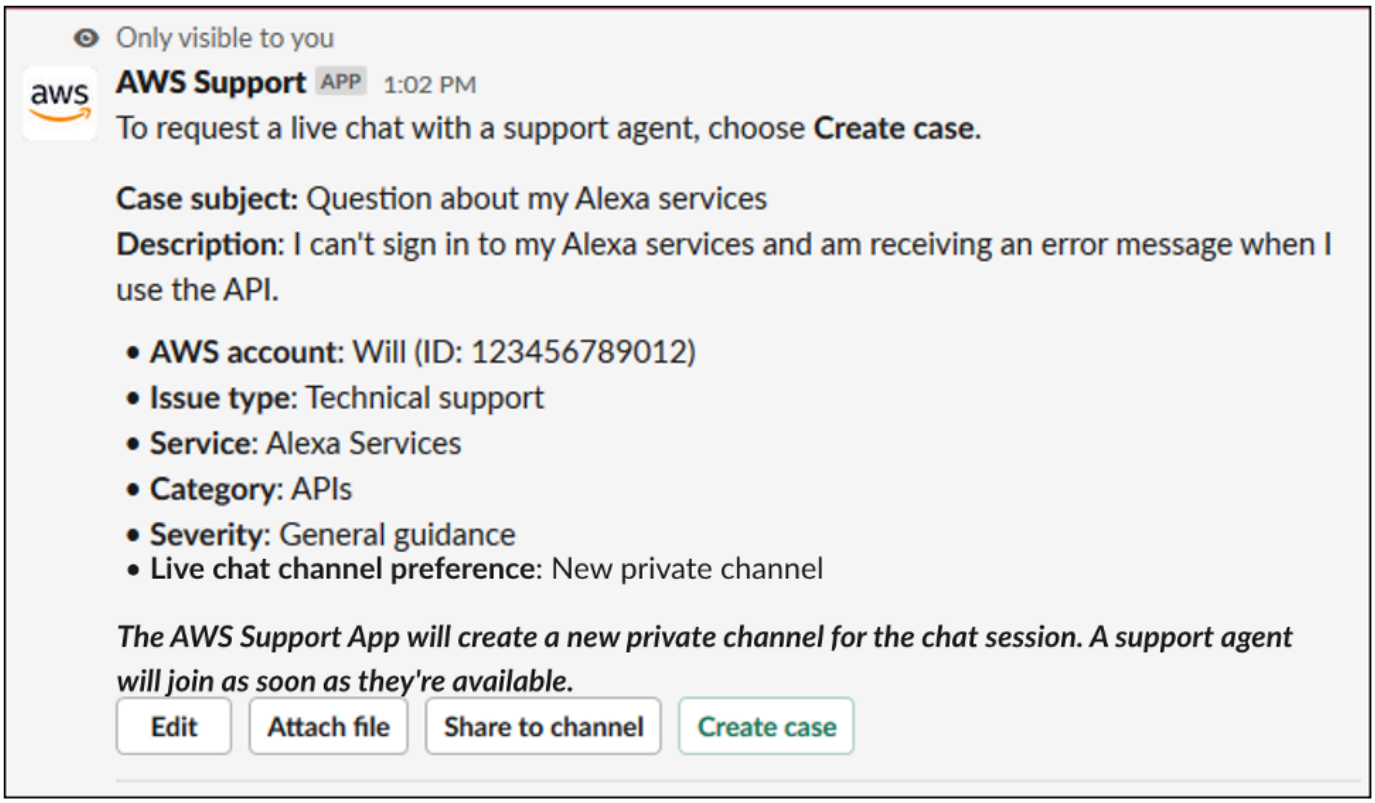
> **メモ**
>
> - 最大 3 つまでのファイルをアタッチできます。各ファイルは、最大 5MB まで可能です。

- サポートケースにファイルをアタッチするときは、1 時間以内にケースを送信する必要があります。送信しない場合は、ファイルを再度追加する必要があります。

- [Share to channel] (チャンネルに共有) を選択し、ケースの詳細を Slack チャンネルにいる他者と共有します。このオプションを使用すると、ケースを作成する前にケースの詳細をチームと共有することができます。

10. ケースの詳細を確認し、[Create case] (ケースを作成) を選択します。

次の例は、Alexa サービスのテクニカルサポートケースを示しています。



サポートケースを作成した後にケースの詳細が表示されるまで、数分かかる場合があります。

11. サポートケースが更新されたら、[See details] (詳細を表示) を選択するとケースの情報を確認できます。続いて、次の操作を行います。

- [Share to channel] (チャンネルに共有) を選択し、ケースの詳細を Slack チャンネルにいる他者と共有します。
- [Reply] (返信) を選択し、コレスポンデンスを追加します。
- [Resolve case] (ケースを解決) を選択します。

> **Note**
>
> Slack でケースの自動更新の受け取りを選択していない場合、サポートケースを検索すれば [See details] (詳細を表示) オプションが見つかります。

Slack でのサポートケースへの返信

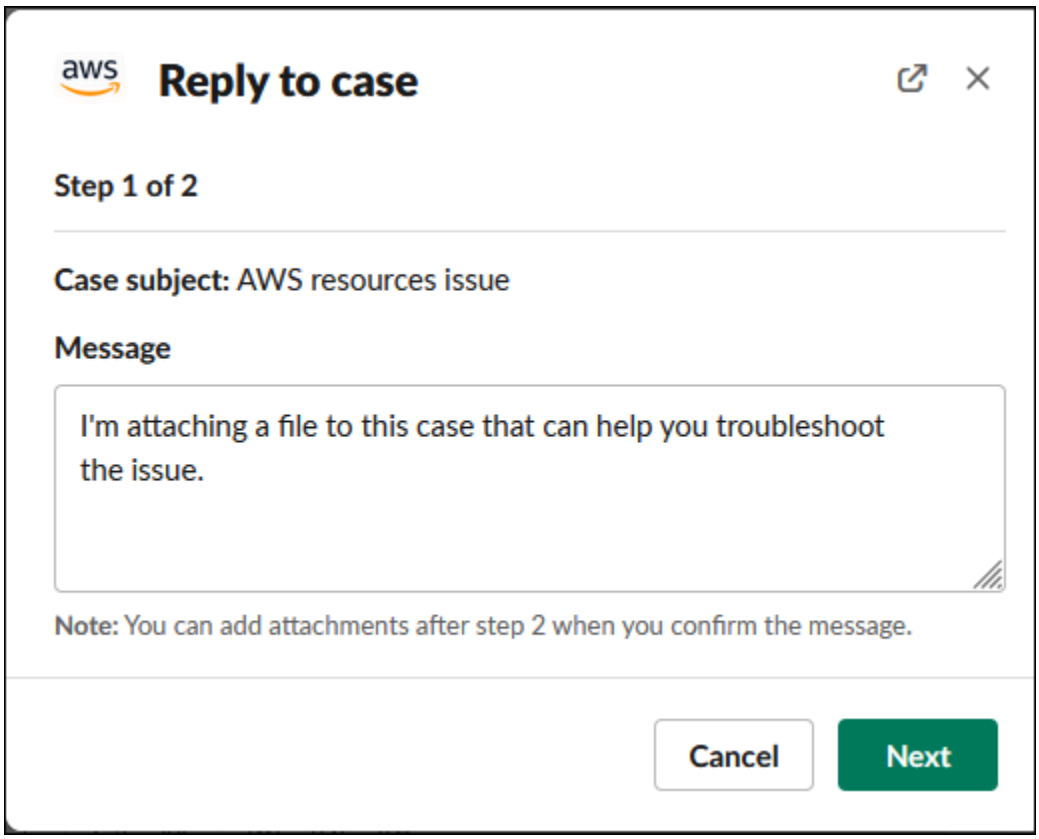
ケースには、ケースの詳細や添付ファイルなどの更新を追加できます。また、サポートエージェントからの応答に返信することもできます。

> **Note**
>
> - を使用してサポートエージェントに AWS Support Center Console 返信することもできます。詳細については、「ケースの更新、解決、および再開」を参照してください。
> - AWS サポート アプリによって作成されたチャットチャネルからケースにコレスポンデンスを追加することはできません。ライブチャットチャネルがエージェントにメッセージを送信するのはライブチャット中のみです。

Slack でサポートケースに返信するには

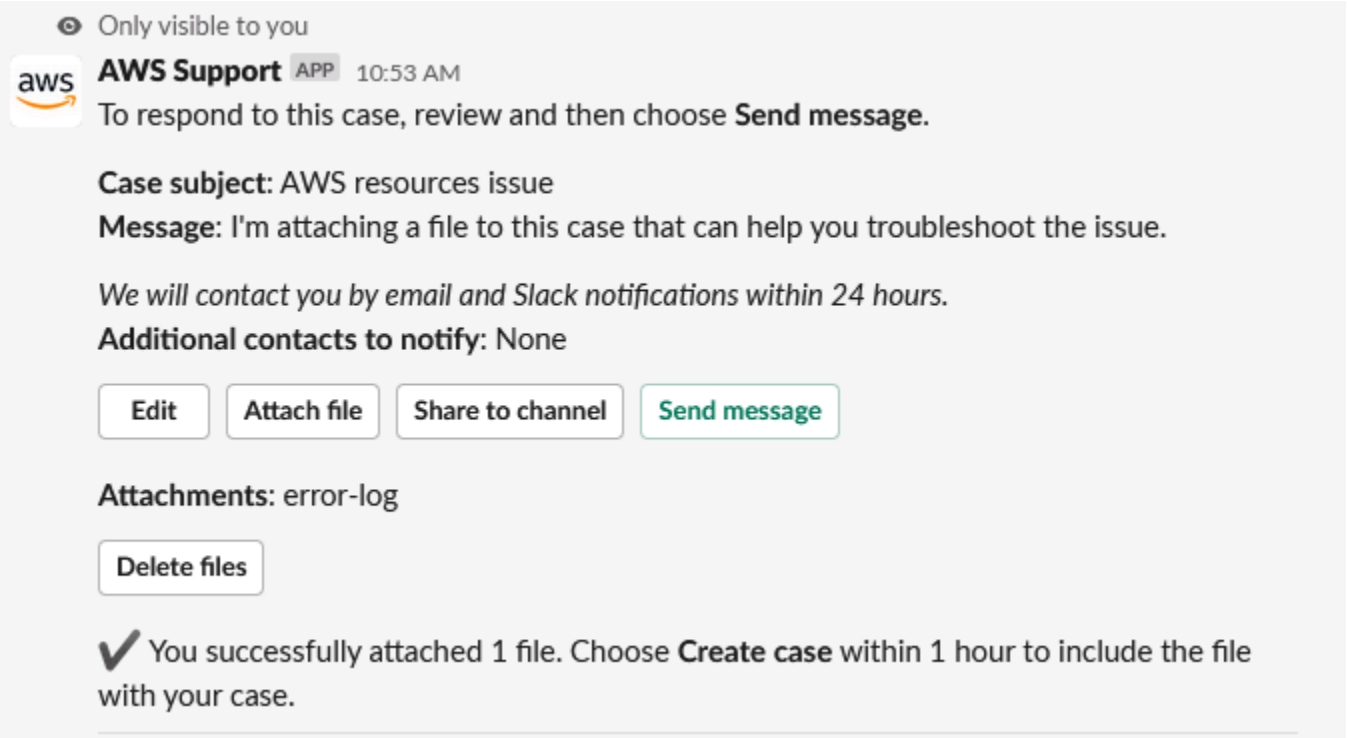
1. Slack チャンネルで、返信するケースを選択します。`/awssupport search` を入力すると、自分のサポートケースを見つけられます。
2. 当該のケースの横にある [See details] (詳細を表示) を選択します。
3. ケースの詳細の下部にある、[Reply] (返信) を選択します。

4. [Reply to case] (ケースに返信) ダイアログボックスの [Message] (メッセージ) フィールドに、問題の簡単な説明を入力します。次いで、[次へ] を選択します。



5. 連絡方法を選択します。利用可能な連絡方法は、ケースの種類とサポートプランに応じて異なります。
6. (オプション) [Additional contacts to notify] (通知の追加連絡先) に、このサポートケースに関する更新を受け取るメールアドレスを追加します。最大 10 件のアドレスを追加できます。
7. [Review] (レビュー) を選択します。その後、返信を編集するか、ファイルをアタッチするか、チャンネルに共有するかを選択できます。
8. 返信の準備ができたら、[Send message] (メッセージを送信) をクリックします。
9. (オプション) ケースの過去のコレスポンデンスを表示するには、[Previous correspondence] (過去のコレスポンデンス) を選択します。短縮されたメッセージをすべて表示するには、[Show full message] (メッセージ全体を表示) を選択します。

Example : Slack でケースに返信する



とのライブチャットセッションに参加する サポート

ケースのライブチャットをリクエストするときは、新しいチャットチャネルを使用するか、現在のチャネルのスレッドを使用するか、 AWS サポート エージェントを選択します。サポートエージェントや、ライブチャットに招待したその他ユーザーとやり取りをするときは、このチャットチャンネルまたはスレッドを使用します。

> **Important**
>
> このライブチャットのチャンネルに参加している人なら誰でも、この特定のサポートケースの詳細を閲覧できます。サポートケースへのアクセスを必要とするユーザーのみを追加するのがベストプラクティスです。チャットチャンネルやスレッドのメンバーなら誰でも、アクティブなチャットに参加できます。

> **Note**
>
> ライブチャットチャネルとスレッドは、ライブチャットセッションの外でケースにコレスポンデンスが追加されると、通知も受け取ります。これはチャットセッションの前、最中、

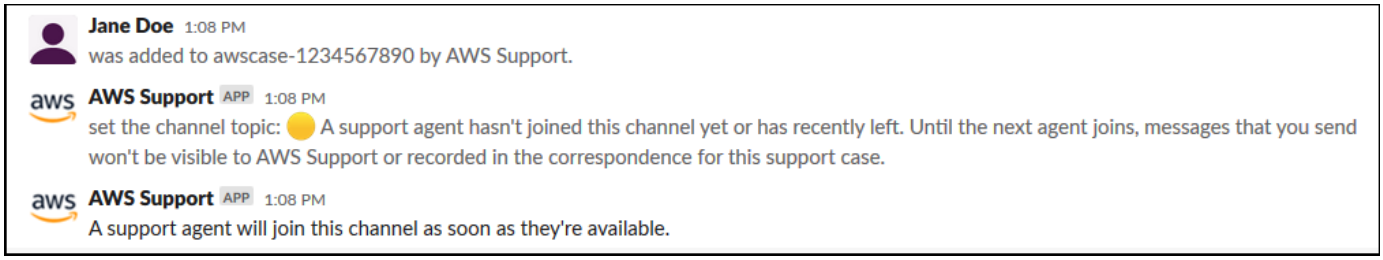
および後に発生するため、チャットチャネルまたはスレッドを使用してケースのすべての更新をモニタリングできます。新しいチャットチャネルを使用することを選択した場合は、AWS サポート アプリを招待した設定チャネルを使用して、これらのコレスポンデンスに返信します。

新しいチャネル サポート で とのライブチャットセッションに参加するには

1. Slack アプリケーションで、 AWS サポート アプリが作成するチャネルに移動します。チャンネル名には、ユーザーのサポートケース ID が含まれます (例: *awscase-1234567890*) が含まれます。

   > **Note**
   >
   > AWS サポート アプリは、サポートケースの詳細を含むピン留めされたメッセージをライブチャットチャネルに追加します。ピン留めされたメッセージから、チャットを終了したりケースを解決したりできます。このチャンネル内のピン留めされたメッセージは、チャンネル名の下にすべて表示されます。

2. サポートエージェントがチャンネルに参加したときは、サポートケースについてチャットすることができます。サポートエージェントがチャネルに参加するまで、エージェントはそのチャットにメッセージを表示せず、メッセージはケースコレスポンデンスに表示されません。

3. (オプション) チャットチャンネルに他のメンバーを追加します。デフォルトでは、チャットチャンネルはプライベートになっています。

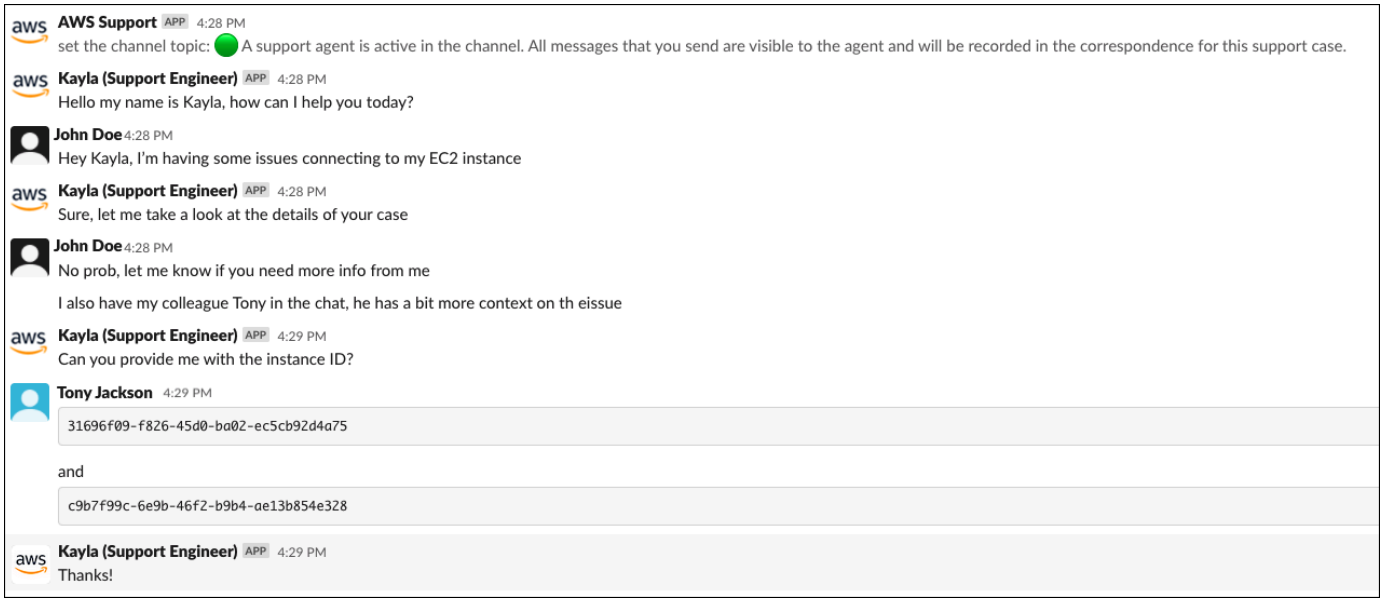
4. サポートエージェントがチャットに参加すると、チャットチャンネルがアクティブになり、AWS サポート アプリがチャットを記録します。

   エージェントとサポートケースについてチャットしたり、添付ファイルをチャンネルにアップロードしたりできます。 AWS サポート アプリは、ファイルとチャットログをケースコレスポンデンスに自動的に保存します。

> **Note**
>
> サポートエージェントとチャットするときは、Slack for the AWS サポート App の次の違いに注意してください。
>
> - サポートエージェントは、共有されたメッセージやスレッドを閲覧できません。メッセージまたはスレッドのテキストを共有するときは、テキストを新規メッセージとして入力します。
> - メッセージの編集や削除を行っても、エージェントは元のメッセージを引き続き閲覧できます。更新されたものを表示するには、新規メッセージをもう一度入力する必要があります。

Example : ライブチャットセッション

以下は、2 つの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにおける接続上の問題を修正する、サポートエージェントとのライブチャットセッションの例を示したものです。

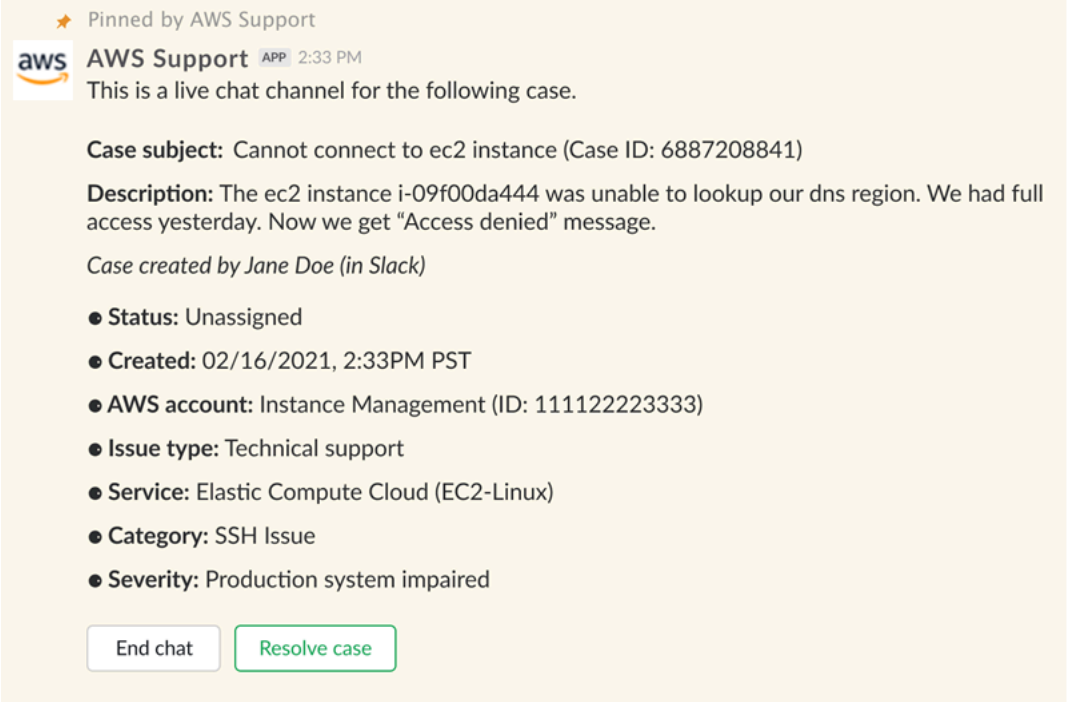


5. (オプション) ライブチャットを停止するには、[End chat] (チャットを終了) を選択します。サポートエージェントはチャネルを離れ、 AWS サポート アプリはライブチャットの記録を停止します。このサポートケースのケースコレスポンデンスに添付されたチャット履歴をご確認いただけます。

6. 問題が解決したら、ピン留めされたメッセージで [Resolve case] (ケースを解決する) をクリックするか、`/awssupport resolve` を入力します。

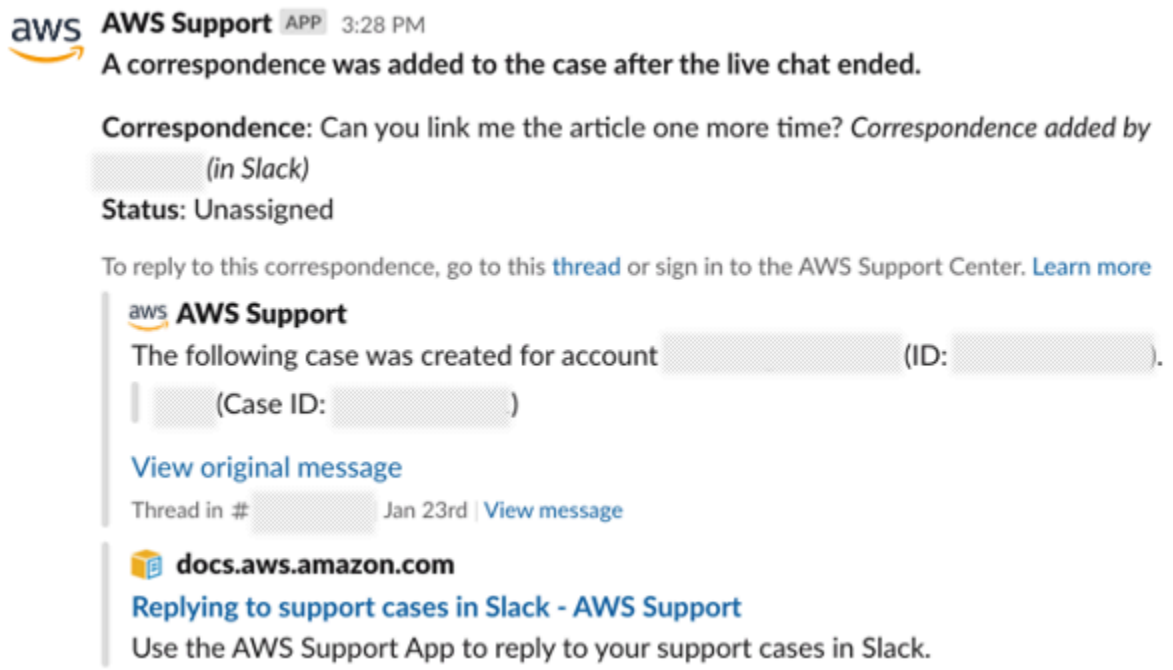
   Example : ライブチャットを終了する

   次のピン留めされたメッセージは、Amazon EC2 インスタンスに関するケースの詳細を示しています。ピン留めされたメッセージは、Slack チャンネル名の下で確認できます。



   Example : チャットチャネルでのコレスポンデンス通知

   以下は、チャットが終了した後に別の共同編集者が更新を追加した場合に通知を受け取ったライブチャットチャンネルの例です。

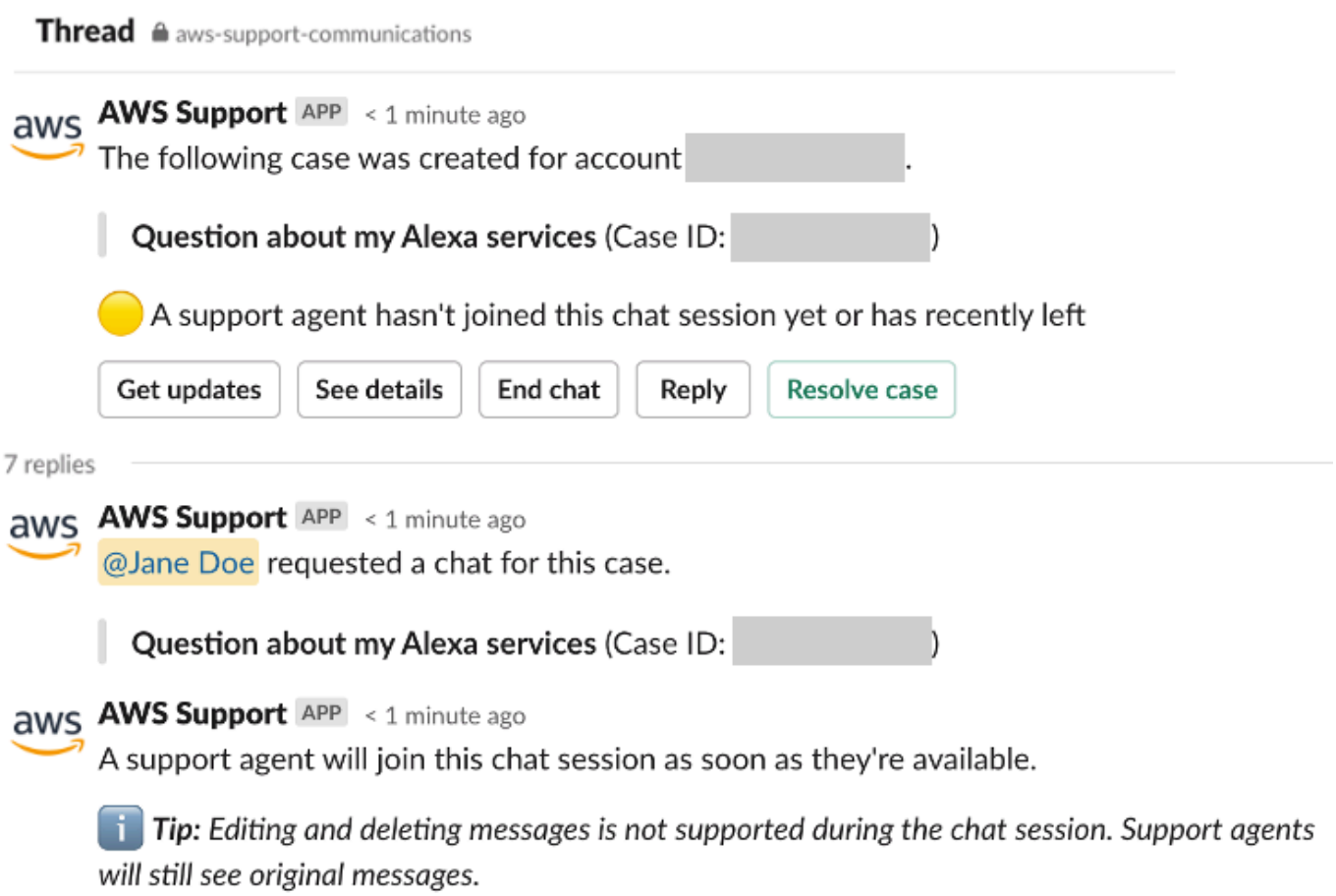


通知には、チャットのステータス (リクエスト済み、進行中、終了済み) 、およびコレスポンデンスがエージェントによって追加されたのか別の共同作業者によって追加されたのかが示されます。Support アプリは、このチャットがリクエストされた元の Slack スレッドまたはチャンネルへのリンク設定も試みます。このケースには、そのチャネル、またはこのケースにアクセスできる他のチャネルから返信できます。

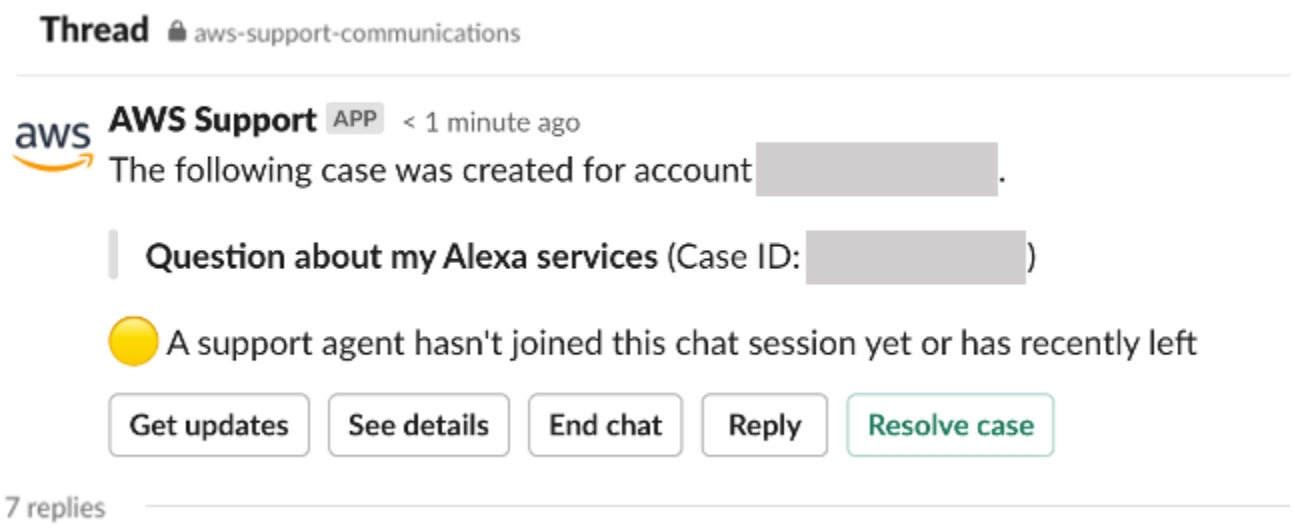
現在のチャネル サポート で とのライブチャットセッションに参加するには

1. Slack アプリケーションで、 AWS サポート アプリがチャットに使用する現在のチャネルのスレッドに移動します。ほとんどの場合、これはケースが最初に作成されたときに開始されたスレッドになります。
2. サポートエージェントがチャンネルに参加すると、サポートケースについてチャットできます。サポートエージェントがチャンネルに参加するまでは、エージェントはそのチャットのメッセージを閲覧できず、チャットが終了すると、メッセージはケースコレスポンデンスに表示されません。

> **Note**
>
> チャットスレッドの外部でこのチャネルに送信されたメッセージは サポート、チャットがアクティブであっても、 によって表示されることはありません。



3. (オプション) 他のチャンネルメンバーにタグを付けて、チャットスレッドで通知します。
4. サポートエージェントがチャットに参加すると、チャットスレッドがアクティブになり、 AWS サポート アプリはチャットを記録します。新しいチャットチャネルのオプションと同様に、エージェントとサポートケースについてチャットしたり、添付ファイルをスレッドにアップロードしたりできます。 AWS サポート アプリは、ファイルとチャットログをケースコレスポンデンスに自動的に保存します。
5. (オプション) ライブチャットを停止するには、このスレッドの最初のメッセージで [チャットを終了] を選択します。サポートエージェントはスレッドを離れ、 AWS サポート アプリはライブチャットの記録を停止します。このサポートケースのケースコレスポンデンスに添付されたチャット履歴をご確認いただけます。
6. 問題が解決したら、このスレッドの最初のメッセージで [ケースの解決] を選択できます。



Slack でのサポートケースの検索

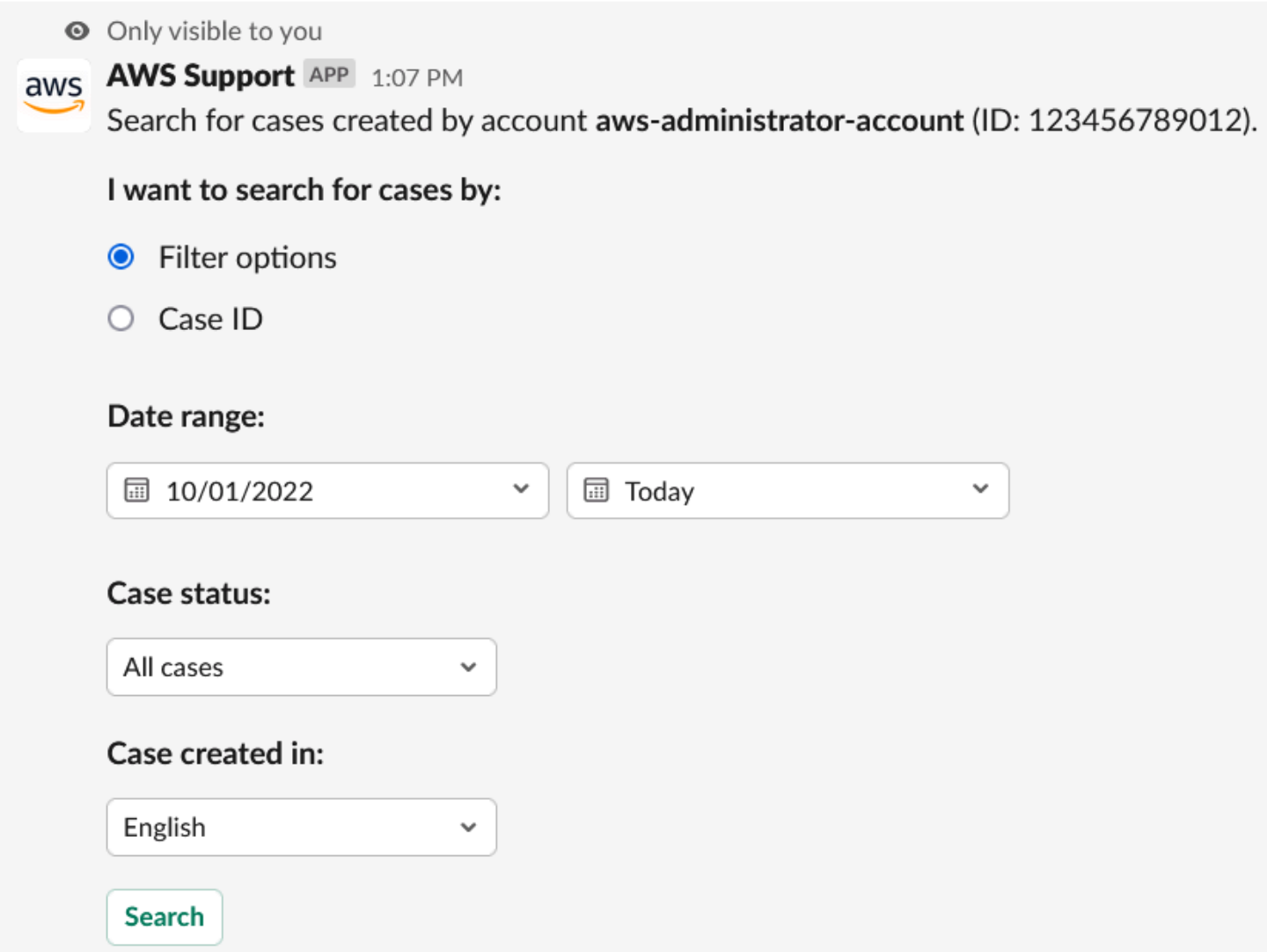
Slack チャンネルから、 および同じチャンネル AWS アカウント とワークスペースを設定した他のアカウントからサポートケースを検索できます。例えば、アカウント (123456789012) と同僚のアカウント (111122223333) が で同じワークスペースとチャネルを設定している場合 AWS Support Center Console、 AWS サポート アプリを使用して互いのサポートケースを検索できます。

検索結果を絞り込むには、次のオプションを使用できます。

- アカウント ID
- ケース ID
- ケースのステータス
- 連絡用言語
- 日付範囲

Example : Slack でのケースの検索

次の例は、日付範囲、ケースステータス、および連絡用言語を指定して、単一のアカウントを [Filter options] (フィルターオプション) で検索する方法を示しています。



Slack でサポートケースを検索するには

1. Slack チャンネルで次のコマンドを入力します。

   ```
   /awssupport search
   ```

2. [I want to search for cases by:] (ケースを次の条件で検索する:) オプションで、次のいずれかを選択します。

   A. [Filter options] (フィルターオプション) – 次のオプションを使用してケースをフィルタリングできます。

   - [AWS アカウント] – このリストは、チャンネルに複数のアカウントがある場合にのみ表示されます。
   - [Date range] (日付範囲) – ケースが作成された日付です。

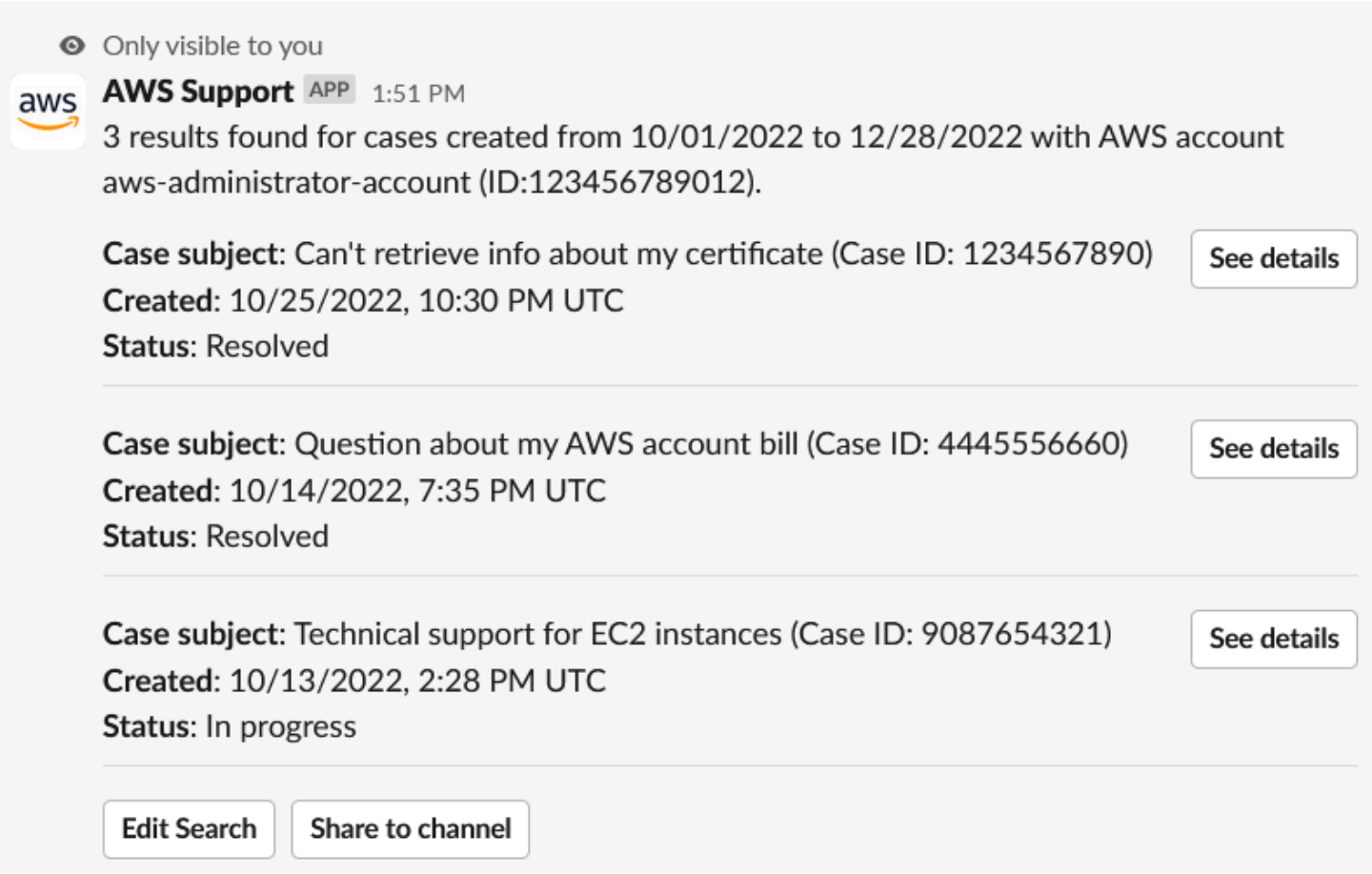
- [Case status] (ケースのステータス) – [All open cases] (すべてのオープンケース) や [Resolved] (解決済み) など、現在のケースステータスです。
- [Case created in] (ケースの作成言語) – ケースの連絡先の言語です。

B. [Case ID] (ケース ID) – ケース ID を入力します。一度に入力できるケース ID は 1 つだけです。チャネルに複数のアカウントがある場合は、 を選択してケース AWS アカウント を検索します。

3. [検索] を選択してください。検索結果は Slack に表示されます。

検索結果の使用

次の例では、1 つの AWS アカウントから 3 件のサポートケースが返されています。



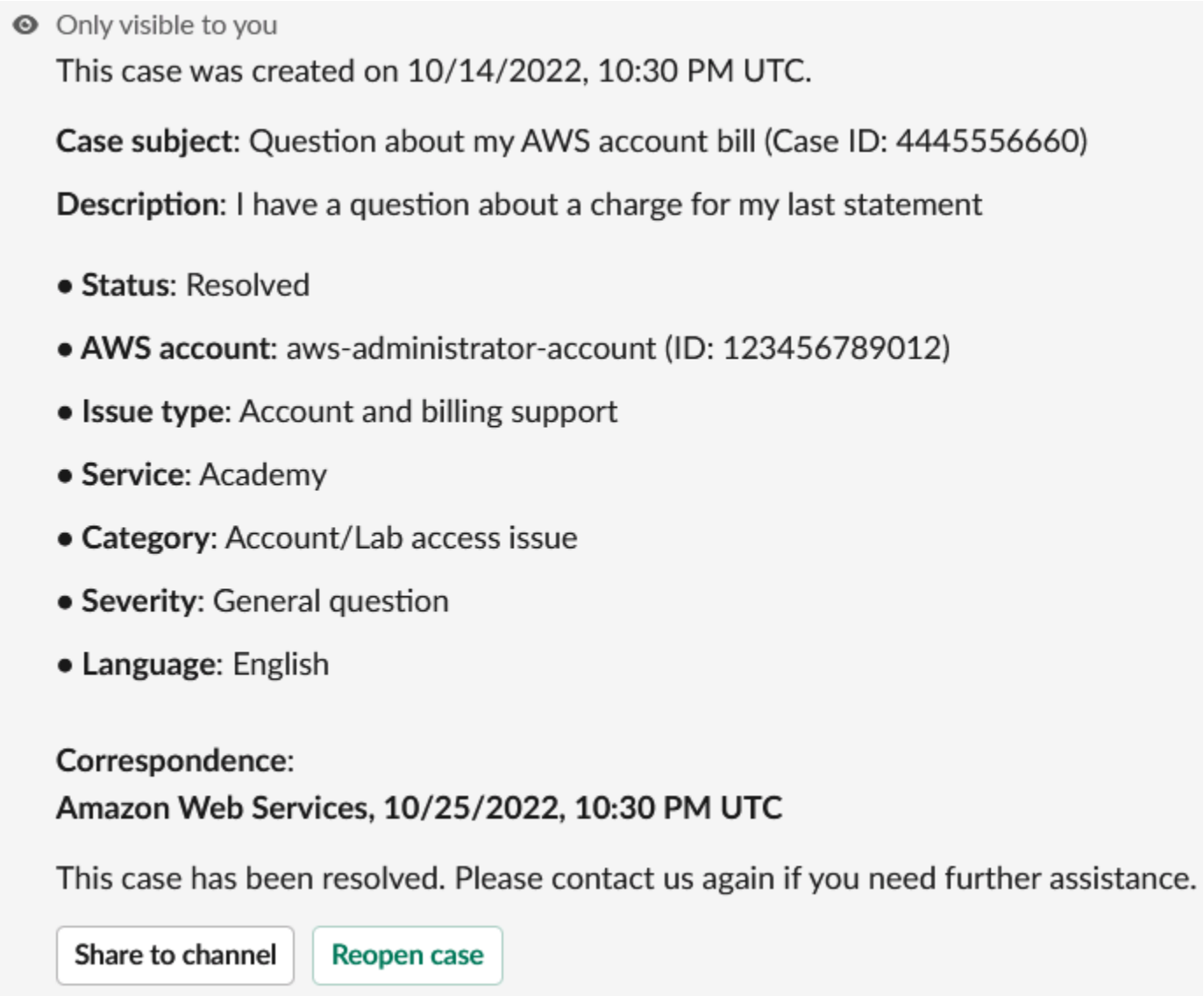
検索結果を受け取ったら、次の手順を実行できます。

検索結果を使用するには

1. [Edit Search] (検索を編集) を選択して、以前のフィルターオプションまたはケース ID を変更します。
2. [Share to channel] (チャンネルに共有) を選択して、検索結果をチャンネルに共有できます。
3. ケースの詳細については、[See details] (詳細を表示) を選択します。[Show full message] (メッセージ全体を表示) を選択すると、最新のコレスポンデンスの残りを表示できます。
4. [Filter options] (フィルターオプション) で検索した場合、検索結果に複数のケースが返される場合があります。[Next 5 results] (次の 5 つの結果) または [Previous 5 results] (前の 5 つの結果) を選択して、次または前の 5 つのケースを表示します。

Example : サポートケースを解決する

次の例は、[See details] (詳細を表示) を選択した後に、アカウントと請求に関する問題を解決したサポートケースを示しています。



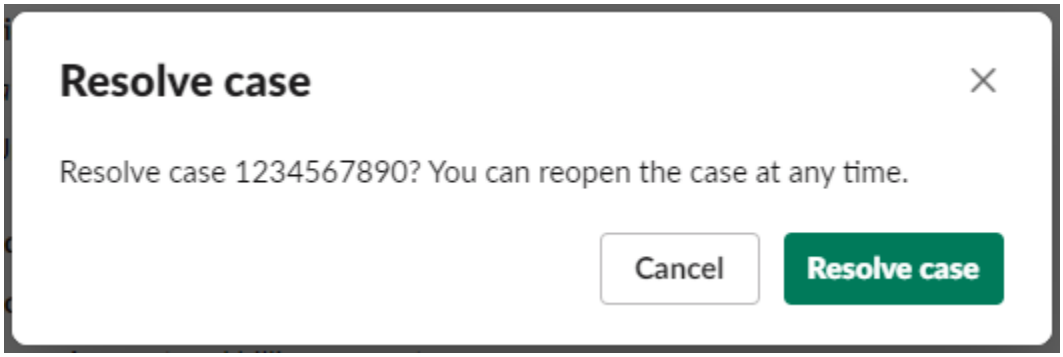
Slack でのサポートケースの解決

サポートケースが不要になったときや、問題が修正されたときは、Slack で直接サポートケースを解決できます。これにより、 AWS Support Center Consoleでもケースが解決されます。解決したケースは、後で再オープンできます。

Slack でサポートケースを解決するには

1. Slack チャンネルで、サポートケースを表示します。「Slack でのサポートケースの検索」を参照してください。
2. ケースの [See details] (詳細を表示) を選択します。
3. [Resolve case] (ケースを解決) を選択します。

4. [Resolve case] (ケースを解決) ダイアログボックスで、[Resolve case] (ケースを解決) を選択します。Slack チャンネルまたはサポートセンターのコンソールから、ケースを再オープンできます。

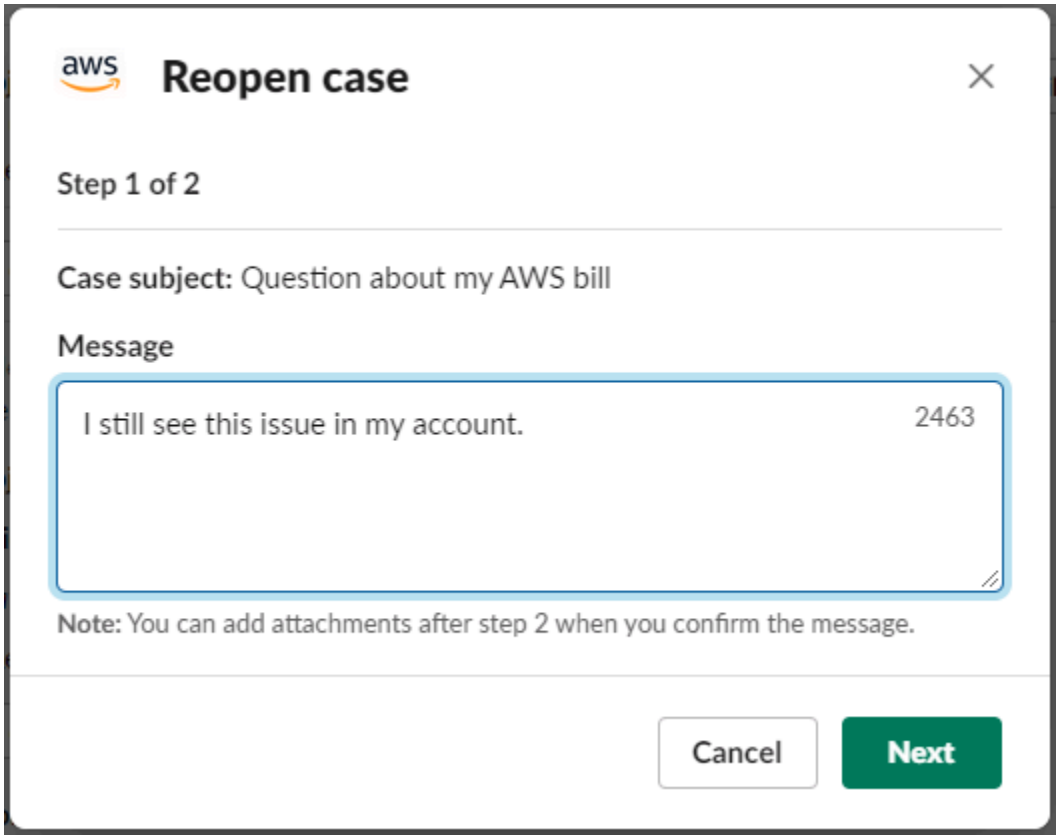


Slack でのサポートケースの再オープン

サポートケースを解決すると、Slack からケースを再オープンできます。

Slack でサポートケースを再オープンするには

1. Slack で再オープンするサポートケースを見つけます。「Slack でのサポートケースの検索」を参照してください。
2. [See Details] (詳細を表示) を選択します。
3. [Reopen case] (ケースを再度開く) を選択します。
4. [Reopen case] (ケースを再オープンする) ダイアログボックスの [Message] (メッセージ) フィールドに、問題の簡単な説明を入力します。
5. [Next (次へ)] を選択します。



6. (オプション) 追加の連絡先を入力します。
7. [Review] (レビュー) を選択します。
8. ケースの詳細を確認し、[Submit message] (メッセージを送信) を選択します。ケースが再オープンします。サポートエージェントとの新しいライブチャットをリクエストすると、Slack は、以前のライブチャットで使用されたのと同じチャットチャンネルまたはスレッドを使用します。新しいチャンネルで初めてライブチャットをリクエストした場合は、新しいチャットチャンネルが開きます。現在のチャンネルで初めてライブチャットをリクエストした場合は、現在のチャンネル内のスレッドが使用されます。

サービスクォータの引き上げリクエスト

Slack チャンネルからアカウントのサービスクォータの引き上げをリクエストできます。

サービスクォータの引き上げをリクエストする

1. Slack チャンネルで次のコマンドを入力します。

```
/awssupport quota
```

2. [Increase service quota] (サービスクォータを引き上げる) ダイアログボックスに次の情報を入力します。

   a. [AWS アカウント] を選択します。

   b. [AWS リージョン] を選択します。

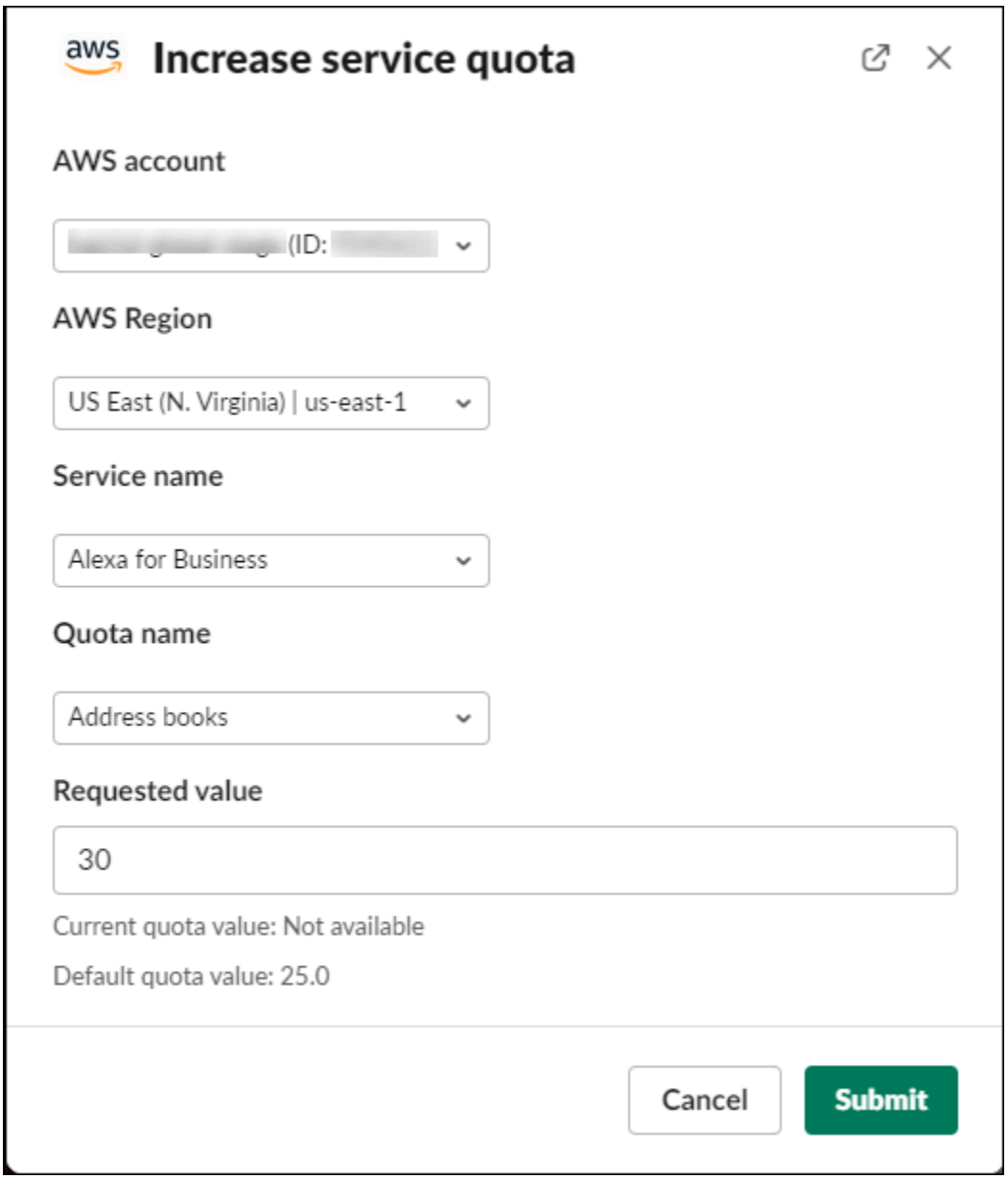
   c. [Service Name] (サービス名) を選択します。

   d. [Quota name] (クォータ名) を選択します。

   e. クォータ引き上げの [Requested value] (リクエスト値) を入力します。必ず、デフォルトのクォータよりも大きい値を入力します。

3. [送信] を選択します。

Example : Alexa for Business のクォータ引き上げ



自分が行ったリクエストは、Service Quotas コンソールからも確認できます。詳細については、「Service Quotasユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

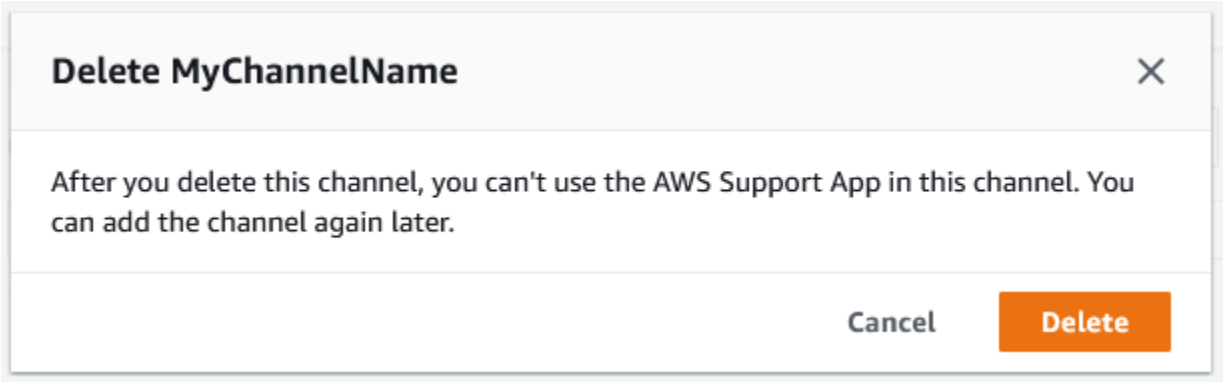
AWS サポート アプリからの Slack チャンネル設定の削除

不要なチャネル設定は、 AWS サポート アプリから削除できます。このアクションは、 AWS サポート アプリと からのみチャネルを削除します AWS Support Center Console。Slack からは削除しません。

AWS アカウントにはチャンネルを 20 件まで追加できます。既にこのクォータに達している場合は、新たに追加する前にチャンネルを削除する必要があります。

Slack チャンネル設定を削除するには

1. サポートセンターコンソールにサインインし、[Slack configuration] (Slack の設定) を選択します。
2. [Slack configuration] (Slack の設定) ページの [Channels] (チャンネル) で、チャンネル名を選択し、[Delete] (削除) を選択します。
3. [Delete channel name] (チャンネル名を削除) ダイアログボックスで、[Delete] (削除) を選択します。このチャネルは、後で再度 AWS サポート アプリに追加できます。



AWS サポート アプリからの Slack ワークスペース設定の削除

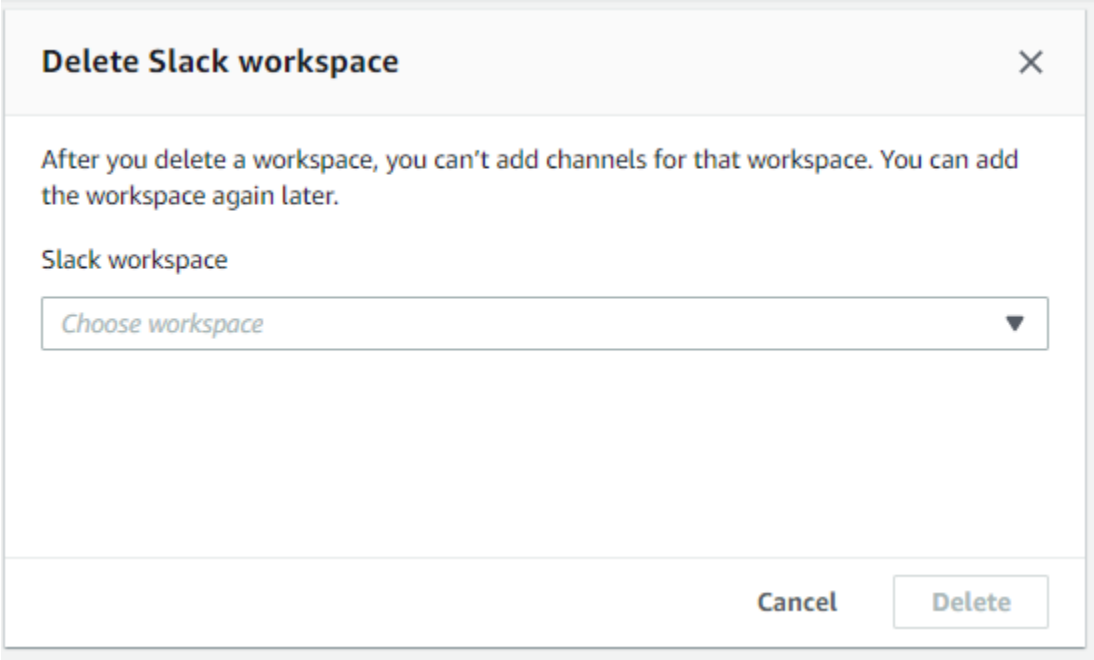
不要なワークスペース設定は、 AWS サポート アプリから削除できます。このアクションは、 AWS サポート アプリと からワークスペースのみを削除します AWS Support Center Console。Slack からは削除されません。

AWS アカウントにはワークスペースを 5 つまで追加できます。既にこのクォータに達している場合は、新たに追加する前に Slack ワークスペースを削除する必要があります。

> **Note**
>
> このワークスペースから AWS サポート アプリにチャネルを追加した場合は、ワークスペースを削除する前に、まずこれらのチャネルを削除する必要があります。「AWS サポート アプリからの Slack チャンネル設定の削除」を参照してください。

Slack ワークスペース設定を削除するには

1. AWS Support Center Console にサインインし、[Slack configuration] (Slack の設定) を選択します。
2. [Slack configuration] (Slack の設定) ページの [Slack workspaces] (Slack ワークスペース) で、[Delete a workspace] (ワークスペースを削除) を選択します。
3. [Delete Slack workspace] (Slack ワークスペースを削除) ダイアログボックスで、Slack ワークスペース名を選択し、[Delete] (削除) を選択します。ワークスペースは後で AWS アカウント 再度に追加できます。



AWS サポート Slack コマンドのアプリ

Slack チャンネルコマンド

AWS サポート アプリを招待した Slack チャンネルには、次のコマンドを入力できます。この Slack チャンネル名は、 AWS Support Center Consoleに、設定済みのチャンネルとしても表示されます。

`/awssupport create`、または `/awssupport create-case`

サポートケースを作成します。

`/awssupport search`、または `/awssupport search-case`

ケースを検索します。同じ Slack チャネルに対して AWS サポート アプリを設定した のサポートケース AWS アカウント を検索できます。

`/awssupport quota`、または `/awssupport service-quota-increase`

サービスクォータの引き上げをリクエストします。

ライブチャットチャンネルコマンド

ライブチャットチャンネルでは、次のコマンドを入力できます。これは、チャットに新しいチャネルを選択した場合に、 AWS サポート アプリが作成するチャネルです サポート。チャットチャンネルには、*awscase-1234567890* のようなサポートケース ID が含まれます。

> **Note**
>
> 次のコマンドは、現在のチャンネルのスレッドをライブチャットに使用する場合には使用できません。代わりに、最初のスレッドメッセージに添付されているボタンを使用して、チャットを終了したり、新しいエージェントを招待したり、ケースを解決したりします。

`/awssupport endchat`

サポートエージェントを削除し、ライブチャットセッションを終了します。

`/awssupport invite`

新しいサポートエージェントをこのチャンネルに招待します。

`/awssupport resolve`

このサポートケースを解決します。

AWS サポート アプリのコレスポンデンスを AWS Support Center Consoleに表示する

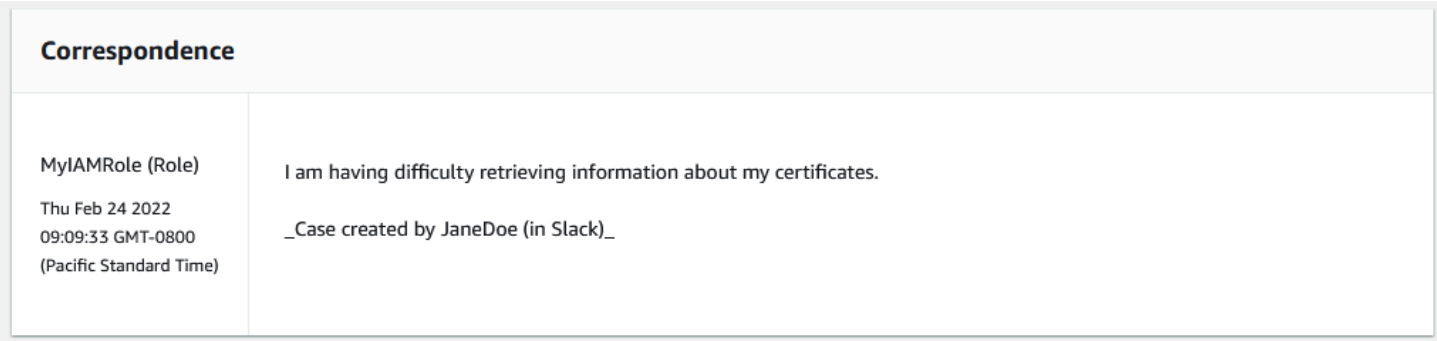
Slack チャンネルでアカウントのサポートケースを作成、更新、解決するときは、サポートセンターコンソールにサインインしてケースを表示することもできます。ケースコレスポンデンスを表示して、ケースが Slack チャンネルで更新されたかどうかを確認したり、サポートエージェントとのチャット履歴を表示したり、Slack からアップロードした添付ファイルを見つけたりできます。

Slack からのケースコレスポンデンスを表示するには

1. アカウントの AWS Support Center Console にサインインします。
2. サポートケースを選択します。
3. [Correspondence] (履歴) では、Slack チャンネルでケースが作成され、更新されたかどうかを確認できます。

Example : サポートケース

次のスクリーンショットでは、Jane Doe が Slack でサポートケースを再オープンしました。このコレスポンデンスは、サポートセンターコンソールのサポートケースに表示されます。



を使用した Slack リソースでの AWS サポート アプリの作成 AWS CloudFormation

AWS サポート Slack のアプリは と統合されています。これは AWS CloudFormation、 AWS リソースとインフラストラクチャの作成と管理に費やす時間を短縮できるように、リソースのモデル化とセットアップを支援するサービスです。必要なすべての AWS リソース (AccountAlias や SlackChannelConfiguration など) を記述するテンプレートを作成すると、 はそれらのリソースを AWS CloudFormation プロビジョニングして設定します。

を使用すると AWS CloudFormation、テンプレートを再利用して AWS サポート アプリリソースを一貫して繰り返しセットアップできます。リソースを 1 回記述し、複数の AWS アカウント およびリージョンで同じリソースを何度もプロビジョニングします。

AWS サポート アプリケーションと AWS CloudFormation テンプレート

AWS サポート アプリおよび関連サービスのリソースをプロビジョニングおよび設定するには、AWS CloudFormation テンプレートを理解する必要があります。テンプレートは、JSON や YAML

でフォーマットされたテキストファイルです。これらのテンプレートは、 AWS CloudFormation スタックにプロビジョニングするリソースを記述します。JSON または YAML に慣れていない場合は、 AWS CloudFormation デザイナーを使用して AWS CloudFormation テンプレートの使用を開始できます。詳細については、「 AWS CloudFormation ユーザーガイド」のAWS CloudFormation「デザイナーとは」を参照してください。

AWS サポート アプリは、 での AccountAlias と SlackChannelConfiguration の作成をサポートしています AWS CloudFormation。AccountAlias と SlackChannelConfiguration リソース向けの JSON および YAML テンプレートの例を含む詳細については、「AWS CloudFormation ユーザーガイド」の「AWS サポート アプリケーションのリソースタイプのリファレンス」を参照してください。

組織用の Slack 設定リソースを作成する

CloudFormation テンプレートを使用して、 AWS サポート アプリケーションに必要なリソースを作成できます。組織の管理者アカウントである場合は、 AWS Organizationsでテンプレートを使用して、メンバーアカウント用にこれらのリソースを作成できます。

例えば、テンプレートを使用して組織内のすべてのアカウントに対して同じ Slack ワークスペース設定を作成し、別のテンプレートを使用して特定の AWS アカウント または組織単位 (OUs) に対して異なる Slack チャネル設定を作成できます。テンプレートを使用して Slack ワークスペース設定を作成して、メンバーアカウントが AWS アカウントの必要な Slack チャンネルを設定できるようにすることもできます。

CloudFormation テンプレートを使用するかどうかを選択できます。CloudFormation テンプレートを使用しない場合は、手動で次の手順を実行できます。

- で AWS サポート アプリリソースを作成します AWS Support Center Console。
- でサポートケースを作成し AWS サポート 、複数のアカウントに AWS サポート アプリの使用を許可します。
- RegisterSlackWorkspaceForOrganization API 操作を呼び出して、アカウントの Slack ワークスペースを登録します。CloudFormation スタックはユーザーに代わってこの API オペレーションを呼び出します。

次の手順に従って、組織で CloudFormation テンプレートをアップロードします。[AWS サポート アプリケーションのリソースタイプのリファレンス] ページで、テンプレートのサンプルを使用できます。

テンプレートは、CloudFormation が次のリソースを作成するよう指示します。

- Slack チャンネル設定。
- Slack ワークスペース設定。
- AWSSupportSlackAppCFNRole 名を持つ IAM ロール。AWSSupportAppFullAccess AWS 管理ポリシーがアタッチされています。

目次

Slack 向けの CloudFormation テンプレートを更新する

まず、以下のテンプレートを使用してスタックを作成します。テンプレートは Slack のワークスペースとチャンネルの有効な値に置き換える必要があります。

> **Note**
>
> テンプレートを使用して組織の AccountAlias リソースを作成することはお勧めしません。AccountAlias リソースは、 AWS サポート アプリ AWS アカウント で を一意に識別します。メンバーアカウントは、サポートセンターコンソールにアカウント名を入力できます。詳細については、「Slack ワークスペースを承認する」を参照してください。

Slack 向けの CloudFormation テンプレートを更新するには

1. 組織の管理者アカウントである場合は、メンバーアカウントが CloudFormation を使用してリソースを作成できるようにするため、アカウントの Slack ワークスペースを手動で承認する必要があります。まだの場合は、「Slack ワークスペースを承認する」を参照してください。
2. [AWS サポート アプリケーションのリソースタイプのリファレンス]ページから、希望するリソース向けの JSON テンプレートまたは YAML テンプレートをコピーします。
3. テキストエディタで、テンプレートを新しいファイルに貼り付けます。
4. テンプレートで、必要なパラメータを指定します。少なくとも、以下のフィールドの値を置き換えてください。
   - Slack ワークスペース ID を使用した TeamId
   - Slack チャンネル ID を使用した ChannelId

- Slack チャンネル設定を識別する名前付き `ChannelName`

> **Tip**
>
> ワークスペースとチャンネル ID を確認するには、ブラウザで Slack チャンネルを開きます。URL は、ワークスペース ID が最初の識別子で、チャンネル ID が 2 番目の識別子です。例えば、https://app.slack.com/client/T012ABCDEFG/C01234A5BCD では、T012ABCDEFG がワークスペース ID で、C01234A5BCD がチャンネル ID です。

5. ファイルを JSON または YAML ファイルとして保存します。

管理者アカウント用のスタックを作成する

次に、組織の管理者アカウント用のスタックを作成する必要があります。この手順では、ユーザーに代わって RegisterSlackWorkspaceForOrganization API 操作が呼び出され、Slack でワークスペースが承認されます。

> **Note**
>
> 前の手順で更新した Slack ワークスペース設定テンプレートを管理者アカウント用にアップロードすることをお勧めします。 AWS サポート アプリを使用するように管理アカウントも設定しない限り、Slack チャネル設定テンプレートをアップロードする必要はありません。

管理者アカウント用のスタックを作成するには

1. 組織の管理アカウント AWS Management Console として にサインインします。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
3. まだの場合は、リージョンセレクタで次のいずれかを選択します AWS リージョン。

   - 欧州 (フランクフルト)
   - 欧州 (アイルランド)
   - 欧州 (ロンドン)
   - 米国東部 (バージニア北部)
   - 米国東部 (オハイオ)

- 米国西部 (オレゴン)
- アジアパシフィック (シンガポール)
- アジアパシフィック (東京)
- カナダ (中部)

4. 手順に従って、スタックを作成します。詳細については、「AWS CloudFormation コンソールでのスタックの作成」を参照してください。

   CloudFormation が正常にスタックを作成したら、同じテンプレートを使用して組織向けのスタックセットを作成できます。

組織のスタックセットを作成する

次に、同じテンプレートを Slack ワークスペース設定に使用して、`service-managed` アクセス許可のあるスタックセットを作成します。スタックセットを使用して組織全体のスタックを作成することも、必要な OU を指定することもできます。詳細については、「スタックセットを作成する」を参照してください。

この手順では、ユーザーに代わって RegisterSlackWorkspaceForOrganization API 操作も呼び出します。この API 操作では、メンバーアカウントの Slack を使用してワークスペースを承認されます。

組織のスタックセットを作成するには

1. 組織の管理アカウント AWS Management Console として にサインインします。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソールを開きます。
3. リージョンセレクタでまだ選択していない場合は、前の手順で使用した AWS リージョン ものと同じ を選択します。
4. ナビゲーションペインから [StackSets] を選択します。
5. [Create StackSet] (StackSet の作成) を選択します。
6. [Choose a template] (テンプレートの選択) ページで、以下のオプションはデフォルトのままにします。

   - [Permissions] (アクセス許可) で、[Service-managed permissions] (サービスマネージド型のアクセス許可) を選択します。
   - [Prerequisite - Prepare template] (前提条件 - テンプレートの準備) で、[Template is ready] (テンプレートの準備完了) を受け入れます。

7. [Specify template] (テンプレートの指定) で、[Upload a template file] (テンプレートファイルのアップロード) を選択し、[Choose file] (ファイルの選択) を選択します。
8. ファイルを選択してから、[Next] (次へ) を選択します。
9. [Specify StackSet details] (StackSet の詳細を指定) ページで、スタック名 (**`support-app-slack-workspace`** など) を入力してから [Next] (次へ) を選択します。
10. [Configure StackSet options] (StackSet オプションを設定) ページで、デフォルトオプションを受け入れてから [Next] (次へ) を選択します。
11. [Set deployment options] (デプロイオプションの設定) ページの [Add stacks to stack set] (スタックをスタックセットに追加) では、デフォルトの [Deploy new stacks] (新しいスタックをデプロイ) オプションを受け入れます。
12. [Deployment targets] (デプロイターゲット) では、組織全体のスタックを作成するか、特定の OU のスタックを作成するかを選択します。OU を選択した場合は、OU ID を入力します。
13. リージョンを指定するには、次のいずれかを入力します AWS リージョン。

    - 欧州 (フランクフルト)
    - 欧州 (アイルランド)
    - 欧州 (ロンドン)
    - 米国東部 (バージニア北部)
    - 米国東部 (オハイオ)
    - 米国西部 (オレゴン)
    - アジアパシフィック (シンガポール)
    - アジアパシフィック (東京)
    - カナダ (中部)

    > 注記:
    >
    > - ワークフローを合理化するには、ステップ 3 で選択した AWS リージョン ものと同じを使用することをお勧めします。
    > - 複数の を選択すると AWS リージョン 、スタックの作成と競合する可能性があります。

14. [Deployment options] (デプロイオプション) の [Failure tolerance - optional] (障害耐性 - オプション) に、CloudFormation がオペレーションを停止するまでにスタックに障害が発生する可能性の

あるアカウントの数を入力します。追加するアカウントの数から 1 を引いた数を入力することをお勧めします。例えば、指定した OU にメンバーアカウントが 10 個ある場合は、「9」と入力します。つまり、CloudFormation がオペレーションを 9 回失敗しても、少なくとも 1 つのアカウントは成功することになります。

15. [Next (次へ)] を選択します。
16. [Review] (確認) ページで選択内容を確認し、[Submit] (送信) を選択します。[Stack Instances] (スタックインスタンス) タブでスタックのステータスをチェックできます。
17. (オプション) Slack チャンネル設定のテンプレートをアップロードするには、この手順を繰り返します。サンプルテンプレートでは、IAM ロールも作成し、 AWS 管理ポリシーをアタッチします。このロールには、お客様に代わって他のサービスにアクセスするために必要なアクセス許可があります。詳細については、「AWS サポート アプリへのアクセスの管理」を参照してください。

    Slack チャンネル設定を作成するスタックセットを作成しない場合、メンバーアカウントは Slack チャンネルを手動で設定できます。詳細については、「Slack チャンネルの設定」を参照してください。

CloudFormation がスタックを作成すると、各メンバーアカウントはサポートセンターコンソールにサインインし、設定した Slack ワークスペースとチャンネルを見つけることができます。その後、AWS サポート アプリを に使用できます AWS アカウント。「Slack チャンネルでのサポートケースの作成」を参照してください。

> **Tip**
>
> 新しいテンプレートをアップロードする必要がある場合は、以前に指定したものと同じ AWS リージョン を使用することをお勧めします。

CloudFormation の詳細はこちら

CloudFormation の詳細については、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation API リファレンス
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

Terraform を使用して AWS サポート アプリリソースを作成する

Terraform を使用して、 の AWS サポート アプリリソースを作成することもできます AWS アカウント。Terraform は、クラウドアプリケーションに使用できるコードとしてのインフラストラクチャツールです。CloudFormation スタックをアカウントにデプロイする代わりに、Terraform を使用して AWS サポート アプリケーションリソースを作成できます。

Terraform をインストールしたら、必要な AWS サポート アプリリソースを指定できます。Terraform は、RegisterSlackWorkspaceForOrganization API 操作を呼び出し、ユーザーに代わって Slack ワークスペースを登録してリソースを作成します。その後、サポートセンターコンソールにログインして、設定した Slack のワークスペースとチャンネルを見つけることができます。

> **メモ**
>
> - 組織の管理者アカウントである場合は、メンバーアカウントがリソースの作成に Terraform を使用できるよう、アカウントの Slack ワークスペースを手動で承認する必要があります。まだの場合は、「Slack ワークスペースを承認する」を参照してください。
> - CloudFormation スタックセットとは異なり、Terraform を使用して組織内の OU 向けの AWS サポート アプリケーションリソースを作成することはできません。
> - これらのアップデートのイベント履歴は、 AWS CloudTrailの Terraform からも確認できます。これらのイベントの `eventSource` は `cloudcontrolapi.amazonaws.com` と `supportapp.amazonaws.com` になります。詳細については、「を使用した Slack API コールでの AWS サポート アプリの ログ記録 AWS CloudTrail」を参照してください。

詳細

Terraform の詳細については、以下のトピックを参照してください。

- Terraform のインストール
- Terraform チュートリアル: のインフラストラクチャを構築する AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

のセキュリティ AWS サポート

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

セキュリティは、 AWS とお客様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。 AWS また、 は、お客様が安全に使用できるサービスも提供します。コンプライアンスAWS プログラムコンプライアンスプログラムコンプライアンスプログラムの一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。が適用されるコンプライアンスプログラムの詳細については AWS サポート、「コンプライアンスプログラムAWS による対象範囲内の のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 を使用する際の責任共有モデルの適用方法を理解するのに役立ちます サポート。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する サポート ようにを設定する方法について説明します。また、 サポート リソースのモニタリングや保護に役立つ他の Amazon Web Services 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 サポート
- AWS サポート ケースのセキュリティ
- の Identity and Access Management AWS サポート
- インシデントへの対応
- および でのログ記録 AWS サポート とモニタリング AWS Trusted Advisor
- のコンプライアンス検証 AWS サポート
- の耐障害性 AWS サポート
- のインフラストラクチャセキュリティ AWS サポート

- での設定と脆弱性の分析 サポート

でのデータ保護 AWS サポート

責任 AWS 共有モデル、 でのデータ保護に適用されます サポート。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

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

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール AWS サポート 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そ

のサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

> **Important**
>
> ケースコレスポンデンスでは、認証情報、クレジットカード、署名URLs、個人を特定できる情報などの機密情報を共有しないでください。

AWS サポート ケースのセキュリティ

サポートケースを作成するときは、サポートケースに含める情報を所有します。 AWS は、お客様の許可なしに AWS アカウント データにアクセスしません。 AWS は、お客様の情報を第三者と共有しません。

サポートケースを作成するときは、以下の点にご注意ください。

- AWS サポート は、`AWSServiceRoleForSupport`サービスにリンクされたロールで定義されたアクセス許可を使用して、お客様の問題をトラブルシューティング AWS のサービス する他の を呼び出します。詳細については、「AWS サポートのサービスにリンクされたロールの使用」および「AWS マネージドポリシー: AWSSupportServiceRolePolicy」を参照してください。
- で AWS サポート 発生した への API コールを表示できます AWS アカウント。例えば、アカウント内の誰かがサポートケースを作成または解決したときに口グ情報を表示できます。詳細については、「 を使用した AWS サポート API コールのログ記録 AWS CloudTrail」を参照してください。
- AWS サポート API を使用して `DescribeCases` API を呼び出すことができます。この API は、ケース ID、作成日と解決日、サポートエージェントとのコレスポンデンスといったサポートケース情報を返します。ケースの詳細は、ケースを作成してから最大 12 か月間、表示できます。詳細については、「AWS サポート API リファレンス」の「DescribeCases」を参照してください。
- サポートケースは、AWS サポートのコンプライアンス検証に従います。
- サポートケースを作成すると、 AWS はアカウントにアクセスできません。必要に応じて、サポートエージェントが画面共有ツールを使ってユーザーの画面をリモートで表示し、問題の特定とトラブルシューティングを行います。このツールは表示専用です。 AWS サポート は、画面共有のセッション中にユーザーに代わって操作することはできません。サポートエージェントと画面を共有するときは、ユーザーに同意していただく必要があります。詳細については、「AWS サポートのよくある質問」を参照してください。
- プランを変更 AWS サポート して、アカウントに必要なヘルプを取得できます。詳細については、AWS サポート 「計画の比較」と「計画の変更 AWS サポート」を参照してください。

の Identity and Access Management AWS サポート

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 サポート リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、作業内容によって異なります サポート。

サービスユーザー – サポート サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの サポート 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 サポート機能にアクセスできない場合は、「AWS サポート 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 サポート リソースを担当している場合は、通常、 へのフルアクセスがあります サポート。サービスユーザーがどの サポート 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更

する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を で使用する方法の詳細については サポート、「」を参照してくださいと IAM の AWS サポート 連携方法。

IAM 管理者 - 管理者は、 サポートへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる サポート アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS サポート アイデンティティベースのポリシーの例。

アイデンティティを使用した認証

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

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、ロールを間接的に引き受けます。

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

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

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

AWS アカウントのルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウ

ント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーのユースケース」を参照してください。

IAM ロール

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

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可と 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リクエストを組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを実行しているアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 インスタンスに AWS ロールを割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

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

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

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

その他のポリシータイプ

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

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。

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

複数のポリシータイプ

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

と IAM の AWS サポート 連携方法

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

IAM サポート を使用して のアクセスを管理する方法については、「 のアクセスを管理する サポート」を参照してください。

トピック

- サポート アイデンティティベースのポリシー
- サポート IAM ロール

サポート アイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションやリソースを指定でき、さらにアクションが許可または拒否された条件を指定できます。 サポート は、特定のアクションをサポートします。JSON ポリシーで使用する要素については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素のリファレンス」(IAM JSON) をご参照ください。

アクション

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

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

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

のポリシーアクションは、アクションの前にプレフィックス サポート を使用しますsupport:。たとえば、 Amazon EC2 `RunInstances` API オペレーションで Amazon EC2 インスタンスを実行するためのアクセス許可をユーザーに付与するには、ポリシーに `ec2:RunInstances` アクションを含めます。ポリシーステートメントには、`Action` 要素または `NotAction` 要素のいずれかを含める必要があります。 サポート は、このサービスで実行できるタスクを説明する独自の一連のアクションを定義します。

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、次のようにカンマで区切ります。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

ワイルドカード (*) を使用して複数アクションを指定できます。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": "ec2:Describe*"
```

サポート 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 サポート」を参照してください。

例

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

サポート 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 サポート

一時的な認証情報を使用して、フェデレーションでサインインする、IAM 役割を引き受ける、またはクロスアカウント役割を引き受けることができます。一時的なセキュリティ認証情報を取得するには、AssumeRole や GetFederationToken などの AWS STS API オペレーションを呼び出します。

サポート では、一時的な認証情報の使用がサポートされています。

サービスにリンクされた役割

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

サポート は、サービスにリンクされたロールをサポートします。 サポート サービスにリンクされたロールの作成または管理の詳細については、「」を参照してくださいAWS サポートのサービスにリンクされたロールの使用。

サービス役割

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

サポート はサービスロールをサポートします。

AWS サポート アイデンティティベースのポリシーの例

デフォルトでは、IAM ユーザーおよびロールには、 サポート リソースを作成または変更するアクセス許可はありません。また、、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

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

トピック

- ポリシーのベストプラクティス
- サポート コンソールを使用する
- ユーザーが自分の許可を表示できるようにする

ポリシーのベストプラクティス

アイデンティティベースポリシーは非常に強力です。アカウント内の サポート 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。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 管理ポリシーを使用して開始する – の使用 サポート をすばやく開始するには、 AWS 管理ポリシーを使用して、従業員に必要なアクセス許可を付与します。これらのポリシーはアカウントで既に有効になっており、 AWSによって管理および更新されています。詳細については、「IAM ユーザーガイド」の「 AWS マネージドポリシーでアクセス許可の使用を開始する」を参照してください。
- 最小特権を付与する - カスタムポリシーを作成するときは、タスクを実行するために必要なアクセス許可のみを付与します。最小限の許可からスタートし、必要に応じて追加の許可を付与します。この方法は、寛容過ぎる許可から始めて、後から厳しくしようとするよりも安全です。詳細については、IAM ユーザーガイドの「最小特権を認める」を参照してください。
- 機密性の高いオペレーションに MFA を有効にする - 追加セキュリティとして、機密性の高リソースまたは API オペレーションにアクセスするために IAM ユーザーに対して、多要素認証 (MFA) の使用を要求します。詳細については、IAM ユーザーガイドの「AWSでの多要素認証 (MFA) の使用」を参照してください。

- 追加セキュリティに対するポリシー条件を使用する - 実行可能な範囲内で、アイデンティティベースのポリシーがリソースにアクセスできる条件を定義します。例えば、あるリクエストの送信が許可される IP アドレスの範囲を指定するための条件を記述できます。指定された日付または時間範囲内でのみリクエストを許可する条件を書くことも、SSL や MFA の使用を要求することもできます。詳細については、IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

サポート コンソールを使用する

AWS サポート 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 サポート リソースの詳細を一覧表示および表示できます。最小限必要な許可よりも厳しく制限されたアイデンティティベースポリシーを作成すると、そのポリシーを添付したエンティティ (IAM ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

これらのエンティティが引き続き サポート コンソールを使用できるようにするには、エンティティに次の AWS 管理ポリシーもアタッチします。詳細については、IAM ユーザーガイド」の「ユーザーへの許可の追加」を参照してください。

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

ユーザーが自分の許可を表示できるようにする

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
```

```
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

サービスにリンクされたロールの使用

AWS サポート および は AWS Identity and Access Management 、(IAM) サービスにリンクされたロール AWS Trusted Advisor を使用します。サービスにリンクされたロールは、 サポート および に直接リンクされた一意の IAM ロールです Trusted Advisor。いずれの場合も、サービスに関連付けられたロールは事前定義されたロールです。このロールには、ユーザーに代わって他の AWS サービスを呼び出すために サポート または が Trusted Advisor 必要とするすべてのアクセス許可が含まれます。以下のトピックでは、サービスにリンクされたロールの動作と、 サポート および でのロールの操作方法について説明します Trusted Advisor。

トピック

- AWS サポートのサービスにリンクされたロールの使用
- Trusted Advisorのサービスにリンクされたロールの使用

AWS サポートのサービスにリンクされたロールの使用

AWS サポート ツールは、API コールを通じて AWS リソースに関する情報を収集し、カスタマーサービスとテクニカルサポートを提供します。サポートアクティビティの透明性と監査可能性を高めるために、 は AWS Identity and Access Management (IAM) サービスにリンクされたロール サポート を使用します。

`AWSServiceRoleForSupport` サービスにリンクされたロールは、直接リンクされた一意の IAM ロールです サポート。このサービスにリンクされたロールは事前定義されており、ユーザーに代わって が他の AWS サービスを呼び出す サポート ために必要なアクセス許可が含まれています。

`AWSServiceRoleForSupport` サービスにリンクされたロールは、ロールを継承するために `support.amazonaws.com` のサービスを信頼します。

これらのサービスを提供するために、ロールの事前定義されたアクセス許可は、顧客データではなくリソースメタデータ サポート へのアクセスを許可します。 AWS アカウント内に存在するこのロールを引き受けることができる サポート のはツールのみです。

お客様データを含む可能性のあるフィールドを修正します。例えば、 AWS Step Functions API コールの GetExecutionHistory の `Input`および `Output`フィールドは表示されません サポート。 AWS KMS keys を使用して機密フィールドを暗号化します。これらのフィールドは API レスポンスで編集され、 AWS サポート エージェントには表示されません。

> **Note**
>
> AWS Trusted Advisor は、別の IAM サービスにリンクされたロールを使用してアカウントの AWS リソースにアクセスし、ベストプラクティスの推奨事項とチェックを提供します。詳細については、「Trusted Advisor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。

`AWSServiceRoleForSupport` サービスにリンクされたロールを使用すると、すべての AWS サポート API コールを顧客に表示することができます AWS CloudTrail。これにより、 がユーザーに代わって サポート 実行するアクションを透過的に理解できるため、要件のモニタリングと監査に役立ちます。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。

サポートのサービスリンクロールのアクセス許可

このロールは AWSSupportServiceRolePolicy 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がロールにアタッチされ、ユーザーに代わってがアクションを完了するためのアクセス許可がロールに付与されます。

これらのアクションには以下が含まれます。

- 請求、管理、サポート、その他のカスタマーサービス – AWS カスタマーサービスは、 マネージドポリシーによって付与されたアクセス許可を使用して、サポートプランの一部として多数のサービスを実行します。アカウントと請求に関するご質問に対する調査および回答、アカウントの管理サポートの提供、サービスクォータの緩和、その他のカスタマーサポートの提供などがあります。
- AWS アカウントのサービス属性と使用状況データの処理 – 管理ポリシーによって付与されたアクセス許可を使用して、アカウントの AWS サービス属性と使用状況データにアクセスする サポート 場合があります。このポリシーにより、 サポート は アカウントの請求、管理、テクニカルサポートを提供できます。サービス属性には、お客様のアカウントのリソース識別子、メタデータタグ、ロール、アクセス権限が含まれます。使用状況データには、試用ポリシー、使用統計、および分析が含まれます。
- アカウントとそのリソースの運用状態を維持する – サポート は、自動化されたツールを使用して、運用およびテクニカルサポートに関連するアクションを実行します。

許可されたサービスとアクションの詳細については、IAM コンソールのAWSSupportServiceRolePolicy ポリシーを参照してください。

> **Note**
>
> AWS サポート は、AWSSupportServiceRolePolicyポリシーを 1 か月に 1 回自動的に更新して、新しい AWS サービスとアクションのアクセス許可を追加します。

詳細については、「AWS の マネージドポリシー AWS サポート」を参照してください。

のサービスにリンクされたロールの作成 サポート

AWSServiceRoleForSupport ロールを手動で作成する必要はありません。 AWS アカウントを作成すると、このロールが自動的に作成および設定されます。

> **Important**
>
> サービスにリンクされたロールのサポート サポート を開始する前に を使用した場合 AWS 、 はアカウントにAWSServiceRoleForSupportロールを作成しました。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

のサービスにリンクされたロールの編集と削除 サポート

AWSServiceRoleForSupport サービスにリンクされたロールの説明は、IAM を使用して編集できます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

AWSServiceRoleForSupport ロールは、 サポート がアカウントの管理、運用、テクニカルサポートを提供するために必要です。そのため、このロールは IAM コンソール、API、または AWS Command Line Interface () から削除できませんAWS CLI。これにより、サポートの各サービスを管理するのに必要なアクセス権限を誤って削除することがなくなり、 AWS アカウントが保護されます。

AWSServiceRoleForSupport ロールまたはそのユーザーの詳細については、サポート にお問い合わせください。

Trusted Advisorのサービスにリンクされたロールの使用

AWS Trusted Advisor は AWS Identity and Access Management 、 (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは、直接リンクされた一意の IAM ロールです AWS Trusted Advisor。サービスにリンクされたロールは、 によって事前定義されており Trusted Advisor、ユーザーに代わって他の AWS サービスを呼び出すためにサービスが必要とするすべてのアクセス許可が含まれています。 はこのロール Trusted Advisor を使用して、 全体の使用状況を確認し AWS 、環境を改善 AWS するための推奨事項を提供します。例えば、 は Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの使用 Trusted Advisor を分析して、コスト削減、パフォーマンスの向上、障害の許容、セキュリティの向上を支援します。

> **Note**
>
> AWS サポート は、別の IAM サービスにリンクされたロールを使用してアカウントのリソースにアクセスし、請求、管理、およびサポートサービスを提供します。詳細については、「AWS サポート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。

サービスにリンクされたロールをサポートするその他のサービスの詳細については、「IAM と連携する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列が「はい」になっているサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、[Yes] (はい) リンクを選択します。

トピック

- Trusted Advisorのサービスリンクロールのアクセス許可
- サービスにリンクされたロールのアクセス許可の管理
- Trusted Advisorのサービスリンクロールの作成
- Trusted Advisorのサービスにリンクされたロールの編集
- Trusted Advisorのサービスリンクロールの削除

Trusted Advisorのサービスリンクロールのアクセス許可

Trusted Advisor は、次の 2 つのサービスにリンクされたロールを使用します。

- AWSServiceRoleForTrustedAdvisor — このロールは Trusted Advisor サービスを信頼して、ロールがユーザーの代理として AWS のサービスにアクセスするロールを継承します。ロールのアクセス許可ポリシーは、すべての AWS リソースへの Trusted Advisor 読み取り専用アクセスを許可します。このロールは、必要なアクセス許可を追加する必要がないため、 AWS アカウントの使用を簡単に開始できます Trusted Advisor。 AWS アカウントを開くと、 によってこのロールが自動的に Trusted Advisor 作成されます。定義された許可には、信頼ポリシーと許可ポリシーが含まれます。その他の IAM エンティティにアクセス許可ポリシーをアタッチすることはできません。

  アタッチされたポリシーの詳細については、「AWSTrustedAdvisorServiceRolePolicy」を参照してください。
- AWSServiceRoleForTrustedAdvisorReporting — このロールは Trusted Advisor サービスを信頼して、組織ビュー機能のロールを継承します。このロールは、 AWS Organizations 組織内の信頼されたサービス Trusted Advisor として を有効にします。組織ビューを有効にすると、 によってこのロール Trusted Advisor が作成されます。

  アタッチされたポリシーの詳細については、「AWSTrustedAdvisorReportingServiceRolePolicy」を参照してください。

  組織ビューを使用して、組織内のすべてのアカウントの Trusted Advisor チェック結果のレポートを作成できます。この機能の詳細については、「の組織ビュー AWS Trusted Advisor」を参照してください。

サービスにリンクされたロールのアクセス許可の管理

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。次の例では、AWSServiceRoleForTrustedAdvisor サービスリンクロールを使用します。

Example : IAM エンティティが **AWSServiceRoleForTrustedAdvisor** サービスリンクロールを作成することを許可します

このステップは、 Trusted Advisor アカウントが無効になっており、サービスにリンクされたロールが削除され、ユーザーが再度有効にするにはロールを再作成する必要がある場合にのみ必要です Trusted Advisor。

サービスにリンクされたロールを作成する IAM エンティティのアクセス権限ポリシーに、次のステートメントを追加できます。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : IAM エンティティが **AWSServiceRoleForTrustedAdvisor** サービスリンクロールの説明を編集することを許可します

説明できるのは、AWSServiceRoleForTrustedAdvisor ロールの説明のみです。サービスにリンクされたロールの説明を編集する IAM エンティティのアクセス許可ポリシーに、次のステートメントを追加できます。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
```

```
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example : IAM エンティティが **AWSServiceRoleForTrustedAdvisor** サービスリンクロールを削除することを許可します

サービスにリンクされたロールを削除する IAM エンティティのアクセス権限ポリシーに、次のステートメントを追加できます。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

AdministratorAccess などの AWS 管理ポリシーを使用して、 へのフルアクセスを提供することもできます Trusted Advisor。

Trusted Advisorのサービスリンクロールの作成

AWSServiceRoleForTrustedAdvisor サービスリンクロールを手動で作成する必要はありません。 AWS アカウントを開くと、 によってサービスにリンクされたロール Trusted Advisor が作成されます。

> **Important**
>
> Trusted Advisor サービスにリンクされたロールのサポートを開始する前に サービスを使用していた場合、 はアカウントにAWSServiceRoleForTrustedAdvisorロールを作成 Trusted Advisor 済みです。詳細については、IAM ユーザーガイドの「IAM アカウントに新しいロールが表示される」を参照してください。

お客様のアカウントに AWSServiceRoleForTrustedAdvisor サービスリンクロールが設定されていない場合、 Trusted Advisor が想定どおりに動作しません。これは、アカウント内のユーザーが Trusted Advisor を無効にした後、サービスにリンクされたロールを削除した場合に発生することが

あります。その場合は、IAM を使用して AWSServiceRoleForTrustedAdvisor サービスリンクロールを作成してから、 Trusted Advisorを有効にします。

を有効にするには Trusted Advisor （ コンソール ）

1. のサービスにリンクされたロールを作成するには AWS CLI、IAM コンソール、または IAM API を使用します Trusted Advisor。詳細については、「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。
2. にサインインし AWS Management Console、 で Trusted Advisor コンソールに移動しますhttps://console.aws.amazon.com/trustedadvisor。

   [無効な Trusted Advisor] ステータスバナーがコンソールに表示されます。
3. ステータスバナーから Trusted Advisor ロールの有効化を選択します。必要な AWSServiceRoleForTrustedAdvisor が検出されない場合は、無効ステータスバナーが表示されたままになります。

Trusted Advisorのサービスにリンクされたロールの編集

さまざまなエンティティから参照される可能性があるため、サービスにリンクされたロールの名前を変更することはできません。ただし、IAM コンソール AWS CLI、または IAM API を使用してロールの説明を編集できます。詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールの編集」を参照してください。

Trusted Advisorのサービスリンクロールの削除

の機能やサービスを使用する必要がない場合は Trusted Advisor、AWSServiceRoleForTrustedAdvisorロールを削除できます。このサービスにリンクされたロールを削除する Trusted Advisor 前に、 を無効にする必要があります。これにより、 Trusted Advisor オペレーションに必要なアクセス権限の削除を防止します。無効にすると Trusted Advisor、オフライン処理や通知など、すべてのサービス機能が無効になります。また、メンバーアカウント Trusted Advisor に対して を無効にすると、個別の支払者アカウントも影響を受けます。つまり、コストを節約する方法を特定する Trusted Advisor チェックは受信されません。 Trusted Advisor コンソールにはアクセスできません。アクセス拒否エラーを Trusted Advisor 返す API コール。

Trusted Advisorを再度有効化するには、AWSServiceRoleForTrustedAdvisor サービスリンクロールを再作成する必要があります。

AWSServiceRoleForTrustedAdvisor サービスにリンクされたロールを削除する前に、コンソール Trusted Advisor で を無効にする必要があります。

を無効にするには Trusted Advisor

1. にサインイン AWS Management Console し、 で Trusted Advisor コンソールに移動しますhttps://console.aws.amazon.com/trustedadvisor。
2. ナビゲーションペインで [設定] を選択します。
3. [Service Linked Role Permissions (サービスにリンクされたロールのアクセス許可)] セクションで、[Disable Trusted Advisor(無効にする)] を選択します。
4. 確認ダイアログボックスで、[OK] を選択して、 Trusted Advisorを無効にすることを確認します。

無効にすると Trusted Advisor、すべての Trusted Advisor 機能が無効になり、 Trusted Advisor コンソールには無効ステータスバナーのみが表示されます。

その後、IAM コンソール、 AWS CLI、または IAM API を使用して、 という名前 Trusted Advisor のサービスにリンクされたロールを削除できますAWSServiceRoleForTrustedAdvisor。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

AWS の マネージドポリシー AWS サポート

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

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

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

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

トピック

- AWS の マネージドポリシー AWS サポート
- AWS Slack の AWS サポート アプリの マネージドポリシー
- AWS の マネージドポリシー AWS Trusted Advisor
- AWSAWS サポート プランの マネージドポリシー
- AWSAWS パートナー主導サポートの マネージドポリシー

AWS の マネージドポリシー AWS サポート

AWS サポート 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: AWSSupportServiceRolePolicy

AWS サポート は AWSSupportServiceRolePolicy 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、`AWSServiceRoleForSupport` サービスにリンクされたロールにアタッチされます。このポリシーは、サービスにリンクされた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、「サポートのサービスリンクロールのアクセス許可」を参照してください。

ポリシーへの変更のリストについては、「AWS サポートAWS マネージドポリシーの更新」および「AWSSupportServiceRolePolicy の許可の変更」を参照してください。

AWS サポートAWS マネージドポリシーの更新

これらのサービスがこれらの変更の追跡を開始 AWS サポート してからの の AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

次の表は、2022 年 2 月 17 日以降に行われた AWS サポート 管理ポリシーの重要な更新を示しています。

AWS サポート

変更	説明	日付
AWSSupportServiceRolePolicy - 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するために、以下のサービスに 88 の新しいアクセス許可を追加しました。 • Amazon Bedrock – Amazon Bedrock に関連する問題をトラブルシューティングします。 • Amazon Connect – Amazon Connect に関連する問題をデバッグします。 • Amazon DataZone – Amazon DataZone に関連する問題をデバッグします。 • Amazon EC2 – Amazon EC2 に関連する問題をトラブルシューティングします。 • Amazon EKS – Amazon EKS に関連する問題をデバッグします。 • AWS Glue – に関連する問題をトラブルシューティングします AWS Glue。 • Amazon Managed Service for Apache Flink – Amazon Managed Service for Apache Flink に関連する問	2024 年 11 月 25 日

変更	説明	日付
	題をトラブルシューティングします。 • AWS Lambda – に関連する問題をデバッグします AWS Lambda。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するために、次のサービスに 79 の新しいアクセス許可を追加しました。 • Amazon OpenSearch Serverless – Amazon OpenSearch Serverless に関連する問題をトラブルシューティングします。 • AWS AppConfig – に関連する問題をデバッグします AWS AppConfig。 • Application Signals – Application Signals に関連する問題をデバッグします。 • Amazon Athena – Amazon Athena に関連する問題をトラブルシューティングします。 • Amazon CloudWatch – Amazon CloudWatch に関連する問題をデバッグします。 • Amazon DynamoDB – Amazon DynamoDB に関連する問題をトラブルシューティングします。 • Amazon EC2 – Amazon EC2 に関連する問題をト	2024 年 10 月 8 日

変更	説明	日付
	ラブルシューティングします。 • AWS IoT – に関連する問題をデバッグします AWS IoT。 • AWS Lambda – に関連する問題をトラブルシューティングします AWS Lambda。 • AWS Launch Wizard – に関連する問題をトラブルシューティングします AWS Launch Wizard。 • AWS Security Hub – に関連する問題をデバッグします AWS Security Hub。 • Amazon WorkSpaces – Amazon WorkSpaces に関連する問題をデバッグします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するために、次のサービスに 79 の新しいアクセス許可を追加しました。 • AWS アカウント – に関連する問題をトラブルシューティングします AWS アカウント。 • AWS Auto Scaling – に関連する問題をデバッグします AWS Auto Scaling。 • Amazon Bedrock – Amazon Bedrock に関連する問題をデバッグします。 • AWS CodeConnections – CodeConnections に関連する問題をトラブルシューティングします AWS 。 • AWS Deadline Cloud – AWS Deadline Cloud に関連する問題をデバッグします。 • Amazon Elastic Kubernetes Service — Amazon Elastic Kubernetes Service に関連する問題をトラブルシューティングします。 • Elastic Load Balancing – Elastic Load Balancing に	2024 年 8 月 5 日

変更	説明	日付
	関連する問題をトラブルシューティングします。 • AWS 無料利用枠 – AWS 無料利用枠に関連する問題をデバッグします。 • Amazon Inspector – Amazon Inspector に関連する問題をトラブルシューティングします。 • Amazon OpenSearch Ingestion – Amazon OpenSearch Ingestion に関連する問題をトラブルシューティングします。 • Amazon WorkSpaces – Amazon WorkSpaces に関連する問題をデバッグします。 • AWS X-Ray – に関連する問題をデバッグします AWS X-Ray。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するために、次のサービスに 17 の新しいアクセス許可を追加しました。 • Amazon CloudWatch Network Monitor – Network Monitor サービスに関連する問題をトラブルシューティングします。 • Amazon CloudWatch Logs – Amazon CloudWatch Logs に関連する問題をデバッグします。 • Amazon Managed Streaming for Apache Kafka – Amazon Managed Streaming for Apache Kafka に関連する問題をデバッグします。 • Amazon Managed Service for Prometheus – Amazon Managed Service for Prometheus に関連する問題をトラブルシューティングします。	2024 年 3 月 22 日

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するために、次のサービスに 63 の新しいアクセス許可を追加しました。 • AWS クリーンルーム – クリーンルームに関連する問題をトラブルシューティングします AWS 。 • CodeConnections – CodeConnections に関連する問題をトラブルシューティングします。 • Amazon EKS – Amazon EKS に関連する問題をデバッグします。 • Image Builder – Image Builder に関連する問題をデバッグします。 • Amazon Inspector2 – Amazon Inspector2 に関連する問題をトラブルシューティングします。 • Amazon Inspector スキャン – Amazon Inspector スキャンに関連する問題をデバッグします。 • Amazon CloudWatch Logs – Amazon CloudWatch Logs に関連する問題をトラブルシューティングします。	2024 年 1 月 17 日

変更	説明	日付
	• AWS Outposts – に関連する問題をトラブルシューティングします AWS Outposts。 • Amazon RDS – Amazon RDS に関連する問題をデバッグします。 • AWS IAM Identity Center – に関連する問題をトラブルシューティングします AWS IAM Identity Center。 • Amazon S3 Express – Amazon S3 Express に関連する問題をデバッグします。 • AWS Trusted Advisor – に関連する問題をトラブルシューティングします AWS Trusted Advisor。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するため、次のサービスに 126 の新たなアクセス許可を追加しました。 • AWS Direct Connect – サービスに関連する問題をトラブルシューティングします AWS Direct Connect 。 • Amazon SageMaker AI – Amazon SageMaker AI サービスに関連する問題をトラブルシューティングします。 • Amazon AppStream — Amazon AppStream に関連する問題をデバッグします。 • AWS Resource Explorer – に関連する問題をデバッグします AWS Resource Explorer。 • Amazon Redshift Serverless – Amazon Redshift Serverless に関連する問題をトラブルシューティングします。 • Amazon ElastiCache – Amazon ElastiCache に関連する問題をデバッグします。	2023 年 12 月 6 日

変更	説明	日付
	• Amazon Comprehend – Amazon Comprehend に関連する問題をトラブルシューティングします。 • Amazon EC2 – Amazon EC2 に関連する問題をトラブルシューティングします。 • Amazon Elastic Kubernetes Service – Amazon Elastic Kubernetes Service に関連する問題をデバッグします。 • AWS Elastic Disaster Recovery – に関連する問題をトラブルシューティングします AWS Elastic Disaster Recovery。 • AWS AppSync – に関連する問題をデバッグします AWS AppSync。 • Amazon CloudWatch Logs – Amazon CloudWatch Logs に関連する問題をトラブルシューティングします。 • AWS Health – サービスに関連する問題をデバッグします AWS Health 。 • Amazon Connect – Amazon Connect に関連する問題をデバッグします。 • AWS Snowball – に関連する問題をトラブルシュー	

変更	説明	日付
	ティングします AWS Snowball。 • AWS Health Imaging – AWS Health Imaging に関連する問題をトラブルシューティングします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連して、お客様側で発生する問題に対するトラブルシューティングのアクションを実行するため、新たに 163 種類のアクセス許可が次のサービスに追加されました。 • Amazon CloudFront — CloudFront サービスに関連する問題をトラブルシューティングします。 • Amazon EC2 – Amazon EC2 サービスに関連する問題をトラブルシューティングします。 • Amazon AppStream — Amazon AppStream に関連する問題をデバッグします。 • AWS WAF – ウェブアプリケーションファイアウォールに関連する問題をデバッグします AWS 。 • Amazon Connect - Amazon Connect に関連する問題をトラブルシューティングします。 • AWS IoT – に関連する問題をデバッグします AWS IoT。 • Amazon Route 53 — Amazon Route 53 に関連	2023 年 10 月 27 日

変更	説明	日付
	する問題をトラブルシューティングします。 • AWS Verified Access – AWS Verified Access サービスに関連する問題をトラブルシューティングします。 • Amazon Simple Email Service — Amazon Simple Email Service に関連する問題をデバッグします。 • AWS Elastic Beanstalk – に関連する問題をトラブルシューティングします AWS Elastic Beanstalk。 • Amazon DynamoDB – Amazon DynamoDB に関連する問題をデバックします。 • AWS EC2 Image Builder – AWS EC2 Image Builder に関連する問題をトラブルシューティングします。 • AWS Outposts – AWS Outposts サービスに関連する問題をデバッグします。 • AWS Glue – に関連する問題をデバッグします AWS Glue。 • AWS Directory Service – に関連する問題をトラブルシューティングします AWS Directory Service。	

変更	説明	日付
	• AWS Elastic Disaster Recovery – に関連する問題をトラブルシューティングします AWS Elastic Disaster Recovery。 • AWS Step Functions – に関連する問題をデバッグします AWS Step Functions。 • Amazon EMR – Amazon EMR に関連する問題をトラブルシューティングします。 • Amazon Relational Database Service – Amazon Relational Database Service に関連する問題のトラブルシューティングします。 • Amazon EC2 Systems Manager — Amazon EC2 Systems Manager に関連する問題をデバッグします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連して、お客様側で発生する問題に対するトラブルシューティングのアクションを実行するため、新たに 176 種類のアクセス許可が次のサービスに追加されました。 • AWS Glue – AWS Glue サービスに関連する問題をトラブルシューティングするには • Amazon EMR – Amazon EMR サービスに関連する問題をトラブルシューティングします。 • Amazon Elastic Lake — Amazon Security Lake に関連する問題をトラブルシューティングします。 • AWS Systems Manager – Systems Manager サービスに関連する問題をデバッグします。 • Amazon Verified Permissions — Amazon Verified Permissions に関連する問題をトラブルシューティングします。 • AWS IAM Access Analyzer – IAM Access Analyzer サービスに関連する問題をデバッグします。	2023 年 8 月 28 日

変更	説明	日付
	• AWS Backup – に関連する問題をトラブルシューティングします AWS Backup。 • AWS Database Migration Service – DMS サービスに関連する問題をトラブルシューティングします。 • Amazon DynamoDB – DynamoDB に関連する問題をデバックします。 • Amazon Elastic Container Registry (Amazon ECR) — Amazon Elastic Container Registry (Amazon ECR) に関連する問題をトラブルシューティングします。 • Amazon Elastic Container Services — Amazon Elastic Container Service に関連する問題をデバッグします。 • Amazon Elastic Kubernetes Service — Amazon Elastic Kubernetes Service に関連する問題をトラブルシューティングします。 • Amazon EMR Serverless — Amazon EMR Serverless に関連する問題をデバッグします。 • AWS Identity and Access Management – に関連する問題をトラブルシューティ	

変更	説明	日付
	ングします AWS Identity and Access Management。 • AWS Network Firewall – AWS Network Firewall に関連する問題をトラブルシューティングします。 • AWS HealthOmics – AWS HealthOmics に関連する問題をデバッグします。 • Amazon QuickSight — Amazon QuickSight に関連する問題をデバッグします。 • Amazon Relational Database Service – Amazon Relational Database Service に関連する問題のトラブルシューティングします。 • Amazon Redshift – Amazon Redshift に関連する問題をトラブルシューティングします。 • Amazon Redshift Serverless — Amazon Redshift Serverless に関連する問題をデバッグします。 • Amazon SageMaker AI – Amazon SageMaker AI に関連する問題をデバッグします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連して、お客様側で発生する問題に対するトラブルシューティングのアクションを実行するため、新たに 141 種類のアクセス許可が次のサービスに追加されました。 • Lambda – Lambda サービスに関連する問題をトラブルシューティングします。 • Amazon Lex – Amazon Lex サービスに関連する問題をトラブルシューティングします。 • AWS Transfer – Transfer サービスに関連する問題をデバッグします。 • AWS Amplify – Amplify サービスに関連する問題をデバッグします。 • Amazon EventBridge Pipes - Pipes に関連するアクセス許可と請求の問題をトラブルシューティングします。 • Amazon EventBridge – Amazon EventBridge に関連する問題をデバッグします。 • Amazon CloudWatch Logs – Amazon CloudWatch Logs に関連する問題をトラブルシューティングします。	2023 年 6 月 26 日

変更	説明	日付
	• AWS Systems Manager – Systems Manager に関連する問題をトラブルシューティングします。 • Amazon CloudWatch – CloudWatch に関連する問題をデバッグします。 • Amazon ElastiCache - Amazon ElastiCache に関連する問題をトラブルシューティングします。 • Amazon Athena – Athena に関連する問題をデバッグします。 • AWS Elastic Disaster Recovery – Elastic Disaster Recovery に関連する問題をトラブルシューティングします。 • Amazon CloudWatch – Amazon CloudWatch の設定をトラブルシューティングします。 • Amazon EC2 – EC2 サービスに関連する問題をデバッグします。 • AWS Certificate Manager – Certificate Manager に関連する問題をトラブルシューティングします。 • Amazon EventBridge Scheduler - EventBridge Scheduler に関連する問題	

変更	説明	日付
	をトラブルシューティングします。 • Amazon OpenSearch Service – OpenSearch に関連する問題をトラブルシューティングします。 • Amazon EventBridge Schemas – EventBridge Schemas に関連する問題をデバッグします。 • AWS ユーザー通知 – ユーザー通知に関連する問題をトラブルシューティングします。 • Amazon CloudWatch Application Insights – CloudWatch Application Insights に関連する問題をトラブルシューティングします。 • Amazon DynamoDB – DynamoDB に関連する問題をトラブルシューティングします。 • Amazon DocumentDB Elastic Clusters – DocumentDB Elastic Clusters に関連する問題をトラブルシューティングします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連して、お客様側で発生する問題に対するトラブルシューティングのアクションを実行するため、新たに 53 種類のアクセス許可が以下のサービスに追加されました。 • Auto Scaling – Auto Scaling サービスに関連する問題をトラブルシューティングします。 • Amazon CloudWatch – Amazon CloudWatch に関連する問題をトラブルシューティングします。 • AWS Compute Optimizer – Compute Optimizer に関連する問題をトラブルシューティングします。 • Amazon CloudWatch Evidently – Evidently に関連する問題をトラブルシューティングします。 • EC2 Image Builder – Image Builder サービスに関連する問題をトラブルシューティングします。 • AWS IoT TwinMaker – に関連する問題をトラブルシューティングします AWS IoT TwinMaker。	2023 年 5 月 2 日

変更	説明	日付
	• Amazon CloudWatch Logs – Amazon CloudWatch Logs に関連する問題をトラブルシューティングします。 • Amazon Pinpoint - Amazon Pinpoint に関連する問題をトラブルシューティングします。 • AWS OAM リンク – OAM リソースに関連する問題をデバッグします。 • AWS Outposts – に関連する問題をトラブルシューティングします AWS Outposts。 • Amazon RDS – Amazon RDS に関連する問題をデバッグします。 • AWS Resource Explorer – Resource Explorer に関連する問題をトラブルシューティングします。 • Amazon CloudWatch RUM – RUM サービスリソースの設定をトラブルシューティングします。 • Amazon SNS – Amazon SNS に関連する問題をトラブルシューティングします。 • Amazon CloudWatch Synthetics – CloudWatch Synthetics に関連する問題	

変更	説明	日付
	をトラブルシューティングします。	
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、テクニカルサポートに関連するお客様の問題をトラブルシューティングするアクションを実行するための 52 の新しいアクセス許可が以下のサービスに追加されました。 • AWS Backup gateway – Backup ゲートウェイに関連する問題をトラブルシューティングします。 • Amazon S3 – Amazon S3 に関連する問題のデバッグ。 • AWS Application Migration Service – Application Migration Service に関連する問題をトラブルシューティングします。 • AWS クリーンルーム – AWS クリーンルームに関連する問題をデバッグします。 • AWS Systems Manager for SAP – AWS Systems Manager for SAP に関連する問題をトラブルシューティングします。 • Amazon VPC Lattice – Amazon VPC Lattice に関連する問題のデバッグ。	2023 年 3 月 16 日

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	220 の新しいアクセス許可により、請求、管理、テクニカルサポート関連の問題のトラブルシューティングに役立つアクションを、次のサービスで実行できるようになりました。 • Amazon Athena – AWS サポート が Athena に関連するクエリで顧客を支援するために使用できるツールを開発できるようにします。 • Amazon Chime - Amazon Chime に関連する問題をトラブルシューティングします。 • Amazon CloudWatch Internet Monitor - Internet Monitor に関連する問題をデバッグします。 • Amazon Comprehend - Amazon Comprehend に関連する問題をトラブルシューティングします。 • Amazon Elastic Compute Cloud - Transit Gateway 接続およびマルチキャスト機能に関連する問題をデバッグします。 • Amazon EventBridge Pipes - EventBridge Pipes に関連する問題をトラブルシューティングします。	2023 年 1 月 10 日

変更	説明	日付
	• Amazon Interactive Video Service – AWS サポート が Amazon IVS リソースをクエリして顧客の問題をトラブルシューティングできるようにします。 • Amazon FSx – AWS サポート が Amazon FSx データリポジトリのインポートとエクスポートをサポートするツールを開発できるようにします。 • Amazon GameLift – Amazon GameLift に関連する問題のトラブルシューティング。 • AWS Glue– AWS Glue Data Quality に関連する問題をトラブルシューティングします。 • Amazon Kinesis Video Streams - Kinesis Video Streams に関連する問題をトラブルシューティングします。 • Amazon Managed Service for Prometheus - Amazon Managed Service for Prometheus に関連する問題をトラブルシューティングします。 • Amazon Managed Streaming for Apache Kafka – Amazon MSK 接続に関連	

変更	説明	日付
	する問題をトラブルシューティングします。 • AWS Network Manager – Network Manager に関連する問題をトラブルシューティングします。 • Amazon Nimble Studio - Nimble Studio に関連する問題をデバッグします。 • Amazon Personalize - Amazon Personalize に関連する問題をデバッグします。 • Amazon Pinpoint - Amazon Pinpoint に関連する問題をトラブルシューティングします。 • AWS HealthOmics – HealthOmics に関連する問題をトラブルシューティングします。 • Amazon Transcribe - Amazon Transcribe に関連する問題をデバッグします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	47 の新しいアクセス許可により、請求、管理、テクニカルサポート関連の問題のトラブルシューティングに役立つアクションを、次のサービスで実行可能になりました。 • AWS Application Migration Service – レプリケーションと起動の問題をトラブルシューティングします。 • AWS CloudFormation フック – AWS サポート が問題の解決に役立つ自動化ツールを開発できるようにします。 • Amazon Elastic Kubernetes Service — Amazon EKS に関連する問題をトラブルシューティングするため。 • AWS IoT FleetWise – AWS IoT FleetWise に関連する問題をトラブルシューティングします。 • AWS Mainframe Modernization – に関連する問題をデバッグします AWS Mainframe Modernization。 • AWS Outposts – 専用ホストとアセットのリスト AWS サポート を取得するのに役立ちます。	2022 年 10 月 4 日

変更	説明	日付
	• AWS Private 5G – Private 5G に関連する問題をトラブルシューティングします。 • AWS Tiros — Tiros に関連する問題をデバッグするため。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	46 の新しいアクセス許可により、請求、管理、テクニカルサポート関連の問題のトラブルシューティングに役立つアクションを、次のサービスで実行可能になりました。 • Amazon Managed Streaming for Apache Kafka – Amazon MSK に関する問題をトラブルシューティングするため。 • AWS DataSync – DataSync に関連する問題をトラブルシューティングします。 • AWS Elastic Disaster Recovery – レプリケーションと起動の問題をトラブルシューティングします。 • Amazon GameSparks – GameSparks に関する問題をトラブルシューティングするため。 • AWS IoT TwinMaker – に関連する問題をデバッグします AWS IoT TwinMaker。 • AWS Lambda – 問題をトラブルシューティングするための関数 URL の設定を表示します。 • Amazon Lookout for Equipment – Lookout for Equipment に関する問題を	2022 年 8 月 17 日

変更	説明	日付
	トラブルシューティングするため。 • Amazon Route 53 および Amazon Route 53 Resolver – が VPC の DNS 解決動作 AWS サポート をチェックできるように、リゾルバー設定を取得します。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、およびテクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するための新しい許可が次のサービスに追加されました。 • Amazon CloudWatch Logs – CloudWatch Logs に関連する問題のトラブルシューティングに役立ちます。 • Amazon Interactive Video Service – 不正または侵害されたアカウントに関するサポートケースについて、既存の Amazon IVS リソース サポート をチェックするのに役立ちます。 • Amazon Inspector – Amazon Inspector 関連の問題をトラブルシューティングします。 Amazon WorkLink などのサービスの許可を削除しました。Amazon WorkLink は 2022 年 4 月 19 日に非推奨となりました。	2022 年 6 月 23 日

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新	請求、管理、およびテクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するための 25 の新しい許可が次のサービスに追加されました。 • AWS Amplify UI Builder – コンポーネントとテーマの生成に関連する問題をトラブルシューティングします。 • Amazon AppStream — 最近起動した機能のリソースを取得して問題をトラブルシューティングします。 • AWS Backup – バックアッププジョブに関連する問題をトラブルシューティングします。 • AWS CloudFormation – IAM、拡張機能、バージョニングに関連する問題の診断を実行します。 • Amazon Kinesis — Kinesis に関連する問題のトラブルシューティングを行う。 • AWS Transfer Family – Transfer Family に関連する問題をトラブルシューティングします。	2022 年 4 月 27 日

変更	説明	日付

AWSSupportServiceRolePolicy – 既存ポリシーへの更新。	請求、管理、およびテクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するための 54 の新しい許可が次のサービスに追加されました。
	• Amazon Elastic Compute Cloud
	  • お客様および AWSマネージドプレフィックス付きリストに関連する問題のトラブルシューティングを行う。
	  • Amazon VPC IP Address Manager (IPAM) に関連する問題のトラブルシューティングを行う。
	• AWS Network Manager – Network Manager に関連する問題をトラブルシューティングします。
	• Savings Plans — 未払いの Savings Plan コミットメントに関するメタデータを取得する。
	• AWS Serverless Application Repository – サポートケースの調査と解決の一環として、対応アクションを改善およびサポートします。
	• Amazon WorkSpaces Web — WorkSpaces Web サービ
		2022 年 3 月 14 日

変更	説明	日付
	スの問題をデバッグおよびトラブルシューティングします。	

変更	説明	日付
AWSSupportServiceRolePolicy – 既存ポリシーへの更新。	請求、管理、およびテクニカルサポートに関連するお客様の問題のトラブルシューティングに役立つアクションを実行するための 74 の新しい許可が次のサービスに追加されました。 • AWS Application Migration Service – Application Migration Service でエージェントレスレプリケーションをサポートするため。 • AWS CloudFormation – IAM、拡張機能、バージョニング関連の問題の診断を実行します。 • Amazon CloudWatch Logs – リソースポリシーを検証するため。 • Amazon EC2 ごみ箱 – ごみ箱の保持ルールに関するメタデータを取得するため。 • AWS Elastic Disaster Recovery – お客様のアカウントのレプリケーションと起動の問題をトラブルシューティングします。 • Amazon FSx — Amazon FSx スナップショットの説明を表示するため。	2022 年 2 月 17 日

変更	説明	日付
	• Amazon Lightsail – Lightsail バケットのメタデータと設定の詳細を表示するため。 • Amazon Macie — 分類ジョブ、カスタムデータ識別子、正規表現、検出結果などの Macie 設定を表示するため。 • Amazon S3 — Amazon S3 バケットのメタデータと設定を収集するため。 • AWS Storage Gateway – 顧客の自動テープ作成ポリシーに関するメタデータを表示します。 • Elastic Load Balancing — Service Quotas コンソールを使用する際のリソース制限の説明を表示するため。 詳細については、「AWSSupportServiceRolePolicy の許可の変更」を参照してください。	
変更ログが発行されました	AWS サポート 管理ポリシーの変更ログ。	2022 年 2 月 17 日

AWSSupportServiceRolePolicy の許可の変更

に追加されたほとんどのアクセス許可 AWS サポート では、 が同じ名前で API オペレーションを呼び出すAWSSupportServiceRolePolicyことができます。ただし、一部の API オペレーションでは、異なる名前の許可が必要です。

次の表に、異なる名前の許可を必要とする API オペレーションのみを示します。この表は、2022 年 2 月 17 日以降のこれらの違いについて説明しています。

日付	API オペレーション名	必要なポリシー許可
2022 年 2 月 17 日に許可を追加しました	s3.GetBucketAnalyticsConfiguration s3.ListBucketAnalyticsConfiguration	s3:GetAnalyticsConfiguration
	s3.GetBucketNotificationConfiguration	s3:GetBucketNotification
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration s3.ListBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguration
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration

日付	API オペレーション名	必要なポリシー許可
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

AWS Slack の AWS サポート アプリの マネージドポリシー

> **Note**
>
> でサポートケースにアクセスして表示するには AWS Support Center Console、「」を参照してくださいAWS サポート センターへのアクセスを管理する。

AWS サポート アプリには以下の 管理ポリシーがあります。

目次

AWS マネージドポリシー: AWSSupportAppFullAccess

AWSSupportAppFullAccess マネージドポリシーは、IAM ロールに Slack チャンネルの設定へのアクセス許可を付与するときに使用します。また、AWSSupportAppFullAccess ポリシーは IAM エンティティにアタッチできます。

詳細については、「AWS サポート Slack のアプリ」を参照してください。

このポリシーは、エンティティが AWS サポート アプリの AWS サポート、Service Quotas、および IAM アクションを実行できるようにするアクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- servicequotas — 既存のサービスクォータとリクエストについて説明し、アカウントのサービスクォータを引き上げます。
- support — サポートケースを作成、更新、解決します。ファイルの添付、コレスポンデンス、重要度レベルなど、ケースに関する情報を更新し、説明します。サポートエージェントとライブチャットのセッションを開始します。
- iam — Service Quotas のサービスにリンクされたロールを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
```

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

詳細については、「AWS サポート アプリへのアクセスの管理」を参照してください。

AWS マネージドポリシー: AWSSupportAppReadOnlyAccess

このAWSSupportAppReadOnlyAccessポリシーは、エンティティが読み取り専用の AWS サポートアプリアクションを実行できるようにするアクセス許可を付与します。詳細については、「AWS サポート Slack のアプリ」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。

- support — サポートケースの詳細と、サポートケースに追加されたコミュニケーションについて説明します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS サポートAWS マネージドポリシーへのアプリの更新

このサービスがこれらの変更の追跡を開始した以降の、 AWS サポート アプリの AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

次の表は、2022 年 8 月 17 日以降に AWS サポート 行われたアプリ管理ポリシーの重要な更新を示しています。

AWS サポート アプリ

変更	説明	日付
AWSSupportAppFullAccess と AWSSupportAppReadOnlyAccess AWS サポート アプリの新しい AWS マネージドポリシー	これらのポリシーは、Slack チャンネルに設定する IAM ロールに使用できます。 詳細については、「AWS サポート アプリへのアクセスの管理」を参照してください。	2022 年 8 月 19 日
変更ログが発行されました	AWS サポート アプリ管理ポリシーの変更ログ。	2022 年 8 月 19 日

AWS の マネージドポリシー AWS Trusted Advisor

Trusted Advisor には以下の AWS マネージドポリシーがあります。

目次

- AWS マネージドポリシーに関するTrusted Advisor の更新

AWS マネージドポリシー: AWSTrustedAdvisorPriorityFullAccess

このAWSTrustedAdvisorPriorityFullAccessポリシーは、 Trusted Advisor Priority へのフルアクセスを許可します。このポリシーでは、ユーザーは を信頼されたサービス Trusted Advisor として に追加 AWS Organizations し、 Trusted Advisor Priority の委任管理者アカウントを指定することもできます。

アクセス許可の詳細

このポリシーは、最初のステートメントに `trustedadvisor` の以下のアクセス許可を含みます。

- アカウントと組織について説明します。
- Trusted Advisor Priority から特定されたリスクについて説明します。このアクセス許可により、リスクステータスをダウンロードし、更新することができます。
- Trusted Advisor Priority E メール通知の設定について説明します。このアクセス許可により、メール通知を設定したり、委任管理者に対して無効にしたりできます。
- アカウントが を有効に Trusted Advisor できるように を設定します AWS Organizations。

2 番目のステートメントには、`organizations` の以下のアクセス許可が含まれます。

- Trusted Advisor アカウントと組織について説明します。
- Organizations の使用を有効に AWS のサービス した を一覧表示します。

3 番目のステートメントには、`organizations` の以下のアクセス許可が含まれます。

- Trusted Advisor Priority の委任管理者を一覧表示します。
- Organizations で信頼されたアクセスを有効または無効にします。

4 番目のステートメントには、`iam` の以下のアクセス許可が含まれます。

- `AWSServiceRoleForTrustedAdvisorReporting` サービスにリンクされたロールを作成します。

5 番目のステートメントには、`organizations` の以下のアクセス許可が含まれます。

- Trusted Advisor Priority の委任管理者を登録または登録解除することを許可します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
```

```
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

AWS マネージドポリシー: AWSTrustedAdvisorPriorityReadOnlyAccess

このAWSTrustedAdvisorPriorityReadOnlyAccessポリシーは、委任された管理者アカウントを表示するアクセス許可を含む、読み取り専用アクセス許可を Trusted Advisor Priority に付与します。

アクセス許可の詳細

このポリシーは、最初のステートメントに `trustedadvisor` の以下のアクセス許可を含みます。

- Trusted Advisor アカウントと組織について説明します。
- Trusted Advisor Priority から特定されたリスクについて説明し、ダウンロードできるようにします。
- Trusted Advisor Priority E メール通知の設定について説明します。

2 番目と 3 番目のステートメントには、organizations の以下のアクセス許可が含まれます。

- 組織を Organizations で説明します。
- Organizations の使用を有効に AWS のサービス した を一覧表示します。
- Trusted Advisor Priority の委任管理者を一覧表示します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
```

```
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "organizations:ServicePrincipal": [
       "reporting.trustedadvisor.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS マネージドポリシー: AWSTrustedAdvisorServiceRolePolicy

このポリシーは、AWSServiceRoleForTrustedAdvisor サービスにリンクされたロールにアタッチされます。これは、サービスにリンクされたロールがユーザーに代わってアクションを実行することを許可します。AWSTrustedAdvisorServiceRolePolicy を AWS Identity and Access Management (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、「Trusted Advisor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、サービスにリンクされたロールが AWS のサービスにアクセスすることを許可する、管理アクセス許可を付与します。これらのアクセス許可により、 のチェック Trusted Advisor でアカウントを評価できます。

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。

- accessanalyzer – AWS Identity and Access Management Access Analyzer リソースについて説明します。
- Auto Scaling — Amazon EC2 Auto Scaling アカウントのクォータとリソースを示します。
- cloudformation – AWS CloudFormation (CloudFormation) アカウントのクォータとスタックについて説明します。
- cloudfront — Amazon CloudFront ディストリビューションを示します。
- cloudtrail – AWS CloudTrail (CloudTrail) 証跡について説明します。

- dynamodb — Amazon DynamoDB アカウントのクォータとリソースを示します。
- dynamodbaccelerator – DynamoDB Accelerator リソースについて説明します。
- ec2 — Amazon Elastic Compute Cloud (Amazon EC2) アカウントのクォータとリソースを示します。
- elasticloadbalancing — Elastic Load Balancing (ELB) アカウントのクォータとリソースを説明します。
- iam — 認証情報、パスワードポリシー、証明書などの IAM リソースを取得します。
- networkfirewall – AWS Network Firewall リソースについて説明します。
- kinesis — Amazon Kinesis (Kinesis) アカウントのクォータを示します。
- rds — Amazon Relational Database Service (Amazon RDS) リソースを示します。
- redshift — Amazon Redshift のリソースを示します。
- route53 — Amazon Route 53 アカウントのクォータとリソースを示します。
- s3 — Amazon Simple Storage Service (Amazon S3) リソースを示します。
- ses — Amazon Simple Email Service (Amazon SES) 送信クォータを取得します。
- sqs – Amazon Simple Queue Service (Amazon SQS) キューを一覧表示します。
- cloudwatch — Amazon CloudWatch Events (CloudWatch Events) メトリクス統計を取得します。
- ce — Cost Explorer サービス (Cost Explorer) のレコメンデーションを取得します。
- route53resolver – Resolver Amazon Route 53 Resolver エンドポイントとリソースを取得します。
- kafka — Amazon Managed Streaming for Apache Kafka リソースを取得します
- ecs - Amazon ECS リソース の取得
- outposts – AWS Outposts リソースを取得します

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid" : "TrustedAdvisorServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers"
                "autoscaling:DescribeAccountLimits",
```

```
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions"
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
```

```
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
```

```
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS マネージドポリシー: AWSTrustedAdvisorReportingServiceRolePolicy

このポリシーは、 が組織ビュー機能のアクションを実行 Trusted Advisor できるようにするAWSServiceRoleForTrustedAdvisorReportingサービスにリンクされたロールにアタッチされます。IAM エンティティに AWSTrustedAdvisorReportingServiceRolePolicy をアタッチすることはできません。詳細については、「Trusted Advisor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、サービスにリンクされたロールが AWS Organizations アクションを実行できるようにする管理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 — 組織を説明し、サービスアクセス、アカウント、親、子、および組織単位を一覧表示します。

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

AWS マネージドポリシーに関するTrusted Advisor の更新

これらのサービスがこれらの変更の追跡を開始した Trusted Advisor 以降の AWS サポート およびの AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

次の表は、2021 年 8 月 10 日以降に行われた Trusted Advisor 管理ポリシーの重要な更新を示しています。

Trusted Advisor

変更	説明	日付
AWSTrustedAdvisorServiceRolePolicy 既存のポリシーの更新。	Trusted Advisor は、elasticloadbalancing:DescribeListeners, および アクセスelasticloadbalancing:DescribeRules 許可を付与する新しいアクションを追加しました。	2024 年 10 月 30 日
AWSTrustedAdvisorServiceRolePolicy 既存のポリシーの更新。	Trusted Advisor は、access-analyzer:ListAnalyzers 、、cloudwatch:ListMetrics 、、、dax:DescribeClusters ec2:DescribeNatGateways 、ec2:DescribeRouteTables 、、ec2:DescribeVpcEndpoints 、ec2:GetManagedPrefixListEntries elasticloadbalancing:DescribeTargetHealth iam:ListSAMLProviders 、kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFi	2024 年 6 月 11 日

変更	説明	日付
	rewall および アクセスsqs:GetQueueAttributes 許可を付与する新しいアクションを追加しました。	
AWSTrustedAdvisorServiceRolePolicy 既存のポリシーの更新。	Trusted Advisor は、outposts:GetOutpost 、、outposts:ListAssets および cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors アクセスoutposts:ListOutposts 許可を付与する新しいアクションを追加しました。	2024 年 1 月 18 日
AWSTrustedAdvisorPriorityFullAccess 既存のポリシーの更新。	Trusted Advisor は、ステートメント ID を含めるように AWSTrustedAdvisorPriorityFullAccess AWS マネージドポリシーを更新しました。 IDs	2023 年 12 月 6 日
AWSTrustedAdvisorPriorityReadOnlyAccess 既存のポリシーの更新	Trusted Advisor は、ステートメント ID を含めるように AWSTrustedAdvisorPriorityReadOnlyAccess AWS マネージドポリシーを更新しました。 IDs	2023 年 12 月 6 日

変更	説明	日付
AWSTrustedAdvisorServiceRolePolicy – 既存ポリシーへの更新	Trusted Advisor は、ec2:DescribeRegions s3:GetLifecycleConfiguration ecs:DescribeTaskDefinition および アクセスecs:ListTaskDefinitions 許可を付与する新しいアクションを追加しました。	2023 年 11 月 9 日
AWSTrustedAdvisorServiceRolePolicy – 既存ポリシーへの更新	Trusted Advisor はroute53resolver:ListResolverEndpoints 、新しいレジリエンスチェックをオンボードkafka:ListNodes するためにroute53resolver:ListResolverEndpointIpAddresses 、新しい IAM アクション 、、ec2:DescribeSubnets 、kafka:ListClustersV2 および を追加しました。	2023 年 9 月 14 日
AWSTrustedAdvisorReportingServiceRolePolicy サービスにリンクされたロールに Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting アタッチされた マネージドポリシーの V2	サービスにリンクされたロールの AWS マネージドポリシーを Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting V2 にアップグレードします。V2 では、もう 1 つの IAM アクション organizations:ListDelegatedAdministrators が追加されました。	2023 年 2 月 28 日

変更	説明	日付
AWSTrustedAdvisorPriorityFullAccess および AWSTrustedAdvisorPriorityReadOnlyAccess の新しい AWS マネージドポリシー Trusted Advisor	Trusted Advisor Trusted Advisor Priority へのアクセスを制御するために使用できる 2 つの新しいマネージドポリシーが追加されました。	2022 年 8 月 17 日
AWSTrustedAdvisorServiceRolePolicy – 既存ポリシーへの更新	Trusted Advisor は、`DescribeTargetGroups` および アクセス`GetAccountPublicAccessBlock` 許可を付与する新しいアクションを追加しました。 `DescribeTargetGroup` アクセス許可は、Auto Scaling グループヘルスチェックが Auto Scaling グループにアタッチされた非 Classic Load Balancer を取得するために必要です。 `GetAccountPublicAccessBlock` アクセス許可は、Amazon S3 バケット許可チェックが AWS アカウントのブロックパブリックアクセス設定を取得するために必要です。	2021 年 8 月 10 日
変更ログが発行されました	Trusted Advisor が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 8 月 10 日

AWSAWS サポート プランの マネージドポリシー

AWS サポート プランには、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: AWSSupportPlansFullAccess

AWS サポート プランは AWSSupportPlansFullAccess AWS マネージドポリシーを使用します。IAM エンティティはこのポリシーを使って、ユーザーに代わって次のサポートプランアクションを実行します。

- のサポートプランを表示する AWS アカウント
- サポートプランの変更リクエストのステータスに関する詳細を表示
- のサポートプランを変更する AWS アカウント
- のサポートプランスケジュールを作成する AWS アカウント
- のすべてのサポートプラン修飾子のリストを表示する AWS アカウント

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
                "supportplans:ListSupportPlanModifiers"
            ],
            "Resource": "*"
        }
    ]
}
```

ポリシーへの変更の一覧は、「AWS サポートAWS 管理ポリシーの更新を計画します」を参照してください。

AWS マネージドポリシー: AWSSupportPlansReadOnlyAccess

AWS サポート プランは AWSSupportPlansReadOnlyAccess AWS マネージドポリシーを使用します。IAM エンティティは、このポリシーを使って、ユーザーに代わって次の読み取り専用のサポートプランアクションを実行します。

- のサポートプランを表示する AWS アカウント
- サポートプランの変更リクエストのステータスに関する詳細を表示
- のすべてのサポートプラン修飾子のリストを表示する AWS アカウント

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
                "supportplans:ListSupportPlanModifiers"
            ],
            "Resource": "*"
        }
    ]
}
```

ポリシーへの変更の一覧は、「AWS サポートAWS 管理ポリシーの更新を計画します」を参照してください。

AWS サポートAWS 管理ポリシーの更新を計画します

これらのサービスがこれらの変更の追跡を開始してからの、サポートプランの AWS マネージドポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

次の表は、2022 年 9 月 29 日現在のサポートプランマネージドポリシーの重要な更新について説明しています。

AWS サポート

変更	説明	日付
AWSSupportPlansReadOnlyAccess – 既存ポリシーへの更新 AWSSupportPlansFullAccess – 既存ポリシーへの更新	AWSSupportPlansFullAccess および AWSSupportPlansReadOnlyAccess 管理ポリシーに ListSupportPlanModifiers アクションを追加します。	2024 年 9 月 9 日
AWSSupportPlansFullAccess – 既存ポリシーへの更新	AWSSupportPlansFullAccess 管理ポリシーに CreateSupportPlanSchedule アクションを追加します。	2023 年 5 月 8 日
変更ログが発行されました	サポートプランマネージドポリシーのログを変更します。	2022 年 9 月 29 日

AWSAWS パートナー主導サポートの マネージドポリシー

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

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

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

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

AWS マネージドポリシー: AWSPartnerLedSupportReadOnlyAccess

ユーザー、グループおよびロールに `AWSPartnerLedSupportReadOnlyAccess` をアタッチできます。

このポリシーを使用して、 AWS アカウント内のサービスのサービスメタデータを読み取ることができる APIs への読み取り専用アクセスを許可できます。このポリシーを使用して、 AWS パートナー主導サポートプログラムのパートナーに、以下のアクセス許可の詳細セクションで指定されたサービスへのアクセスを提供できます。

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。

- `acm` – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Certificate Manager。
- `acm-pca` – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Private Certificate Authority。
- `apigateway` – プリンシパルが Amazon API Gateway に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- `athena` – プリンシパルが Amazon Athena に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- `backup` – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Backup。
- `backup-gateway` — AWS Backup Gateway に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- `cloudformation` – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS CloudFormation。
- `cloudfront` – プリンシパルが Amazon CloudFront に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- `cloudtrail` – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS CloudTrail。

- cloudwatch – プリンシパルが Amazon CloudWatch に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- codepipeline – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS CodePipeline。
- cognito-identity – プリンシパルが Amazon Cognito ID に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- cognito-idp – プリンシパルが Amazon Cognito ユーザープールに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- cognito-sync – プリンシパルが Amazon Cognito Sync に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- connect – プリンシパルが Amazon Connect に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- directconnect – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Direct Connect。
- dms – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Database Migration Service。
- ds – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Directory Service。
- ec2 – プリンシパルが Amazon Elastic Compute Cloud に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。これには、EC2 (Windows および Linux)、Virtual Private Cloud (VPC)、VPC のテクニカルサポートカテゴリが含まれます。
- ecs – プリンシパルが Amazon Elastic Container Service に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- eks – プリンシパルが Amazon Elastic Kubernetes Service に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- elasticache – プリンシパルが Amazon ElastiCache に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- elasticbeanstalk – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Elastic Beanstalk。
- elasticfilesystem – プリンシパルが Amazon Elastic File System に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- elasticloadbalancing – プリンシパルが Elastic Load Balancing に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。

- emr-containers – プリンシパルが Amazon EMR on EKS に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- emr-serverless – Amazon EMR Serverless に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- es – Amazon OpenSearch Service に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。これには、OpenSearch Service マネージドクラスターなどのテクニカルサポートカテゴリが含まれます。
- events – プリンシパルが Amazon EventBridge に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- fsx – プリンシパルが Amazon FSx に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。これには、FSX for Windows File Server などのテクニカルサポートカテゴリが含まれます。
- glue – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Glue。
- guardduty – プリンシパルが Amazon GuardDuty に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- iam – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Identity and Access Management。
- kafka – プリンシパルが Amazon Managed Streaming for Apache Kafka に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- kafkaconnect – プリンシパルが Amazon Managed Streaming for Apache Kafka Connect に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- lambda – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Lambda。
- logs – プリンシパルが Amazon CloudWatch Logs に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- medialive – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Elemental MediaLive。
- mobiletargeting – プリンシパルが Amazon Pinpoint に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- pipes – プリンシパルが Amazon EventBridge Pipes に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。

- polly – プリンシパルが Amazon Polly に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- quicksight – Amazon QuickSight に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- rds – Amazon Relational Database Service に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。これには、リレーショナルデータベースサービス (Aurora - MySQL-Compat)、リレーショナルデータベースサービス (Aurora - PostgreSQL-c)、リレーショナルデータベースサービス (PostgreSQL)、リレーショナルデータベースサービス (SQL Server)、リレーショナルデータベースサービス (MySQL)、リレーショナルデータベースサービス (Oracle) などのテクニカルサポートカテゴリが含まれます。
- redshift – プリンシパルが Amazon Redshift に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- redshift-data – プリンシパルが Amazon Redshift Data API に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- redshift-serverless – プリンシパルが Amazon Redshift Serverless に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- route53 – プリンシパルが Amazon Route 53 に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- route53domains – プリンシパルが Amazon Route 53 ドメインに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- route53-recovery-cluster – プリンシパルが Amazon Route 53 リカバリクラスターに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- route53-recovery-control-config – Amazon Route 53 リカバリコントロールに関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- route53-recovery-readiness – プリンシパルが Amazon Route 53 Recovery Readiness に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- route53resolver – プリンシパルが Amazon Route 53 Resolver に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- s3 – Amazon Simple Storage Service に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- s3express – プリンシパルが Amazon S3 Express に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- sagemaker – プリンシパルが Amazon SageMaker AI に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。

- scheduler – プリンシパルが Amazon EventBridge スケジューラに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- servicequotas – Service Quotas に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- ses – Amazon Simple Email Service に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- sns – プリンシパルが Amazon Simple Notification Service に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- ssm – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Systems Manager。
- ssm-contacts – プリンシパルが AWS Systems Manager Incident Manager 問い合わせに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- ssm-incidents – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS Systems Manager Incident Manager。
- ssm-sap – プリンシパルが AWS Systems Manager for SAP に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- swf – Amazon Simple Workflow Service に関連するテクニカルサポートケースのトラブルシューティングをプリンシパルに許可します。
- vpc-lattice – プリンシパルが Amazon VPC Lattice に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。これには、VPC - Transit Gateway などのテクニカルサポートカテゴリが含まれます。
- waf – プリンシパルが関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します AWS WAF。
- waf-regional – プリンシパルが AWS WAF リージョンに関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- wafv2 – プリンシパルが AWS WAF V2 に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。
- workspaces – プリンシパルが Amazon WorkSpaces に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。これには、Workspaces (Windows) などのテクニカルサポートカテゴリが含まれます。
- workspaces-web – プリンシパルが Amazon WorkSpaces Secure Browser に関連するテクニカルサポートケースのトラブルシューティングを行うことを許可します。これには、Workspaces (Windows) などのテクニカルサポートカテゴリが含まれます。

このポリシーのアクセス許可を確認するにはAWS マネージドポリシーリファレンスの「AWSPartnerLedSupportReadOnlyAccess」を参照してください。

AWS パートナー主導のサポートによる AWS マネージドポリシーの更新

AWS パートナー主導サポートの AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページの変更に関する自動通知については、「 AWS パートナー主導のサポートドキュメント履歴」ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSPartnerLedSupportReadOnlyAccess - 新しいポリシー	AWS アカウント内のサービスのサービスメタデータを読み取ることができるアクセス許可を含む新しい AWS マネージドポリシーを追加しました。	2024 年 11 月 22 日
AWS パートナー主導のサポートが変更の追跡を開始	AWS パートナー主導のサポートが AWS マネージドポリシーの変更の追跡を開始しました。	2024 年 11 月 22 日

AWS サポート センターへのアクセスを管理する

サポートセンターにアクセスする許可とサポートケースを作成する許可が必要です。

サポートセンターにアクセスするには、次のいずれかのオプションを使用できます。

- AWS アカウントに関連付けられた E メールアドレスとパスワードを使用します。この ID は AWS アカウントのルートユーザーと呼ばれます。
- AWS Identity and Access Management (IAM) を使用します。

Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合は、サポート API を使用してプログラムで サポート および Trusted Advisor オペレーションにアクセスすることもできます。詳細については、「APIリファレンスAWS サポート」を参照してください。

> **Note**
>
> サポートセンターにサインインできない場合は、お問い合わせページを使用できます。このページでは、請求およびアカウントの問題に関するヘルプを参照できます。

AWS アカウント

にサインイン AWS Management Console し、 AWS アカウントの E メールアドレスとパスワードを使用して サポートセンターにアクセスできます。この ID は AWS アカウントのルートユーザーと呼ばれます。ただし、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことを強くお勧めします。代わりに、IAM を使用してアカウント内で特定のタスクを実行できるユーザーを制御することをお勧めします。

AWS サポートアクション

コンソールで次の サポート アクションを実行できます。これらの サポート アクションを IAM ポリシーで指定して、特定のアクションを許可または拒否することもできます。

> **Note**
>
> IAM ポリシーで以下のアクションのいずれかを拒否している場合、サポートケースの作成時もしくは操作時に、意図しない動作がサポートセンターで発生する可能性があります。

[アクション]	説明
`DescribeSupportLevel`	AWS アカウント識別子のサポートレベルを返すアクセス許可を付与します。これは、サポートレベルを識別するために サポート センターによって内部的に使用されます。
`InitiateCallForCase`	サポート センターで通話を開始する許可を付与。これは、ユーザーに代わって呼び出しを開

[アクション]	説明
	始するために、 サポート センターによって内部的に使用されます。
InitiateChatForCase	サポート センターでチャットを開始する許可を付与します。これは、ユーザーに代わってチャットを開始するために サポート センターによって内部的に使用されます。
RateCaseCommunication	サポート ケース通信を評価する許可を付与。
DescribeCaseAttributes	セカンダリサービスが サポート ケースの属性を読み取れるようにするための許可を付与します。これは、ケースにタグ付けされた属性を取得するために サポート 、 センターによって内部的に使用されます。
DescribeIssueTypes	サポート ケースの問題タイプを返す許可を付与します。これは、アカウントで利用可能な問題タイプを取得するために、 サポート センターの内部で使用されます。
SearchForCases	指定された入力に一致する サポート ケースのリストを返すアクセス許可を付与します。これは、検索されたケースを見つけるために サポート センターによって内部的に使用されます。
PutCaseAttributes	セカンダリサービスが サポート ケースに属性をアタッチすることを許可するアクセス許可を付与します。これは、 サポート ケースに運用タグを追加するために サポート Center によって内部的に使用されます。

IAM

デフォルトでは、IAM ユーザーはサポートセンターにアクセスできません。IAM を使用して、ユーザーまたはグループを作成できます。次に、IAM ポリシーをこれらのエンティティにアタッチして、サポートセンターのケースを開いて サポート API を使用するなど、アクションを実行し、リソースにアクセスするアクセス許可を付与します。

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とアカウント固有のサインインページを提供することができます。その後、 AWS アカウントにサインインし、 サポートセンターで作業できます。 AWS サポート アクセス権限を持つ IAM ユーザーは、アカウント用に作成されたすべてのケースを表示できます。

詳細については、「IAM ユーザーガイド」の「IAM ユーザー AWS Management Console として にサインインする」を参照してください。

アクセス許可を付与する最も簡単な方法は、 AWS 管理ポリシー AWSSupportAccess をユーザー、グループ、またはロールにアタッチすることです。 AWS サポート は、特定の AWS サポート オペレーションへのアクセスを制御するアクションレベルのアクセス許可を許可します。 AWS サポート はリソースレベルのアクセスを提供しないため、 Resource要素は常に に設定されます*。特定のサポートケースへのアクセスを許可または拒否することはできません。

Example : すべての サポート アクションへのアクセスを許可する

AWS 管理ポリシー AWSSupportAccess は、IAM ユーザーにアクセス権を付与します サポート。このポリシーを持つ IAM ユーザーは、すべての AWS サポート オペレーションとリソースにアクセスできます。

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

AWSSupportAccess ポリシーをエンティティにアタッチする方法の詳細については、IAM ユーザーガイドの「IAM ID 許可の追加 (コンソール)」を参照してください。

Example : ResolveCase アクションを除くすべてのアクションへのアクセスを許可する

IAM でカスタマー管理ポリシーを作成して、許可または拒否するアクションを指定します。次のポリシーステートメントでは、IAM ユーザーがケースを解決する サポート 場合を除き、 ですべてのアクションを実行することを許可します。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
       "Action": "support:ResolveCase",
       "Resource": "*"
    }]
}
```

カスタマー管理の IAM ポリシーの作成の詳細については、IAM ユーザーガイドの「IAM ポリシーの作成 (コンソール)」を参照してください。

ユーザーまたはグループに既にポリシーがある場合は、そのポリシーに AWS サポート固有のポリシーステートメントを追加できます。

> **Important**
>
> - サポートセンターでケースを表示できない場合は、必要な許可があることを確認します。必要に応じて、IAM 管理者に連絡してください。詳細については、「の Identity and Access Management AWS サポート」を参照してください。

へのアクセス AWS Trusted Advisor

では AWS Management Console、別の IAM `trustedadvisor` 名前空間がアクセスを制御します Trusted Advisor。 サポート API では、IAM `support` 名前空間がアクセスを制御します Trusted Advisor。詳細については、「へのアクセスを管理する AWS Trusted Advisor」を参照してください。

AWS サポート プランへのアクセスを管理する

トピック

サポートプランのコンソールのアクセス許可

サポートプランのコンソールにアクセスするには、一連の、最小限のアクセス許可が必要です。これらの許可により、ユーザーは AWS アカウントにあるサポートプランリソースの詳細を、リスト化し表示することができます。

supportplans 名前空間を使用して AWS Identity and Access Management (IAM) ポリシーを作成できます。このポリシーを使用して、アクションとリソースの許可を指定できます。

ポリシーを作成するときに、アクションを許可または拒否するサービスの名前空間を指定できます。サポートプランの名前空間は supportplans です。

AWS 管理ポリシーを使用して、IAM エンティティにアタッチできます。詳細については、「AWSAWS サポート プランの マネージドポリシー」を参照してください。

サポートプランアクション

コンソールで、次のサポートプランアクションを実行できます。また、これらのサポートプランアクションを IAM ポリシーで指定し、特定のアクションを許可または拒否することもできます。

[アクション]	説明
GetSupportPlan	この AWS アカウントにおける現在のサポートプランの詳細を表示する許可を付与します。
GetSupportPlanUpdateStatus	サポートプランの更新をリクエストするために、ステータスに関する詳細を表示する許可を付与します。

[アクション]	説明
StartSupportPlanUpdate	この AWS アカウントのサポートプランを更新するリクエストを実行する許可を付与します。
CreateSupportPlanSchedule	この AWS アカウントのための、サポートプランスケジュールを作成する許可を付与します。
ListSupportPlanModifiers	このすべてのサポートプラン修飾子のリストを表示するアクセス許可を付与します AWS アカウント。

サポートプランの IAM ポリシーの例

次のポリシーの例を活用して、サポートプランへのアクセスを管理できます。

サポートプランへのフルアクセス

次のポリシーは、サポートプランへのフルアクセスをユーザーに許可します。

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

サポートプランへの読み取り専用アクセス

次のポリシーは、サポートプランへの読み取り専用アクセスを許可します。

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

```
            "Action": "supportplans:Get*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "supportplans:List*",
            "Resource": "*"
        },
    ]
}
```

サポートプランへアクセスの拒否

次のポリシーは、サポートプランへのユーザーのアクセスを拒否します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

トラブルシューティング

サポートプランへのアクセスの管理については、以下のトピックを参照してください。

サポートプランを表示または変更しようとすると、サポートプランのコンソールに **GetSupportPlan** アクセス許可がないことが表示されます。

IAM ユーザーは、サポートプランのコンソールにアクセスするために必要なアクセス許可を持っている必要があります。IAM ポリシーを更新して不足しているアクセス許可が含まれるようにするか、AWSSupportPlansFullAccess または AWSSupportPlansReadOnlyAccess などの AWS マネージドポリシーを使用することができます。詳細については、「AWSAWS サポート プランの マネージドポリシー」を参照してください。

IAM ポリシーを更新するためのアクセスができない場合は、 AWS アカウント 管理者にお問い合わせください。

関連情報

詳細については、IAM ユーザーガイドにある下記のトピックを参照してください。

- IAM ポリシーシミュレーターを使用した IAM ポリシーのテスト
- アクセス拒否エラーメッセージのトラブルシューティング

サポートプランへの適切なアクセス許可を持っていますが、同じエラーが引き続き表示されます

AWS アカウント が の一部であるメンバーアカウントである場合は AWS Organizations、サービスコントロールポリシー (SCP) の更新が必要になる場合があります。SCP は、組織内のアクセス許可を管理するポリシーの一種です。

サポートプgランはグローバルサービスであるため、 AWS リージョン を制限するポリシーにより、メンバーアカウントがサポートプランを表示または変更できない場合があります。IAM やサポートプランなどのグローバルサービスを組織で実行するには、該当する任意の SCP の除外リストにサービスを追加する必要があります。つまり、SCP が指定された を拒否した場合でも、組織内のアカウントはこれらのサービスにアクセスできます AWS リージョン。

例外としてサポートプランを追加するには、SCP の "NotAction" リストに "supportplans:*" を入力します。

```
"supportplans:*",
```

SCP は次のポリシースニペットとして表示される場合があります。

Example : 組織がサポートプランにアクセスできるようにする SCP

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

メンバーアカウントを持っていて SCP を更新できない場合は、 AWS アカウント 管理者にお問い合わせください。場合によっては、管理者アカウントは SCP を更新し、すべてのメンバーアカウントがサポートプランにアクセスできるようにする必要があります。

> に関する注意事項 AWS Control Tower
>
> - 組織が で SCP を使用している場合は AWS Control Tower、リクエストされたコントロール (一般的にリージョン拒否コントロールと呼ばれます) AWS に基づいて、 へのアクセス AWS リージョン拒否を更新できます。
> - を許可する AWS Control Tower ように の SCP を更新するとsupportplans、ドリフトを修復すると SCP の更新が削除されます。詳細については、「ドリフトを検出して解決する AWS Control Tower」を参照してください。

関連情報

詳細については、以下の各トピックを参照してください。

- 「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」。
- 「AWS Control Tower ユーザーガイド」の「Configure the Region deny control」(リージョン拒否コントロールを設定する)
- AWS Control Tower ユーザーガイドでリクエストされた AWS に基づいて へのアクセスを拒否する AWS リージョン

へのアクセスを管理する AWS Trusted Advisor

AWS Trusted Advisor から にアクセスできます AWS Management Console。すべての AWS アカウント は、選択したコアTrusted Advisor チェックにアクセスできます。Business、Enterprise On-Ramp、または Enterprise Support プランをお持ちの場合は、すべてのチェックにアクセスできます。詳細については、AWS Trusted Advisor チェックリファレンス を参照してください。

AWS Identity and Access Management (IAM) を使用してアクセスを制御できます Trusted Advisor。

トピック

- Trusted Advisor コンソールのアクセス許可
- Trusted Advisor アクション

- IAM ポリシーの例
- 関連情報

Trusted Advisor コンソールのアクセス許可

Trusted Advisor コンソールにアクセスするには、ユーザーに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、ユーザーは 内の Trusted Advisor リソースの詳細を一覧表示および表示できます AWS アカウント。

次のオプションを使用して、 Trusted Advisorへのアクセスを制御できます。

- Trusted Advisor コンソールのタグフィルター機能を使用します。ユーザーまたはロールには、タグに関連付けられたアクセス許可が必要です。

  AWS 管理ポリシーまたはカスタムポリシーを使用して、タグごとにアクセス許可を割り当てることができます。詳細については、「タグを使用した IAM ユーザーおよびロールへのアクセスのアクセスの制御」を参照してください。
- `trustedadvisor` 名前空間を使用して IAM ポリシーを作成します。このポリシーを使用して、アクションとリソースの許可を指定できます。

ポリシーを作成するときに、アクションを許可または拒否するサービスの名前空間を指定できます。の名前空間は Trusted Advisor ですtrustedadvisor。ただし、 trustedadvisor名前空間を使用して API の Trusted Advisor API オペレーションを許可または拒否することはできません サポート 。代わりに、 サポート の support 名前空間を使用する必要があります。

> **Note**
>
> AWS サポート API へのアクセス許可がある場合、 の Trusted Advisor ウィジェットには Trusted Advisor 結果の概要ビュー AWS Management Console が表示されます。 Trusted Advisor コンソールで結果を表示するには、 trustedadvisor名前空間へのアクセス許可が必要です。

Trusted Advisor アクション

コンソールで次の Trusted Advisor アクションを実行できます。これらの Trusted Advisor アクションを IAM ポリシーで指定して、特定のアクションを許可または拒否することもできます。

[アクション]	説明
DescribeAccount	サポート プランとさまざまな Trusted Advisor 設定を表示する許可を付与。
DescribeAccountAccess	AWS アカウント が有効か無効かを表示する許可を付与 Trusted Advisor。
DescribeCheckItems	チェックアイテムの詳細を表示するアクセス許可を付与します。
DescribeCheckRefreshStatuses	Trusted Advisor チェックの更新ステータスを表示するアクセス許可を付与します。
DescribeCheckSummaries	Trusted Advisor チェックの概要を表示する許可を付与。
DescribeChecks	Trusted Advisor チェックの詳細を表示する許可を付与。
DescribeNotificationPreferences	AWS アカウントの通知設定を表示するアクセス許可を付与します。
ExcludeCheckItems	Trusted Advisor チェックのレコメンデーションを除外するアクセス許可を付与します。
IncludeCheckItems	Trusted Advisor チェックのレコメンデーションを含めるアクセス許可を付与します。
RefreshCheck	Trusted Advisor チェックを更新する許可を付与。
SetAccountAccess	アカウントの を有効または無効に Trusted Advisor するアクセス許可を付与します。
UpdateNotificationPreferences	Trusted Advisorの通知設定を更新するアクセス許可を付与します。

[アクション]	説明
DescribeCheckStatusHistoryChanges	過去 30 日間のチェックについて、その結果と変化したステータスを表示するための許可を付与します。

Trusted Advisor 組織ビューの アクション

以下の Trusted Advisor アクションは、組織ビュー機能用です。詳細については、「の組織ビュー AWS Trusted Advisor」を参照してください。

[アクション]	説明
DescribeOrganization	が組織ビュー機能を有効にする AWS アカウント 要件を満たしているかどうかを表示するアクセス許可を付与します。
DescribeOrganizationAccounts	組織内の連結 AWS アカウントを表示する許可を付与。
DescribeReports	組織ビューレポートの詳細 (レポート名、ランタイム、作成日、ステータス、形式など) を表示するアクセス許可を付与します。
DescribeServiceMetadata	、チェックカテゴリ、チェック名 AWS リージョン、リソースステータスなど、組織ビューレポートに関する情報を表示する許可を付与。
GenerateReport	組織内の Trusted Advisor チェックのレポートを作成する許可を付与。
ListAccountsForParent	ルートまたは組織単位 (OU) に含まれる AWS 組織内のすべてのアカウントを Trusted Advisor コンソールで表示する許可を付与。
ListOrganizationalUnitsForParent	Trusted Advisor コンソールで、親組織単位またはルート内のすべての組織単位 (OUs) を表示するアクセス許可を付与します。

[アクション]	説明
`ListRoots`	AWS 組織で定義されているすべてのルートを Trusted Advisor コンソールで表示するアクセス許可を付与します。
`SetOrganizationAccess`	組織ビュー機能を有効にするアクセス許可を付与します Trusted Advisor。

Trusted Advisor Priority アクション

アカウントで Trusted Advisor Priority が有効になっている場合は、 コンソールで次の Trusted Advisor アクションを実行できます。また、これらの Trusted Advisor アクションを IAM ポリシーに追加し、特定のアクションを許可または拒否することもできます。詳細については、「Trusted Advisor Priority の IAM ポリシー例」を参照してください。

> **Note**
>
> Trusted Advisor Priority に表示されるリスクは、テクニカルアカウントマネージャー (TAM) がアカウントに対して特定した推奨事項です。 Trusted Advisor チェックなどのサービスからの推奨事項が自動的に作成されます。TAM からのレコメンデーションは手動で作成されます。次に、TAM はこれらのレコメンデーションを送信して、アカウントの Trusted Advisor Priority に表示されます。

詳細については、「AWS Trusted Advisor Priority の使用を開始する」を参照してください。

[アクション]	説明
`DescribeRisks`	Trusted Advisor Priority でリスクを表示する許可を付与。
`DescribeRisk`	Trusted Advisor Priority でリスクの詳細を表示する許可を付与。
`DescribeRiskResources`	Trusted Advisor Priority でリスクの影響を受けるリソースを表示する許可を付与します

[アクション]	説明
DownloadRisk	Trusted Advisor Priority のリスクに関する詳細を含むファイルをダウンロードする許可を付与。
UpdateRiskStatus	Trusted Advisor Priority でリスクステータスを更新する許可を付与します
DescribeNotificationConfigurations	Trusted Advisor Priority の E メール通知設定を取得する許可を付与。
UpdateNotificationConfigurations	Trusted Advisor Priority のメール通知設定を作成または更新する許可を付与します。
DeleteNotificationConfigurationForDelegatedAdmin	Trusted Advisor Priority の委任管理者アカウントから E メール通知設定を削除するアクセス許可を組織管理アカウントに付与します。

Trusted Advisor Engage アクション

アカウントで Trusted Advisor Engage を有効にしている場合は、 コンソールで次の Trusted Advisor アクションを実行できます。これらの Trusted Advisor アクションを IAM ポリシーに追加して、特定のアクションを許可または拒否することもできます。詳細については、「Trusted Advisor Engage の IAM ポリシー例」を参照してください。

詳細については、「AWS Trusted Advisor Engage の使用を開始する (プレビュー)」を参照してください。

[アクション]	説明
CreateEngagement	Trusted Advisor Engage でエンゲージメントを作成する許可を付与。
CreateEngagementAttachment	Trusted Advisor Engage でエンゲージメントアタッチメントを作成する許可を付与。

[アクション]	説明
CreateEngagementCommunication	Trusted Advisor Engage でエンゲージメントコミュニケーションを作成する許可を付与。
GetEngagement	Trusted Advisor Engage でエンゲージメントを表示する許可を付与。
GetEngagementAttachment	Trusted Advisor Engage でエンゲージメントアタッチメントを表示する許可を付与。
GetEngagementType	Trusted Advisor Engage で特定のエンゲージメントタイプを表示する許可を付与。
ListEngagementCommunications	エンゲージメントに対するすべてのコミュニケーションを Trusted Advisor Engage で表示するアクセス許可を付与。
ListEngagements	Trusted Advisor Engage ですべてのエンゲージメントを表示する許可を付与。
ListEngagementTypes	Trusted Advisor Engage ですべてのエンゲージメントタイプを表示する許可を付与。
UpdateEngagement	Trusted Advisor Engage でエンゲージメントの詳細を更新する許可を付与。
UpdateEngagementStatus	Trusted Advisor Engage でエンゲージメントのステータスを更新する許可を付与。

IAM ポリシーの例

次のポリシーは、 Trusted Advisorへのアクセスを許可および拒否する方法を示しています。以下のいずれかのポリシーを使用して、IAM コンソールでカスタマーマネージドポリシーを作成できます。例えば、サンプルポリシーをコピーして IAM コンソールの [JSON] タブに貼り付けることができます。次に、IAM ユーザー、グループ、またはロールにポリシーをアタッチします。

IAM ポリシーの作成方法の詳細については、IAM ユーザーガイドの「IAM ポリシーの作成 (コンソール)」を参照してください。

例

- へのフルアクセス Trusted Advisor
- Trusted Advisorへの読み取り専用アクセス
- へのアクセスを拒否する Trusted Advisor
- 特定のアクションを許可および拒否する
- の サポート API オペレーションへのアクセスを制御する Trusted Advisor
- Trusted Advisor Priority の IAM ポリシー例
- Trusted Advisor Engage の IAM ポリシー例

へのフルアクセス Trusted Advisor

次のポリシーでは、 Trusted Advisor コンソールですべてのチェックですべての Trusted Advisor アクションを表示および実行することをユーザーに許可します。

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

Trusted Advisorへの読み取り専用アクセス

次のポリシーでは、 Trusted Advisor コンソールへの読み取り専用アクセスをユーザーに許可します。ユーザーは、変更 (更新チェックや通知設定の変更など) を行うことはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
```

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

へのアクセスを拒否する Trusted Advisor

次のポリシーでは、ユーザーが Trusted Advisor コンソールでチェックを表示またはアクションを実行 Trusted Advisor することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

特定のアクションを許可および拒否する

次のポリシーでは、ユーザーは Trusted Advisor コンソールですべての Trusted Advisor チェックを表示できますが、チェックの更新は許可されません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

の サポート API オペレーションへのアクセスを制御する Trusted Advisor

では AWS Management Console、別の IAM `trustedadvisor` 名前空間がアクセスを制御します Trusted Advisor。`trustedadvisor` 名前空間を使用して API の Trusted Advisor API オペレーションを許可または拒否することはできません サポート 。代わりに、`support` 名前空間を使用します。 Trusted Advisor プログラムで を呼び出すには、 サポート API へのアクセス許可が必要です。

たとえば、RefreshTrustedAdvisorCheck オペレーションを呼び出す場合は、ポリシーでこのアクションに対するアクセス許可が必要です。

Example : Trusted Advisor API オペレーションのみを許可する

次のポリシーでは、 の サポート API オペレーションへのアクセスをユーザーに許可しますが Trusted Advisor、残りの サポート API オペレーションへのアクセスは許可しません。例えば、ユーザーは API を使用してチェックを表示および更新できます。 AWS サポート ケースを作成、表示、更新、解決することはできません。

このポリシーを使用して Trusted Advisor API オペレーションをプログラムで呼び出すことはできますが、このポリシーを使用してコンソールで Trusted Advisor チェックを表示または更新することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
```

```
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM が サポート および と連携する方法の詳細については Trusted Advisor、「」を参照してくださいアクション。

Trusted Advisor Priority の IAM ポリシー例

Priority へのアクセスを制御するには、次の AWS 管理ポリシーを使用できます Trusted Advisor 。詳細については、AWS の マネージドポリシー AWS Trusted AdvisorおよびAWS Trusted Advisor Priority の使用を開始するを参照してください。

Trusted Advisor Engage の IAM ポリシー例

> **Note**
>
> Trusted Advisor Engage はプレビューリリースであり、現在 AWS 管理ポリシーはありません。以下のいずれかのポリシーを使用して、IAM コンソールでカスタマーマネージドポリシーを作成できます。

Trusted Advisor Engage で読み取りおよび書き込みアクセスを許可するポリシーの例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
```

```
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Trusted Advisor Engage で読み取り専用アクセスを許可するポリシーの例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Trusted Advisor Engage での読み取りおよび書き込みアクセスと、以下への信頼されたアクセスを有効にする機能を付与するポリシーの例 Trusted Advisor。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        }
    ]
}
```

関連情報

アクセス Trusted Advisor 許可の詳細については、以下のリソースを参照してください。

- IAM ユーザーガイドの「AWS Trusted Advisorで定義されるアクション」
- Trusted Advisor コンソールへのアクセスの制御

AWS Trusted Advisor のサービスコントロールポリシーの例

AWS Trusted Advisor は、サービスコントロールポリシー (SCPsをサポートしています。SCP は、組織内のアクセス許可を管理する目的で組織内の要素にアタッチされるポリシーです。SCP

は、SCP をアタッチする 要素のすべての AWS アカウントに適用されます。SCP では、組織のすべてのアカウントで使用可能な最大アクセス許可を一元的に制御できます。これらは、 AWS アカウントが組織のアクセスコントロールガイドラインの範囲内に収まるようにするのに役立ちます。詳細については、AWS Organizations ユーザーガイドの「サービスコントロールポリシー」を参照してください。

トピック

- 前提条件
- サービスコントロールポリシーの例

前提条件

SCP を使用するには、まず以下のことをする必要があります。

- 組織内のすべての機能の有効化。詳細については、「AWS Organizations ユーザーガイド」の「組織内のすべての機能の有効化」を参照してください。
- SCP を有効にして組織内で使用できるようにするには 詳細については、「AWS Organizations ユーザーガイド」の「ポリシータイプの有効化と無効化」を参照してください。
- 必要な SCP を作成します。SCP の作成の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシーの作成、更新、および削除」を参照してください。

サービスコントロールポリシーの例

以下の例では、組織内のリソース共有のさまざまな側面を制御する方法を説明します。

Example : ユーザーが Trusted Advisor Engage でエンゲージメントを作成または編集できないようにする

次の SCP により、ユーザーは新しいエンゲージメントを作成したり、既存のエンゲージメントを編集したりできなくなります。

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

```
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example : Trusted Advisor Engage と Trusted Advisor Priority Access を拒否する

次の SCP は、ユーザーが Trusted Advisor Engage と Trusted Advisor Priority 内のアクションにアクセスしたり実行したりできないようにします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS サポート ID とアクセスのトラブルシューティング

次の情報は、 と IAM の使用時に発生する可能性がある一般的な問題の診断 サポート と修正に役立ちます。

トピック

- iam: PassRole を実行する権限がない
- アクセスキーを表示したい
- 管理者として、他のユーザーにアクセスを許可したい サポート
- AWS アカウント外のユーザーに サポート リソースへのアクセスを許可したい

iam: PassRole を実行する権限がない

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

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

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して サポートでアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

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

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン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後は、いつでもアクセスキー ID を表示できます。ただし、シークレットアクセスキーを再表示することはできません。シークレットアクセスキーを紛失した場合は、新しいアクセスキーペアを作成する必要があります。

アクセスキーは、アクセスキー ID (例: AKIAIOSFODNN7EXAMPLE) とシークレットアクセスキー (例: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY) の 2 つで構成されています。ユーザー名とパスワードと同様に、リクエストを認証するために、アクセスキー ID とシークレットアクセスキーの

両方を使用する必要があります。ユーザー名とパスワードと同様に、アクセスキーは安全に管理してください。

> **Important**
>
> 正規のユーザー ID を確認するためであっても、アクセスキーを第三者に提供しないでください。これにより、 への永続的なアクセス権をユーザーに付与できます AWS アカウント。

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

管理者として、他のユーザーにアクセスを許可したい サポート

他のユーザーにアクセスを許可するには サポート、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。 AWS IAM Identity Center を使用してユーザーとアプリケーションを管理する場合は、アクセスレベルを定義するアクセス許可セットをユーザーまたはグループに割り当てます。アクセス許可セットは、ユーザーまたはアプリケーションに関連付けられている IAM ロールに自動的に IAM ポリシーを作成して割り当てます。詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

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

AWS アカウント外のユーザーに サポート リソースへのアクセスを許可したい

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

詳細については、以下を参照してください:

- がこれらの機能 サポート をサポートしているかどうかを確認するには、「」を参照してくださいと IAM の AWS サポート 連携方法。
- 所有 AWS アカウント する 全体のリソースへのアクセスを提供する方法については、「IAM ユーザーガイド」の「所有 AWS アカウント する別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、「IAM ユーザーガイド」の「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

インシデントへの対応

のインシデント対応 サポート は AWS 責任です。 AWS には、インシデント対応を管理する正式な文書化されたポリシーとプログラムがあります。詳細については、AWS 「セキュリティインシデント対応の紹介」ホワイトペーパーを参照してください。

以下のオプションを使用すると、運用上の問題について通知を受けることができます。

- AWS Service Health Dashboard に広範な影響を与える AWS 運用上の問題を表示します。たとえば、アカウントに固有ではないサービスやリージョンに影響するイベントなどです。
- AWS Health Dashboardで、個々のアカウントの運用上の問題を表示します。たとえば、アカウントのサービスやリソースに影響するイベントなどです。詳細については、AWS Health ユーザーガイドのAWS Health Dashboardの開始を参照してください。

および でのログ記録 AWS サポート とモニタリング AWS Trusted Advisor

モニタリングは、 および およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、以下のモニタリングツール AWS を提供し AWS Trusted

Advisor、問題を監視 AWS サポート して報告し、必要に応じてアクションを実行 AWS サポート AWS Trusted Advisor します。

- Amazon CloudWatch は、 AWS リソースと AWS で実行しているアプリケーションをリアルタイムでモニタリングします。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、CloudWatch で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動することができます。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。
- Amazon EventBridge は、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。EventBridge は、特定のイベントを監視し、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できるため、自動イベント駆動型コンピューティングを有効にします。詳細については、「Amazon EventBridge ユーザーガイド」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 コールおよび関連イベントをキャプチャし、指定した Amazon Simple Storage Service (Amazon S3) バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

詳細については、のモニタリングとログ記録 AWS サポートおよびのモニタリングとログ記録 AWS Trusted Advisorを参照してください。

のコンプライアンス検証 AWS サポート

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

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading AWS Artifact reports 」を参照してください。

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

- セキュリティのコンプライアンスとガバナンス – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- HIPAA 対応サービスのリファレンス – HIPAA 対応サービスの一覧が提供されています。すべてが HIPAA 対応 AWS のサービス であるわけではありません。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と場所に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティスをまとめたものです。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、セキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – 環境をモニタリングして AWS アカウント不審なアクティビティや悪意のあるアクティビティがないか調べることで、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービス を検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS サポート

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾー

ンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

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

のインフラストラクチャセキュリティ AWS サポート

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

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

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

での設定と脆弱性の分析 サポート

の場合 AWS Trusted Advisor、 はゲストオペレーティングシステム (OS) やデータベースのパッチ適用、ファイアウォール設定、ディザスタリカバリなどの基本的なセキュリティタスク AWS を処理します。

設定と IT コントロールは、 AWS とお客様の間で責任を共有します。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 SDKs サポート を使用するためのコード例

次のコード例は、 Software AWS Development Kit (SDK) サポート で を使用する方法を示しています。

基本は、重要なオペレーションをサービス内で実行する方法を示すコード例です。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

開始方法

こんにち サポートは

次のコード例は、 サポートの使用を開始する方法を示しています。

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
```

```
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeServices」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
```

```
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
```

```
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeServices」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

`main()` を呼び出してサンプルを実行します。

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    }
    throw err;
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeServices」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
```

```
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeServices」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
```

```
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeServices」を参照してください。

コードの例

- AWS SDKs サポート を使用するための基本的な例
  - こんにち サポートは
  - AWS SDK サポート を使用した の基本について説明します。

- AWS SDKs サポート を使用するためのアクション
  - AWS SDK または CLI AddAttachmentsToSetで を使用する
  - AWS SDK または CLI AddCommunicationToCaseで を使用する
  - AWS SDK または CLI CreateCaseで を使用する
  - AWS SDK または CLI DescribeAttachmentで を使用する
  - AWS SDK または CLI DescribeCasesで を使用する
  - AWS SDK または CLI DescribeCommunicationsで を使用する
  - AWS SDK または CLI DescribeServicesで を使用する
  - AWS SDK または CLI DescribeSeverityLevelsで を使用する
  - CLI で DescribeTrustedAdvisorCheckRefreshStatuses を使用する
  - CLI で DescribeTrustedAdvisorCheckResult を使用する
  - CLI で DescribeTrustedAdvisorCheckSummaries を使用する
  - CLI で DescribeTrustedAdvisorChecks を使用する
  - CLI で RefreshTrustedAdvisorCheck を使用する
  - AWS SDK または CLI ResolveCaseで を使用する

AWS SDKs サポート を使用するための基本的な例

次のコード例は、 SDKs AWS サポート で AWS の基本を使用する方法を示しています。

例

- こんにち サポートは
- AWS SDK サポート を使用した の基本について説明します。
- AWS SDKs サポート を使用するためのアクション
  - AWS SDK または CLI AddAttachmentsToSetで を使用する
  - AWS SDK または CLI AddCommunicationToCaseで を使用する
  - AWS SDK または CLI CreateCaseで を使用する
  - AWS SDK または CLI DescribeAttachmentで を使用する
  - AWS SDK または CLI DescribeCasesで を使用する
  - AWS SDK または CLI DescribeCommunicationsで を使用する
  - AWS SDK または CLI DescribeServicesで を使用する

- AWS SDK または CLI DescribeSeverityLevelsで を使用する
- CLI で DescribeTrustedAdvisorCheckRefreshStatuses を使用する
- CLI で DescribeTrustedAdvisorCheckResult を使用する
- CLI で DescribeTrustedAdvisorCheckSummaries を使用する
- CLI で DescribeTrustedAdvisorChecks を使用する
- CLI で RefreshTrustedAdvisorCheck を使用する
- AWS SDK または CLI ResolveCaseで を使用する

こんにち サポートは

次のコード例は、 サポートの使用を開始する方法を示しています。

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
 profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
```

```
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient =
 host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeServices」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
```

```
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
                .region(region)
                .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
    }

    // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
```

```
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                }
                index++;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeServices」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

`main()` を呼び出してサンプルを実行します。

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";
```

```
// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    }
    throw err;
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeServices」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
```

```
            }
        }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeServices」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)


def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
```

```
        if err.response["Error"]["Code"] == "SubscriptionRequiredException":
            logger.info(
                "You must have a Business, Enterprise On-Ramp, or Enterprise
 Support "
                "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                "examples."
            )
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


if __name__ == "__main__":
    hello_support(boto3.client("support"))
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeServices」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK サポート を使用した の基本について説明します。

次のコード例は、以下を実行する方法を示しています。

- ケースの利用可能なサービスと重要度レベルを取得して表示する方法
- 選択したサービス、カテゴリ、重要度レベルを使用してサポートケースを作成する方法
- 当日のオープンケースのリストを取得して表示する方法
- 新しいケースに添付セットとコミュニケーションを追加する方法
- ケースの新しい添付ファイルとコミュニケーションについて説明する方法
- ケースを解決する方法
- 当日の解決済みケースのリストを取得して表示する方法

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

コマンドプロンプトからインタラクティブのシナリオを実行します。

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the
 list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
```

```
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default
profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
{ Profile = "default" })
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));

        try
        {
            var apiSupported = await _supportWrapper.VerifySubscription();
            if (!apiSupported)
            {
                logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                                "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
                return;
            }

            var service = await DisplayAndSelectServices();

            var category = DisplayAndSelectCategories(service);
```

```
            var severityLevel = await DisplayAndSelectSeverity();

            var caseId = await CreateSupportCase(service, category,
severityLevel);

            await DescribeTodayOpenCases();

            var attachmentSetId = await CreateAttachmentSet();

            await AddCommunicationToCase(attachmentSetId, caseId);

            var attachmentId = await ListCommunicationsForCase(caseId);

            await DescribeCaseAttachment(attachmentId);

            await ResolveCase(caseId);

            await DescribeTodayResolvedCases();

            Console.WriteLine(new string('-', 80));
            Console.WriteLine("AWS Support case example scenario complete.");
            Console.WriteLine(new string('-', 80));
        }
        catch (Exception ex)
        {
            logger.LogError(ex, "There was a problem executing the scenario.");
        }
    }

    /// <summary>
    /// List some available services from AWS Support, and select a service for
the example.
    /// </summary>
    /// <returns>The selected service.</returns>
    private static async Task<Service> DisplayAndSelectServices()
    {
        Console.WriteLine(new string('-', 80));
        var services = await _supportWrapper.DescribeServices();
        Console.WriteLine($"AWS Support client returned {services.Count}
services.");

        Console.WriteLine($"1. Displaying first 10 services:");
        for (int i = 0; i < 10 && i < services.Count; i++)
```

```
        {
            Console.WriteLine($"\t{i + 1}. {services[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > services.Count)
        {
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
```

```
        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for
the example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
```

```
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category:
{category.Name} " +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code,
category.Code, severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current
day.");
        // Describe the cases. If it is empty, try again and allow time for the
new case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
```

```
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
 {openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
```

```
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</
param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId,
 string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to
 {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");

        var communications = await
 _supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
 {communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
```

```
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with
data: \n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
```

```
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
 day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status
 {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

サポート アクションのシナリオで使用されるラッパーメソッド。

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }
```

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }



    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
```

```
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
               CommunicationBody = body
           });
       return response.CaseId;
   }



   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does
not exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
```

```
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
```

```
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
```

```
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
 Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
 Defaults to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
```

```
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }



    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
```

```
            }
            else throw;
        }
    }
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の以下のトピックを参照してください。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

さまざまな サポート オペレーションを実行します。

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
```

```
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * Before running this Java (v2) code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 * In addition, you must have the AWS Business Support Plan to use the AWS
 * Support Java API. For more information, see:
 *
 * https://aws.amazon.com/premiumsupport/plans/
 *
 * This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and
 * severity level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <fileAttachment>Where:
                    fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String fileAttachment = args[0];
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
```

```
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("***** Welcome to the AWS Support case example
scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Get and display available services.");
        List<String> sevCatList = displayServices(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("") == 0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
        } else
            System.out.println("Support case " + caseId + " was successfully
created!");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Get open support cases.");
        getOpenCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Create an attachment set with a generated file to
add to the case.");
        String attachmentSetId = addAttachment(supportClient, fileAttachment);
        System.out.println("The Attachment Set id value is" + attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
```

```
        System.out.println("6. Add communication with the attachment to the
support case.");
        addAttachSupportCase(supportClient, caseId, attachmentSetId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. List the communications of the support case.");
        String attachId = listCommunications(supportClient, caseId);
        System.out.println("The Attachment id value is" + attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("8. Describe the attachment set included with the
communication.");
        describeAttachment(supportClient, attachId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("9. Resolve the support case.");
        resolveSupportCase(supportClient, caseId);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("10. Get a list of resolved cases for the current
day.");
        getResolvedCase(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("***** This Scenario has successfully completed");
        System.out.println(DASHES);
    }

    public static void getResolvedCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(30)
                    .afterTime(yesterday.toString())
```

```
                    .beforeTime(now.toString())
                    .includeResolvedCases(true)
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                if (sinCase.status().compareTo("resolved") == 0)
                    System.out.println("The case status is " + sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                    .caseId(caseId)
                    .build();

            ResolveCaseResponse response =
supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient, String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                    .attachmentId(attachId)
                    .build();
```

```
            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is " +
response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
```

```
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                    .fileName(myFile.getName())
                    .data(sourceBytes)
                    .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                    .attachments(attachment)
                    .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();
```

```
        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                    .maxResults(20)
                    .afterTime(yesterday.toString())
                    .beforeTime(now.toString())
                    .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase : cases) {
                System.out.println("The case status is " + sinCase.status());
                System.out.println("The case Id is " + sinCase.caseId());
                System.out.println("The case subject is " + sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                    .categoryCode(caseCat.toLowerCase())
                    .serviceCode(serviceCode.toLowerCase())
```

```
                    .severityCode(sevLevel.toLowerCase())
                    .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                    .subject("Test case, please ignore")
                    .language("en")
                    .issueType("technical")
                    .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                    .language("en")
                    .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel : severityLevels) {
                System.out.println("The severity level name is: " +
sevLevel.name());
                if (sevLevel.name().compareTo("High") == 0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                   .language("en")
                   .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();

           System.out.println("Get the first 10 services");
           int index = 1;
           for (Service service : services) {
               if (index == 11)
                   break;

               System.out.println("The Service name is: " + service.name());
               if (service.name().compareTo("Account") == 0)
                   serviceCode = service.code();

               // Get the Categories for this service.
               List<Category> categories = service.categories();
               for (Category cat : categories) {
                   System.out.println("The category name is: " + cat.name());
                   if (cat.name().compareTo("Security") == 0)
                       catName = cat.name();
               }
               index++;
           }

           // Push the two values to the list.
           sevCatList.add(serviceCode);
           sevCatList.add(catName);
           return sevCatList;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
```

```
            return null;
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の以下のトピックを参照してください。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

ターミナルでインタラクティブシナリオを実行します。

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
```

```
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature.",
      );
    }
    throw err;
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

/**
```

```
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const selectedSeverityLevel = await inquirer.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
```

```
};

// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases.",
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};
```

```
// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
 */
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0,
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const shouldResolve = await inquirer.confirm({
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};
```

```
/**
 * Find a specific case in the list of provided cases by case ID.
 * If the case is not found, and the results are paginated, continue
 * paging through the results.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
 * }} options
 * @returns
 */
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      }),
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
```

```
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
    console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

    // Verify that the account is subscribed to support.
    await verifyAccount();

    // Provided a truncated list of services and prompt the user to select one.
    const selectedService = await getService();

    // Provided the categories for the selected service and prompt the user to
 select one.
    const selectedCategory = await getCategory(selectedService);

    // Provide the severity available severity levels for the account and prompt
 the user to select one.
    const selectedSeverityLevel = await getSeverityLevel();

    // Create a support case.
    console.log("\nCreating a support case.");
    caseId = await createCase({
      selectedService,
      selectedCategory,
      selectedSeverityLevel,
    });
    console.log(`Support case created: ${caseId}`);

    // Display a list of open support cases created today.
    const todaysOpenCases = await retry(
      { intervalInMs: 1000, maxRetries: 15 },
      getTodaysOpenCases,
    );
    console.log(
      `\nOpen support cases created today: ${todaysOpenCases.length}`,
    );
    console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));
```

```
    // Create an attachment set.
    console.log("\nCreating an attachment set.");
    const attachmentSetId = await createAttachmentSet();
    console.log(`Attachment set created: ${attachmentSetId}`);

    // Add the attachment set to the support case.
    console.log(`\nAdding attachment set to ${caseId}`);
    await linkAttachmentSetToCase(attachmentSetId, caseId);
    console.log(`Attachment set added to ${caseId}`);

    // List the communications for a support case.
    console.log(`\nListing communications for ${caseId}`);
    const communications = await getCommunications(caseId);
    console.log(
      communications
        .map(
          (c) =>
            `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`,
        )
        .join("\n"),
    );

    // Describe the first attachment.
    console.log(`\nDescribing attachment ${attachmentSetId}`);
    const attachmentId = getFirstAttachment(communications);
    const attachment = await getAttachment(attachmentId);
    console.log(
      `Attachment is the file '${
        attachment.fileName
      }' with data: \n${new TextDecoder().decode(attachment.data)}`,
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
time.",
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
```

```
        () => getTodaysResolvedCases(caseId),
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の以下のトピックを参照してください。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.
```

```
For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()
```

```
    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add
 to the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
```

```
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 30
            afterTime = yesterday.toString()
            beforeTime = now.toString()
            includeResolvedCases = true
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
```

```
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}

suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?,
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
```

```
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String,
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
```

```
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
```

```
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の以下のトピックを参照してください。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase

- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

コマンドプロンプトからインタラクティブのシナリオを実行します。

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print("-" * 88)
        services_list = self.support_wrapper.describe_services("en")
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")
```

```
        service_choices = [svc["name"] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
preceding list:",
            service_choices,
        )
        selected_service = services_list[selected_index]
        print("-" * 88)
        return selected_service

    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select
one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print("-" * 88)
        print(
            f"Available support categories for Service {service['name']}
{len(service['categories'])}:"
        )
        categories_choices = [category["name"] for category in
service["categories"]]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices,
        )
        selected_category = service["categories"][selected_index]
        print("-" * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print("-" * 88)
        severity_levels_list =
self.support_wrapper.describe_severity_levels("en")
```

```
        print(f"Available severity levels:")
        severity_choices = [level["name"] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices,
        )
        selected_severity = severity_levels_list[selected_index]
        print("-" * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print("-" * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print("-" * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print("-" * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)

    def create_attachment_set(self):
        """
```

```
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print("-" * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print("-" * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print("-" * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id,
case_id)
        print(
            f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}."
        )
        print("-" * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attachment_id = ""
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(
                f"\tCommunication created on {communication['timeCreated']} "
```

```
                f"has {len(communication['attachmentSet'])} attachments."
            )
            if len(communication["attachmentSet"]) > 0:
                attachment_id = communication["attachmentSet"][0]["attachmentId"]
        print("-" * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print("-" * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print("-" * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.

        :param case_id: The ID of the case to resolve.
        """
        print("-" * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print("-" * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print("-" * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time,
end_time, True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print("-" * 88)
```

```
    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format="%(levelname)s:
 %(message)s")

        print("-" * 88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print("-" * 88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(
            selected_service, selected_category, selected_severity
        )
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print("-" * 88)


if __name__ == "__main__":
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

サポートされるクライアントアクションをラップするクラスを定義します。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
```

```
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

```
        else:
            return services


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
```

```
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return case_id


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
```

```
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
support case.",
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
support case.",
                attachmentSetId=attachment_set_id,
            )
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
```

```
                )
                raise
        else:
            return communications


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
```

```
        """
        try:
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
```

```
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            if resolved:
                cases = filter(lambda case: case["status"] == "resolved", cases)
            return cases
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の以下のトピックを参照してください。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDKs サポート を使用するためのアクション

次のコード例は、 AWS SDKs で個々の サポート アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「AWS サポート API リファレンス」を参照してください。

例

- AWS SDK または CLI AddAttachmentsToSetで を使用する
- AWS SDK または CLI AddCommunicationToCaseで を使用する
- AWS SDK または CLI CreateCaseで を使用する
- AWS SDK または CLI DescribeAttachmentで を使用する
- AWS SDK または CLI DescribeCasesで を使用する
- AWS SDK または CLI DescribeCommunicationsで を使用する
- AWS SDK または CLI DescribeServicesで を使用する
- AWS SDK または CLI DescribeSeverityLevelsで を使用する
- CLI で DescribeTrustedAdvisorCheckRefreshStatuses を使用する
- CLI で DescribeTrustedAdvisorCheckResult を使用する
- CLI で DescribeTrustedAdvisorCheckSummaries を使用する
- CLI で DescribeTrustedAdvisorChecks を使用する
- CLI で RefreshTrustedAdvisorCheck を使用する
- AWS SDK または CLI ResolveCaseで を使用する

AWS SDK または CLI **AddAttachmentsToSet**で を使用する

以下のコード例は、AddAttachmentsToSet の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Add an attachment to a set, or create a new attachment set if one does
not exist.
    /// </summary>
    /// <param name="data">The data for the attachment.</param>
    /// <param name="fileName">The file name for the attachment.</param>
    /// <param name="attachmentSetId">Optional setId for the attachment. Creates
a new attachment set if empty.</param>
    /// <returns>The setId of the attachment.</returns>
    public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
    {
        var response = await _amazonSupport.AddAttachmentsToSetAsync(
            new AddAttachmentsToSetRequest
            {
                AttachmentSetId = attachmentSetId,
                Attachments = new List<Attachment>
                {
                    new Attachment
                    {
                        Data = data,
                        FileName = fileName
                    }
                }
            });
        return response.AttachmentSetId;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「AddAttachmentsToSet」を参照してください。

CLI

AWS CLI

セットに添付ファイルを追加するには

次の のadd-attachments-to-set例では、 AWS アカウントでサポートケースに指定できるイメージをセットに追加します。

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

出力:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「AddAttachmentsToSet」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
           File myFile = new File(fileAttachment);
           InputStream sourceStream = new FileInputStream(myFile);
           SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

           Attachment attachment = Attachment.builder()
                   .fileName(myFile.getName())
                   .data(sourceBytes)
                   .build();

           AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                   .attachments(attachment)
                   .build();

           AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
           return response.attachmentSetId();

       } catch (SupportException | FileNotFoundException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「AddAttachmentsToSet」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set
 with a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB
 per attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      }),
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「AddAttachmentsToSet」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal =
        Attachment {
            fileName = myFile.name
            data = sourceBytes
        }

    val setRequest =
        AddAttachmentsToSetRequest {
            attachments = listOf(attachmentVal)
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「AddAttachmentsToSet」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does
 not exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        "fileName": "attachment_file.txt",
                        "data": b"This is a sample file for attachment to a
 support case.",
```

```
                    }
                ]
            )
            new_set_id = response["attachmentSetId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return new_set_id
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「AddAttachmentsToSet」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **AddCommunicationToCase**で を使用する

以下のコード例は、AddCommunicationToCase の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</
param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「AddCommunicationToCase」を参照してください。

CLI

AWS CLI

ケースに通信を追加するには

次の のadd-communication-to-case例では、 AWS アカウントのサポートケースに通信を追加します。

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

出力:

```
{
    "result": true
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「AddCommunicationToCase」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
```

```
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                    .caseId(caseId)
                    .attachmentSetId(attachmentSetId)
                    .communicationBody("Please refer to attachment for details.")
                    .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication
to an AWS Support case");
            else
                System.out.println("There was an error adding the communication
to an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「AddCommunicationToCase」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
```

```
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add
 attachments to the case.
        attachmentSetId,
      }),
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「AddCommunicationToCase」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?,
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
```

```
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS
 Support case")
        } else {
            println("There was an error adding the communication to an AWS
 Support case")
        }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「AddCommunicationToCase」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定したケースに E メール通信の本文を追加します。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

例 2: 指定されたケースに E メール通信の本文と、E メールの CC 行に含まれる 1 つ以上の E メールアドレスを追加します。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のAddCommunicationToCase」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id,
            )
```

```
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「AddCommunicationToCase」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **CreateCase**で を使用する

以下のコード例は、CreateCase の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Create a new support case.
    /// </summary>
    /// <param name="serviceCode">Service code for the new case.</param>
    /// <param name="categoryCode">Category for the new case.</param>
    /// <param name="severityCode">Severity code for the new case.</param>
    /// <param name="subject">Subject of the new case.</param>
    /// <param name="body">Body text of the new case.</param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set for the
new case.</param>
    /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
    /// <returns>The caseId of the new support case.</returns>
    public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
        string body, string language = "en", string? attachmentSetId = null,
string issueType = "customer-service")
    {
        var response = await _amazonSupport.CreateCaseAsync(
            new CreateCaseRequest()
            {
                ServiceCode = serviceCode,
                CategoryCode = categoryCode,
                SeverityCode = severityCode,
                Subject = subject,
                Language = language,
                AttachmentSetId = attachmentSetId,
                IssueType = issueType,
```

```
                CommunicationBody = body
            });
        return response.CaseId;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「CreateCase」を参照してください。

CLI

AWS CLI

ケースを作成する

次の のcreate-case例では、 AWS アカウントのサポートケースを作成します。

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

出力:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「create-case」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                   .categoryCode(caseCat.toLowerCase())
                   .serviceCode(serviceCode.toLowerCase())
                   .severityCode(sevLevel.toLowerCase())
                   .communicationBody("Test issue with " +
serviceCode.toLowerCase())
                   .subject("Test case, please ignore")
                   .language("en")
                   .issueType("technical")
                   .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「CreateCase」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each
 service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore.",
      }),
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「CreateCase」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun createSupportCase(
    sevCatListVal: List<String>,
    sevLevelVal: String,
): String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest =
        CreateCaseRequest {
            categoryCode = caseCategory.lowercase(Locale.getDefault())
            serviceCode = serCode.lowercase(Locale.getDefault())
            severityCode = sevLevelVal.lowercase(Locale.getDefault())
            communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
            subject = "Test case, please ignore"
            language = "en"
            issueType = "technical"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「CreateCase」を参照してください。

PowerShell

Tools for PowerShell

例 1: AWS サポートセンターで新しいケースを作成します。-ServiceCode および -CategoryCode パラメータの値は、Get-ASAService コマンドレットを使用して取得できます。-SeverityCode パラメータの値は、Get-ASASeverityLevel コマンドレットを使用して取得できます。-IssueType パラメータ値は、「customer-service」または「technical」のいずれかです。成功すると、 AWS サポートケース番号が出力されます。デフォルトでは、ケースは英語で処理され、日本語を使用するには -Language "ja" パラメータを追加します。-ServiceCode、-CategoryCode、-Subject、-CommunicationBody パラメータは必須です。

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のCreateCase」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
```

```
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject="Example case for testing, ignore.",
                serviceCode=service["code"],
                severityCode=severity["code"],
                categoryCode=category["code"],
                communicationBody="Example support case body.",
                language="en",
                issueType="customer-service",
            )
            case_id = response["caseId"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return case_id
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateCase」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribeAttachment**で を使用する

以下のコード例は、DescribeAttachment の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
```

```
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeAttachment」を参照してください。

CLI

AWS CLI

添付ファイルについて説明する

次の describe-attachment の例では、指定された ID の添付ファイルに関する情報を返します。

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

出力:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeAttachment」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static void describeAttachment(SupportClient supportClient, String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                   .attachmentId(attachId)
                   .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is " +
response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeAttachment」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      }),
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeAttachment」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeAttachment」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
```

```
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response["attachment"]["fileName"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return attached_file
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeAttachment」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI `DescribeCases`で を使用する

以下のコード例は、`DescribeCases` の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication.
Defaults to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases.
Defaults to false.</param>
```

```
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeCases」を参照してください。

CLI

AWS CLI

ケースについて説明する

次の のdescribe-cases例では、 AWS アカウントで指定されたサポートケースに関する情報を返します。

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

出力:

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeCases」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                   .maxResults(20)
                   .afterTime(yesterday.toString())
                   .beforeTime(now.toString())
                   .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase : cases) {
               System.out.println("The case status is " + sinCase.status());
               System.out.println("The case Id is " + sinCase.caseId());
               System.out.println("The case subject is " + sinCase.subject());
           }

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeCases」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeCases」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest =
        DescribeCasesRequest {
            maxResults = 20
            afterTime = yesterday.toString()
            beforeTime = now.toString()
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeCases」を参照してください。

PowerShell

Tools for PowerShell

例 1: すべてのサポートケースの詳細を返します。

```
Get-ASACase
```

例 2: 指定された日時以降のすべてのサポートケースの詳細を返します。

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

例 3: 解決されたサポートケースを含め、最初の 10 件のサポートケースの詳細を返します。

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

例 4: 指定された単一のサポートケースの詳細を返します。

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

例 5: 指定されたサポートケースの詳細を返します。

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」の[DescribeCases]」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、[AWS コード例リポジトリ]での設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
```

```
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator("describe_cases")
            for page in paginator.paginate(
                afterTime=after_time,
                beforeTime=before_time,
                includeResolvedCases=resolved,
                language="en",
            ):
                cases += page["cases"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
```

```
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
    else:
        if resolved:
            cases = filter(lambda case: case["status"] == "resolved", cases)
        return cases
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeCases」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribeCommunications**で を使用する

以下のコード例は、DescribeCommunications の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/// <summary>
/// Describe the communications for a case, optionally with a date filter.
```

```
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in
 paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeCommunications」を参照してください。

CLI

AWS CLI

ケースの最新のコミュニケーションについて説明する

次の のdescribe-communications例では、 AWS アカウントで指定されたサポートケースの最新通信を返します。

```
aws support describe-communications \
```

```
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

出力:

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMDAwMH0="
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeCommunications」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
```

```
                    .caseId(caseId)
                    .maxResults(10)
                    .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm : communications) {
                System.out.println("the body is: " + comm.body());

                // Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeCommunications」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";
```

```
import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the
 DescribeCommunicationsCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      }),
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeCommunications」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
```

```
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeCommunications」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定されたケースのすべての通信を返します。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

例 2: 指定されたケースについて、2012 年 1 月 1 日の午前 0 時 UTC 以降のすべての通信を返します。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のDescribeCommunications」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
 self.support_client.get_paginator("describe_communications")
            for page in paginator.paginate(caseId=case_id):
                communications += page["communications"]
        except ClientError as err:
```

```
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return communications
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeCommunications」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribeServices**で を使用する

以下のコード例は、DescribeServices の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeServices」を参照してください。

CLI

AWS CLI

AWS サービスとサービスカテゴリを一覧表示するには

次の `describe-services` の例では、一般的な情報をリクエストするためのサービスカテゴリを一覧表示します。

```
aws support describe-services \
    --service-code-list "general-info"
```

出力:

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
```

```
            ]
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeServices」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                    .language("en")
                    .build();

            DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service : services) {
                if (index == 11)
                    break;

                System.out.println("The Service name is: " + service.name());
```

```
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat : categories) {
                    System.out.println("The category name is: " + cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
                index++;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeServices」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
```

```
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest =
        DescribeServicesRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeServices」を参照してください。

PowerShell

Tools for PowerShell

例 1: 使用可能なすべてのサービスコード、名前、カテゴリを返します。

```
Get-ASAService
```

例 2: 指定されたコードを持つサービスの名前とカテゴリを返します。

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

例 3: 指定されたサービスコードの名前とカテゴリを返します。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

例 4: 指定されたサービスコードの名前とカテゴリ (日本語) を返します。現在、英語 (「en」) と日本語 (「ja」) の言語コードがサポートされています。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」の[DescribeServices]」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、[AWS コード例リポジトリ]での設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
```

```
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a
language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(language=language)
            services = response["services"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
```

```
            return services
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeServices」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **DescribeSeverityLevels**で を使用する

以下のコード例は、DescribeSeverityLevels の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language
= "en")
```

```
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「DescribeSeverityLevels」を参照してください。

CLI

AWS CLI

利用可能な重要度レベルを一覧表示する

次の describe-severity-levels の例では、サポートケースの重要度レベルを一覧表示します。

```
aws support describe-severity-levels
```

出力:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
```

```
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「緊急度の選択」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeSeverityLevels」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static String displaySevLevels(SupportClient supportClient) {
       try {
           DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                   .language("en")
                   .build();

           DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
           List<SeverityLevel> severityLevels = response.severityLevels();
           String levelName = null;
           for (SeverityLevel sevLevel : severityLevels) {
               System.out.println("The severity level name is: " +
sevLevel.name());
               if (sevLevel.name().compareTo("High") == 0)
                   levelName = sevLevel.name();
```

```
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeSeverityLevels」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeSeverityLevels」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response =
 supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「DescribeSeverityLevels」を参照してください。

PowerShell

Tools for PowerShell

例 1: AWS サポートケースに割り当てることができる重要度レベルのリストを返します。

```
Get-ASASeverityLevel
```

例 2: AWS サポートケースに割り当てることができる重要度レベルのリストを返します。レベルの名前は日本語で返されます。

```
Get-ASASeverityLevel -Language "ja"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」の[DescribeSeverityLevels]」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、[AWS コード例リポジトリ]での設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
```

```
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response =
self.support_client.describe_severity_levels(language=language)
            severity_levels = response["severityLevels"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why:
%s: %s",
                    language,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return severity_levels
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeSeverityLevels」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeTrustedAdvisorCheckRefreshStatuses** を使用する

以下のコード例は、DescribeTrustedAdvisorCheckRefreshStatuses の使用方法を示しています。

CLI

AWS CLI

AWS Trusted Advisor チェックの更新ステータスを一覧表示するには

次の describe-trusted-advisor-check-refresh-statuses の例では、Amazon S3 バケットのアクセス許可と IAM の使用という 2 つの Trusted Advisor チェックの更新ステータスを一覧表示します。

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

出力:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「AWS Trusted Advisor」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeTrustedAdvisorCheckRefreshStatuses」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定されたチェックの更新リクエストの現在のステータスを返します。Request-ASATrustedAdvisorCheckRefresh を使用して、チェックのステータス情報の更新をリクエストできます。

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のDescribeTrustedAdvisorCheckRefreshStatuses」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeTrustedAdvisorCheckResult** を使用する

以下のコード例は、DescribeTrustedAdvisorCheckResult の使用方法を示しています。

CLI

AWS CLI

AWS Trusted Advisorチェックの結果を一覧表示するには

次の describe-trusted-advisor-check-result の例では、IAM 使用チェックの結果を一覧表示します。

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

出力:

```
{
    "result": {
```

```
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

詳細については、「AWS サポートユーザーガイド」の「AWS Trusted Advisor」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeTrustedAdvisorCheckResult」を参照してください。

PowerShell

Tools for PowerShell

例 1: Trusted Advisor チェックの結果を返します。利用可能な Trusted Advisor チェックのリストは、Get-ASATrustedAdvisorChecks を使用して取得できます。出力は、チェックの全体的なステータス、チェックが最後に実行されたタイムスタンプ、および特定のチェックの一意のチェック ID です。結果を日本語で出力するには、-Language "ja" パラメータを追加します。

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のDescribeTrustedAdvisorCheckResult」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeTrustedAdvisorCheckSummaries** を使用する

以下のコード例は、DescribeTrustedAdvisorCheckSummaries の使用方法を示しています。

CLI

AWS CLI

AWS Trusted Advisor チェックの概要を一覧表示するには

次の describe-trusted-advisor-check-summaries の例では、Amazon S3 バケットのアクセス許可と IAM の使用という 2 つの Trusted Advisor チェックの結果を一覧表示します。

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

出力:

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
```

```
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「AWS Trusted Advisor」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeTrustedAdvisorCheckSummaries」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定された Trusted Advisor チェックの最新の概要を返します。

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

例 2: 指定された Trusted Advisor チェックの最新の概要を返します。

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のDescribeTrustedAdvisorCheckSummaries」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeTrustedAdvisorChecks** を使用する

以下のコード例は、DescribeTrustedAdvisorChecks の使用方法を示しています。

CLI

AWS CLI

AWS Trusted Advisorチェックを一覧表示するには

次の のdescribe-trusted-advisor-checks例では、 AWS アカウントで利用可能な Trusted Advisor チェックを一覧表示します。この情報には、チェック名、ID、説明、カテゴリ、メタデータが含まれます。読みやすくするために、出力が短縮されることに注意してください。

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

出力:

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
```

```
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

詳細については、「AWS サポートユーザーガイド」の「AWS Trusted Advisor」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「DescribeTrustedAdvisorChecks」を参照してください。

PowerShell

Tools for PowerShell

例 1: Trusted Advisor チェックのコレクションを返します。英語出力には「en」、日本語出力には「ja」のいずれかを受け入れる言語パラメータを指定する必要があります。

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のDescribeTrustedAdvisorChecks」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RefreshTrustedAdvisorCheck** を使用する

以下のコード例は、RefreshTrustedAdvisorCheck の使用方法を示しています。

CLI

AWS CLI

AWS Trusted Advisorチェックを更新するには

次の のrefresh-trusted-advisor-check例では、 AWS アカウントの Amazon S3 Bucket Permissions Trusted Advisor チェックを更新します。

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

出力:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

詳細については、「AWS サポートユーザーガイド」の「AWS Trusted Advisor」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「RefreshTrustedAdvisorCheck」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定された Trusted Advisor チェックの更新をリクエストします。

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のRefreshTrustedAdvisorCheck」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI **ResolveCase**で を使用する

以下のコード例は、ResolveCase の使用方法を示しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

.NET

AWS SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
/// <summary>
/// Resolve a support case by caseId.
/// </summary>
/// <param name="caseId">Id for the support case.</param>
/// <returns>The final status of the case after resolving.</returns>
public async Task<string> ResolveCase(string caseId)
{
    var response = await _amazonSupport.ResolveCaseAsync(
        new ResolveCaseRequest()
        {
            CaseId = caseId
        });
    return response.FinalCaseStatus;
}
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「ResolveCase」を参照してください。

CLI

AWS CLI

サポートケースを解決する

次の のresolve-case例では、 AWS アカウントのサポートケースを解決します。

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

出力:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

詳細については、「AWS サポートユーザーガイド」の「ケース管理」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ResolveCase」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
   public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
       try {
           ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                   .caseId(caseId)
                   .build();
```

```
            ResolveCaseResponse response =
 supportClient.resolveCase(caseRequest);
            System.out.println("The status of case " + caseId + " is " +
 response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ResolveCase」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      }),
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「ResolveCase」を参照してください。

Kotlin

SDK for Kotlin

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- API の詳細については、「AWS SDK for Kotlin API リファレンス」の「ResolveCase」を参照してください。

PowerShell

Tools for PowerShell

例 1: 指定されたケースの初期状態と、解決のための呼び出しが完了した後の現在の状態を返します。

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- API の詳細については、AWS Tools for PowerShell 「 コマンドレットリファレンス」のResolveCase」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。用例一覧を検索し、AWS コード例リポジトリでの設定と実行の方法を確認してください。

```
class SupportWrapper:
    """Encapsulates Support actions."""

    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client("support")
        return cls(support_client)


    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
```

```
            response = self.support_client.resolve_case(caseId=case_id)
            final_status = response["finalCaseStatus"]
        except ClientError as err:
            if err.response["Error"]["Code"] == "SubscriptionRequiredException":
                logger.info(
                    "You must have a Business, Enterprise On-Ramp, or Enterprise
Support "
                    "plan to use the AWS Support API. \n\tPlease upgrade your
subscription to run these "
                    "examples."
                )
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        else:
            return final_status
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「ResolveCase」を参照してください。

AWS SDK 開発者ガイドとコード例の完全なリストについては、「」を参照してくださいAWS SDK AWS サポート での の使用。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

のモニタリングとログ記録 AWS サポート

モニタリングは、 およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する サポート 上で重要な部分です。 AWS には、監視 サポート、問題発生時の報告、および必要に応じて自動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 EventBridge は、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。EventBridge は、特定のイベントを監視し、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できるため、自動イベント駆動型コンピューティングを有効にします。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

Amazon EventBridge による AWS サポート ケースのモニタリング

Amazon EventBridge を使用して、 AWS サポート ケースの変更を検出して対応できます。次に、作成したルールで指定した値とイベントが一致すると、EventBridge で 1 つ以上のターゲットアクションが呼び出されます。

イベントに応じて、通知の送信、イベント情報の取得、是正措置の実施、またはその他の対策を行うことができます。例えば、アカウント内で次のアクションが発生したときに通知を受け取ることができます。

- サポートケースの作成
- 既存のサポートケースにケース対応を追加する
- サポートケースの解決

- サポートケースを再度開く

> **Note**
>
> AWS サポート は、ベストエフォートベースでイベントを提供します。イベントが常に EventBridge に配信されるとは限りません。

AWS サポート ケースの EventBridge ルールの作成

EventBridge ルールを作成して、 AWS サポート ケースイベントの通知を受け取ることができます。ルールは、ユーザー、IAM ユーザー、またはサポートエージェントが実行するアクションなど、アカウント内のサポートケースの更新をモニタリングします。 AWS サポート ケースイベントのルールを作成する前に、次の操作を行います。

- EventBridge のイベント、ルール、ターゲットに精通しておいてください。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge とは」を参照してください。
- イベントルールで使用するターゲットを作成します。例えば、サポートケースが更新されるたびにテキストメッセージまたは E メールを受信できるように、Amazon Simple Notification Service (Amazon SNS) トピックを作成できます。詳細については、「EventBridge ターゲット」を参照してください。

> **Note**
>
> AWS サポート はグローバルサービスです。サポートケースの最新情報を受け取るには、米国東部 (バージニア北部) リージョン、米国西部 (オレゴン) リージョン、または欧州 (アイルランド) リージョンのいずれかを使用できます。

AWS サポート ケースイベントの EventBridge ルールを作成するには

1. Amazon EventBridge コンソールの https://console.aws.amazon.com/events/ を開いてください。
2. まだ行っていない場合は、ページの右上にあるリージョンセレクターを使用して、[US East (N. Virginia)] (米国東部 (バージニア北部)) を選択します。
3. ナビゲーションペインで [ルール] を選択します。

4. [Create rule] (ルールを作成) を選択します。
5. [Define rule detail] (ルールの詳細を定義) ページで、ルールの名前と説明を入力します。
6. [Event bus] (イベントバス) と [Rule type] (ルールタイプ) のデフォルト値を維持して、[Next] (次へ) を選択します。
7. [イベントパターンを構築] ページの [イベントソース] で、[AWS イベント] または [EventBridge パートナーイベント] を選択します。
8. [Event pattern] (イベントパターン) で、AWS のサービス をデフォルト値のままにしておきます。
9. AWS のサービスの場合、[Support] (サポート)を選択します。
10. [Event type] (イベントタイプ) で、[Support Case Update] (サポートケースを更新) を選択します。
11. [Next (次へ)] を選択します。
12. [Select target(s)] (ターゲットの選択) セクションで、このルール用に作成したターゲットを選択し、そのタイプに必要な追加オプションを設定します。例えば、Amazon SNS を選択した場合、メールまたは SMS で通知されるように SNS トピックが正しく設定されていることを確認してください。
13. [Next (次へ)] を選択します。
14. (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。
15. [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。
16. ルールの作成を選択します。これで、ルールは サポート ケースイベントをモニタリングし、指定したターゲットにそれらのケースイベントを送信するようになりました。

> **メモ**
>
> - イベントを受け取ったら、 `origin`パラメータを使用して、ユーザーまたは AWS サポート エージェントがサポートケースにケースコレスポンデンスを追加したかどうかを判断できます。`origin` の値は、`CUSTOMER` または `AWS` のいずれかになります。
>
> 現在、この値があるのは `AddCommunicationToCase` アクションのイベントのみです。
> - イベントパターンの作成の詳細については、「Amazon EventBridge ユーザーガイド」の「イベントパターン」を参照してください。

- [CloudTrail 経由のAWS API 呼び出し] イベントタイプ用に、別のルールを作成することもできます。このルールは、アカウント内の AWS サポート API コールの AWS CloudTrail ログをモニタリングします。

AWS サポート イベントの例

アカウント内でサポートアクションが発生すると、次のイベントが作成されます。

Example : サポートケースを作成する

サポートケースが作成されると、次のイベントが作成されます。

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

Example : サポートケースを更新する

サポートケースに AWS サポート 返信すると、次のイベントが作成されます。

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
```

```
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example : サポートケースを解決する

サポートケースが解決されると、次のイベントが作成されます。

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example : サポートケースを再度開く

サポートケースが解決されると、次のイベントが再度開きます。

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
```

```
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

関連情報

で EventBridge を使用する方法の詳細については AWS サポート、以下のリソースを参照してください。

- Amazon EventBridge で AWS サポート API を自動化する方法
- GitHub の AWS サポート ケースアクティビティ通知機能

を使用した AWS サポート API コールのログ記録 AWS CloudTrail

AWS サポート は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています AWS サポート。CloudTrail は、 の API コールをイベント AWS サポート としてキャプチャします。キャプチャされた呼び出しには、 AWS サポート コンソールからの呼び出しと AWS サポート API オペレーションへのコード呼び出しが含まれます。

証跡を作成する場合は、 イベントなど、Amazon Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます AWS サポート。証跡を設定しない場合でも、CloudTrail コンソールの [Event history] (イベント履歴) で最新のイベントを表示できます。

CloudTrail で収集された情報を使用して、 AWS サポートに対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

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

AWS サポート CloudTrail の情報

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

のイベントなど、 AWS アカウントのイベントの継続的な記録については AWS サポート、証跡を作成します。証跡により、ログファイルを CloudTrail で 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、すべての AWS リージョンに証跡が適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントを口グに記録し、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 口グで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail 口グファイルを複数のリージョンから受け取ると複数のアカウントから CloudTrail 口グファイルを受け取る

すべての AWS サポート API オペレーションは CloudTrail によって口グに記録され、 AWS サポート API リファレンスに記載されています。

例えば、`CreateCase`、`DescribeCases`、および `ResolveCase` オペレーションへの呼び出しによって CloudTrail 口グファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- 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 エレメント」を参照してください。

複数の AWS リージョンと複数の AWS アカウントの AWS サポート 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。

AWS Trusted Advisor CloudTrail ログ記録の情報

Trusted Advisor は、 AWS アカウントのコスト削減、セキュリティの向上、アカウントの最適化を行う方法を確認するために使用できる AWS サポート サービスです。

すべての Trusted Advisor API オペレーションは CloudTrail によってログに記録され、 AWS サポート API リファレンスに記載されています。

例えば、`DescribeTrustedAdvisorCheckRefreshStatuses`、`DescribeTrustedAdvisorCheckResult` および `RefreshTrustedAdvisorCheck` オペレーションへの呼び出しによって CloudTrail ログファイルにエントリが生成されます。

> **Note**
>
> CloudTrail は Trusted Advisor コンソールアクションもログに記録します。「を使用した AWS Trusted Advisor コンソールアクションのログ記録 AWS CloudTrail」を参照してください。

AWS サポート ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail ログファイルには、1 つ以上のログエントリがあります。イベント は、任意の送信元からの単一の要求を表します。これには、リクエストされたオペレーション、オペレーションの日時、リクエストパラメーターなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Example : CreateCase のログエントリ

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

```
{
   "Records": [
      {
```

```
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
         "sourceIPAddress": "198.51.100.15",
         "userAgent": "signin.amazonaws.com",
         "requestParameters": {
            "severityCode": "low",
            "categoryCode": "other",
            "language": "en",
            "serviceCode": "support-api",
            "issueType": "technical"
         },
         "responseElements": {
            "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
         },
         "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
         "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
         "eventType": "AwsApiCall",
         "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example : RefreshTrustedAdvisorCheck のログエントリ

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


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


を使用した Slack API コールでの AWS サポート アプリのログ記録 AWS CloudTrail

Slack の AWS サポート アプリは と統合されています AWS CloudTrail。CloudTrail は、ユーザー、ロール、または によって実行されたアクションのレコードを AWS サポート アプリ AWS のサービス に提供します。このレコードを作成するために、CloudTrail は AWS サポート App のすべてのパブリック API コールをイベントとしてキャプチャします。これらのキャプチャされた呼び出しには、 AWS サポート アプリコンソールからの呼び出しと、 AWS サポート アプリパブリック API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、 のイベントなど、Amazon

S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます これには、 AWS サポート アプリのイベントが含まれます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail が収集した情報を使用して、 AWS サポート アプリに対して行われたリクエストを判断できます。また、呼び出し元の IP アドレス、リクエスト実行者、実行日時、追加の詳細を知ることもできます。

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 サポート CloudTrail のアプリ情報

を作成すると AWS アカウント、アカウントで CloudTrail がアクティブ化されます。 AWS サポート アプリでパブリック API アクティビティが発生すると、そのアクティビティは CloudTrail イベントとイベント履歴の他の AWS サービスイベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、 CloudTrail イベント履歴でのイベントの表示を参照してください。

AWS サポート アプリのイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての 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口グに記録し、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、データに基づいて行動 AWS のサービス するように他の を設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

CloudTrail は、すべてのパブリック AWS サポート アプリアクションを口グに記録します。これらのアクションについては、「Slack のAWS サポート アプリケーションの API リファレンス」にも記載されています。例えば、`CreateSlackChannelConfiguration`、`GetAccountAlias`、`UpdateSlackChannelConfigurat`の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

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

AWS サポート アプリケーションログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではありません。つまり、ログは特定の順序で表示されるわけではありません。

Example : **`CreateSlackChannelConfiguration`** のログの例

次の例は、CreateSlackChannelConfiguration オペレーションの CloudTrail ログエントリを示したものです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **ListSlackChannelConfigurations** のログの例

次の例は、ListSlackChannelConfigurations オペレーションの CloudTrail ログエントリを示したものです。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example : **`GetAccountAlias`** のログの例

次の例は、GetAccountAlias オペレーションの CloudTrail ログエントリを示したものです。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

AWS サポート プランのモニタリングとログ記録

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

- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

- を使用した AWS サポート Plans API コールのログ記録 AWS CloudTrail

を使用した AWS サポート Plans API コールのログ記録 AWS CloudTrail

AWS サポート プランは、ユーザー AWS CloudTrail、ロール、または によって実行されたアクションを記録するサービスである と統合されています AWS のサービス。CloudTrail は、 AWS サポート プランの API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、 AWS サポート プランコンソールからの呼び出しと AWS サポート 、プラン API オペレーションへのコード呼び出しが含まれます。

証跡を作成する場合は、 AWS サポート プランのイベントなど、Amazon Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。

CloudTrail で収集された情報を使用して、 AWS サポート プランに対するリクエスト、リクエスト元の IP アドレス、リクエスト元のユーザー、リクエスト日時などの詳細を確認できます。

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

AWS サポート CloudTrail で情報を計画する

CloudTrail は、アカウントの作成 AWS アカウント 時に で有効になります。サポートされているイベントアクティビティが AWS サポート プランで発生すると、そのアクティビティはイベント履歴の他の AWS のサービス イベントとともに CloudTrail イベントに記録されます。 最近のイベントは、アカウントで表示、検索、ダウンロードできます。詳細については、「Viewing events with CloudTrail event history」(CloudTrail イベント履歴でのイベントの表示) を参照してください。

AWS サポート プランのイベントなど、 アカウントのイベントの継続的な記録については、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きに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントを口グに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それを基にアクションを取るために他の AWS のサービス を設定できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- 「CloudTrail がサポートされているサービスと統合」
- 「CloudTrail の Amazon SNS 通知の設定」
- CloudTrail ログファイルを複数のリージョンから受け取ると複数のアカウントから CloudTrail ログファイルを受け取る

すべての AWS サポート Plans API オペレーションは CloudTrail によって口グに記録されます。各イベントまたは口グエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

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

複数のアカウント AWS リージョン と複数のアカウントの AWS サポート プラン口グファイルを 1 つの Amazon S3 バケットに集約することもできます。

AWS サポート Plans ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail ログファイルには、1 つ以上のログエントリがあります。イベント は、任意の送信元からの単一の要求を表します。これには、リクエストされたオペレーション、オペレーションの日時、リクエストパラメーターなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Example : **GetSupportPlan** のログエントリ

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
```

```
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **GetSupportPlanUpdateStatus** のログエントリ

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **StartSupportPlanUpdate** のログエントリ

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **CreateSupportPlanSchedule** のログエントリ

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example : **ListSupportPlanModifiers** のログエントリ

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

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-08-15T15:44:43Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-08-15T16:29:59Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "ListSupportPlanModifiers",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
```

```
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

サポート プランへの変更のログ記録

> **Important**
>
> 2022 年 8 月 3 日以降、以下のオペレーションは廃止され、新しく作成される CloudTrail ログには表示されません。サポートされているオペレーションのリストについては、AWS サポート Plans ログファイルエントリについてを参照してください。

- `DescribeSupportLevelSummary` — このアクションは、[Support plans] (サポートプラン) ページを開くとログに記録されます。
- `UpdateProbationAutoCancellation` — デベロッパーサポートまたはビジネスサポートにサインアップし、30 日以内にキャンセルしようとすると、プランは、その期間の終了時に自動的にキャンセルされます。このアクションは、[Support plans] (サポートプラン) ページに表示されるバナーの [Opt-out of automatic cancellation] (自動キャンセルのオプトアウト) を選択するとログに記録されます。デベロッパーサポートまたはビジネスサポートのプランを再開します。
- `UpdateSupportLevel` — このアクションは、サポートプランを変更するとログに表示されます。

> **Note**
>
> `eventSource` フィールドには、これらのアクションの `support-subscription.amazonaws.com` 名前空間があります。

Example : DescribeSupportLevelSummary のログエントリ

次の例は、`DescribeSupportLevelSummary` アクションの CloudTrail ログエントリを示しています。

```
{
```

```
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example : UpdateProbationAutoCancellation のログエントリ

次の例は、UpdateProbationAutoCancellation アクションの CloudTrail ログエントリを示しています。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
```

```
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example : UpdateSupportLevel のログエントリ

次の例は、デベロッパーサポートを変更する UpdateSupportLevel アクションの CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
```

```
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

のモニタリングとログ記録 AWS Trusted Advisor

モニタリングは、 およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する Trusted Advisor 上で重要な部分です。 AWS には、監視 Trusted Advisor、問題発生時の報告、および必要に応じて自動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 EventBridge は、 AWS リソースの変更を記述するシステムイベントのほぼリアルタイムのストリームを提供します。EventBridge は、特定のイベントを監視し、これらのイベントが発生したときに他の AWS サービスで自動アクションをトリガーするルールを記述できるため、自動イベント駆動型コンピューティングを有効にします。

  例えば、 は Amazon S3 バケットのアクセス許可チェック Trusted Advisor を提供します。このチェックでは、オープンアクセス許可を持つバケットがあるか、認証された AWS ユーザーへのアクセスを許可するバケットがあるかどうかを確認します。バケットのアクセス許可が変更されると、 Trusted Advisor チェックのステータスが変化します。EventBridge はこのイベントを検出し、ユーザーがアクションを実行できるように通知を送信します。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。
- AWS Trusted Advisor チェックでは、 AWS アカウントのコスト削減、パフォーマンスの向上、セキュリティの向上の方法を特定します。EventBridge を使用して、 Trusted Advisor チェックのステータスをモニタリングできます。その後、Amazon CloudWatch を使用して Trusted Advisor メトリクスのアラームを作成できます。これらのアラームは、更新されたリソースやサービスクォータに達したなど、 Trusted Advisor チェックのステータスが変更されたときに通知します。
- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。が呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

トピック

- Amazon EventBridge による AWS Trusted Advisor チェック結果のモニタリング
- AWS Trusted Advisor メトリクスをモニタリングする Amazon CloudWatch アラームを作成する
- を使用した AWS Trusted Advisor コンソールアクションのログ記録 AWS CloudTrail

Amazon EventBridge による AWS Trusted Advisor チェック結果のモニタリング

EventBridge を使用して、 Trusted Advisor 変更ステータスをチェックするタイミングを検出できます。その後、ルールに指定した値のステータスが変更されたときに、EventBridge は、1 つ以上のターゲットアクションを呼び出します。

ステータス変更に従って、通知を送信したり、ステータス情報を取得したり、是正措置を取ったり、イベントを開始したり、その他の措置を取ることができます。例えば、チェックのステータスが、問題が検出されませんでした (緑) から推奨される対応 (赤) に変わった場合に、次のターゲットタイプを指定できます。

- AWS Lambda 関数を使用して、Slack チャネルに通知を渡します。
- チェックに関するデータを Amazon Kinesis ストリームにプッシュして、包括的でリアルタイムのステータスモニタリングをサポートします。
- Amazon Simple Notification Service トピックをお客様のメールアドレスに送信します。
- Amazon CloudWatch のアラームアクションで通知を受け取ります。

EventBridge 関数と Lambda 関数を使用して Trusted Advisorの応答を自動化する方法の詳細については、GitHubの「Trusted Advisor tools」(ツール) を参照してください。

> **メモ**
>
> - Trusted Advisor は、ベストエフォートベースでイベントを提供します。イベントが常に EventBridge に配信されるとは限りません。
> - Trusted Advisor チェックのルールを作成するには、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 AWS サポート プランが必要です。詳細については、「AWS サポート プランの変更」を参照してください。
> - グローバルサービス Trusted Advisor と同様に、すべてのイベントは米国東部 (バージニア北部) リージョンの EventBridge に発行されます。

EventBridge ルールを作成するには、次の手順に従います Trusted Advisor。イベントルールを作成する前に、次の手順を実行します。

- EventBridge のイベント、ルール、ターゲットに精通しておいてください。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge とは」を参照してください。
- イベントルールで使用するターゲットを作成します。

の EventBridge ルールを作成するには Trusted Advisor

1. Amazon EventBridge コンソールの https://console.aws.amazon.com/events/ を開いてください。
2. リージョンを変更するには、ページの右上にあるリージョンセレクターを使用して、[US East (N. Virginia)] (米国東部 (バージニア北部)) を選択します。
3. ナビゲーションペインで [ルール] を選択します。
4. [Create rule] (ルールを作成) を選択します。
5. [Define rule detail] (ルールの詳細を定義) ページで、ルールの名前と説明を入力します。
6. [Event bus] (イベントバス) と [Rule type] (ルールタイプ) のデフォルト値を維持して、[Next] (次へ) を選択します。
7. [イベントパターンを構築] ページの [イベントソース] で、[AWS イベント] または [EventBridge パートナーイベント] を選択します。
8. [Event pattern] (イベントパターン) で、AWS のサービス をデフォルト値のままにしておきます。
9. [AWS のサービス] で、[Trusted Advisor] を選択します。
10. [Event type] (イベントタイプ) で、[Check Item Refresh Status] (アイテムの更新ステータスを確認) を選択します。
11. チェックのステータスについて、次のいずれかのオプションを選択します。
    - [Any status] (任意のステータス) を選択して、ステータスの変更をモニタリングするルールを作成します。
    - [Specific status(es)] (特定のステータス) を選択してから、ルールでモニタリングする値を選択します。
      - ERROR – Trusted Advisor チェックのアクションを推奨します。
      - INFO – Trusted Advisor チェックのステータスを判断できません。
      - OK – Trusted Advisor チェックの問題は検出されません。
      - WARN – チェックで発生する可能性のある問題 Trusted Advisor を検出し、調査を推奨します。

12. チェックについて、次のいずれかのオプションを選択します。

    - [Any check] (任意のチェック) を選択します。
    - [Specific check(s)] (特定のチェック) を選択し、リストから 1 つ以上のチェック名を選択します。

13. AWS リソースに対して次のいずれかのオプションを選択します。

    - [Any resource ID] (任意のリソース ID) を選択して、すべてのリソースをモニタリングするルールを作成します。
    - ARN ごとの特定のリソース ID を選択し、必要な Amazon リソースネーム (ARN) を入力します。

14. [Next (次へ)] を選択します。
15. [Select target(s)] (ターゲットの選択) 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、そのタイプに必要な追加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。
16. 次へ をクリックします。
17. (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。
18. [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。
19. ルールの作成を選択します。これで、ルールは Trusted Advisor チェックをモニタリングし、指定したターゲットにイベントを送信します。

AWS Trusted Advisor メトリクスをモニタリングする Amazon CloudWatch アラームを作成する

がチェック AWS Trusted Advisor を更新すると、 はチェック結果に関するメトリクスを CloudWatch に Trusted Advisor 発行します。CloudWatch コンソールでメトリクスを表示できます。リソースの Trusted Advisor チェックやステータスの変更、およびサービスクォータの使用 (以前は制限と呼ばれていました) に関するステータスの変更を検出するアラームを作成することもできます。

特定の Trusted Advisor メトリクスの CloudWatch アラームを作成するには、次の手順に従います。

トピック

前提条件

Trusted Advisor メトリクスの CloudWatch アラームを作成する前に、次の情報を確認してください。

- CloudWatch がどのようにメトリクスとアラームを使用するかを理解します。詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch の仕組み」を参照してください。
- Trusted Advisor コンソールまたは AWS サポート API を使用して、チェックを更新し、最新のチェック結果を取得します。詳細については、「チェック結果の更新」を参照してください。

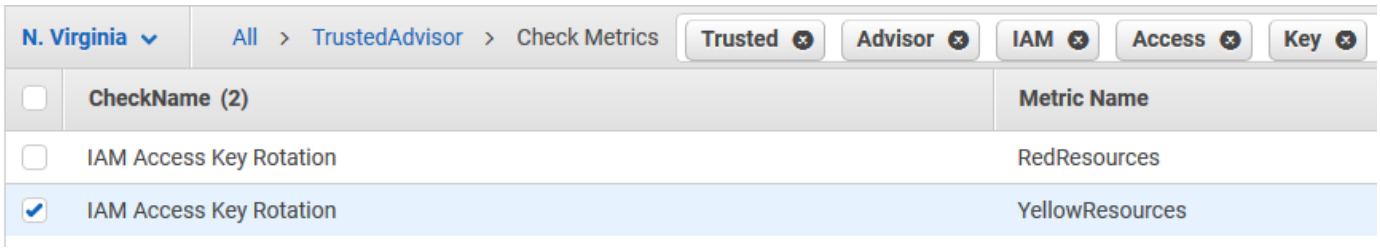
Trusted Advisor メトリクスの CloudWatch アラームを作成するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. リージョンセレクタを使用して、米国東部 (バージニア北部) AWS リージョンを選択します。
3. ナビゲーションペインで、[Alarms] (アラーム) を選択します。
4. [アラームの作成] を選択します。
5. メトリクスの選択 を選択します。
6. [メトリクス] にディメンション値を入力してメトリクスリストをフィルターします。例えば、メトリクス名 ServiceLimitUsage または Trusted Advisor チェック名などのディメンションを入力できます。

   > **Tip**
   >
   > - **`Trusted Advisor`** を検索して、サービスのすべてのメトリクスを一覧表示します。
   > - メトリクスとディメンション名のリストについては、「Trusted Advisor メトリクスとディメンション」を参照してください。

7. 結果の表で、目的のメトリクスのチェックボックスを選択します。

次の例では、チェック名は IAM アクセスキーの更新で、メトリクス名は YellowResources です。

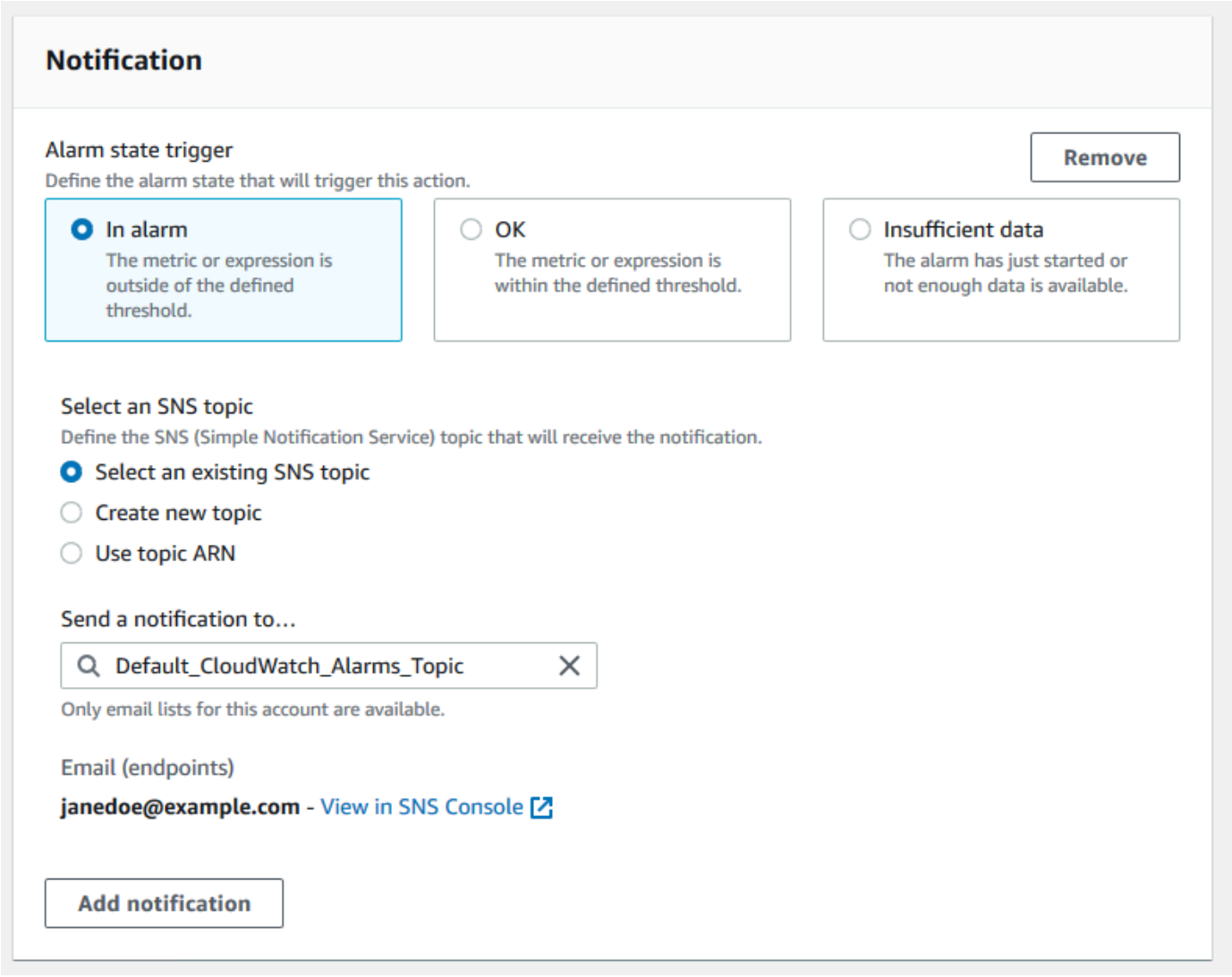


8. [メトリクスの選択] を選択します。
9. [メトリクスと条件の指定] ページで、選択したメトリクス名と チェック名 がページに表示されていることを確認します。
10. [期間] では、チェックのステータスが変化したときにアラームを開始する期間 (5 分など) を指定できます。
11. [条件] で [静的] を選択し、アラームを開始するアラーム条件を指定します。

    例えば、[以上 >= しきい値] を選択し、しきい値に「**1**」と入力すると、過去 90 日間に更新されていない IAM アクセスキーが Trusted Advisor で検出されたときにアラームが開始します。

    > **メモ**
    >
    > - GreenChecks、RedChecks、YellowChecks、RedResources、および YellowResources の各メトリクスで、0 以上の任意の整数であるしきい値を指定できます。
    > - Trusted Advisor は、 Trusted Advisor が問題を検出していないリソースである GreenResources のメトリクスを送信しません。

12. [Next (次へ)] を選択します。
13. [アクションの設定] ページの [アラーム状態トリガー] で [アラーム状態] を選択します。
14. [SNS トピックの選択] で既存の Amazon Simple Notification Service (Amazon SNS) トピックを選択するか、トピックを新規作成します。



15. [Next (次へ)] を選択します。
16. [名前と説明] にアラームの名前と説明を入力します。
17. [Next (次へ)] を選択します。
18. [プレビューと作成] ページでアラームの詳細をレビューし、[アラームの作成] を選択します。

    [IAM アクセスキーの更新] チェックのステータスが 5 分間、赤になった場合、アラームは SNS トピックに通知を送信します。

Example : CloudWatch アラームの E メール通知

次の E メールメッセージは、アラームが IAM アクセスキーの更新チェックの変化を検出したことを示します。

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the
 ALARM state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my
 AWS account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1
 datapoint for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0
 for 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

Trusted Advisorの CloudWatch メトリクス

CloudWatch コンソールまたは AWS Command Line Interface （ AWS CLI) を使用して、 で使用できるメトリクスを検索できます Trusted Advisor。

メトリクスを発行するすべてのサービスの名前空間、メトリクス、ディメンションのリストについては、Amazon CloudWatch ユーザーガイドの「CloudWatch メトリクスを発行するAWS のサービス」を参照してください。

Trusted Advisor メトリクスを表示する (コンソール)

CloudWatch コンソールにサインインして、使用可能なメトリクスを表示できます Trusted Advisor。

使用可能な Trusted Advisor メトリクスを表示するには (コンソール)

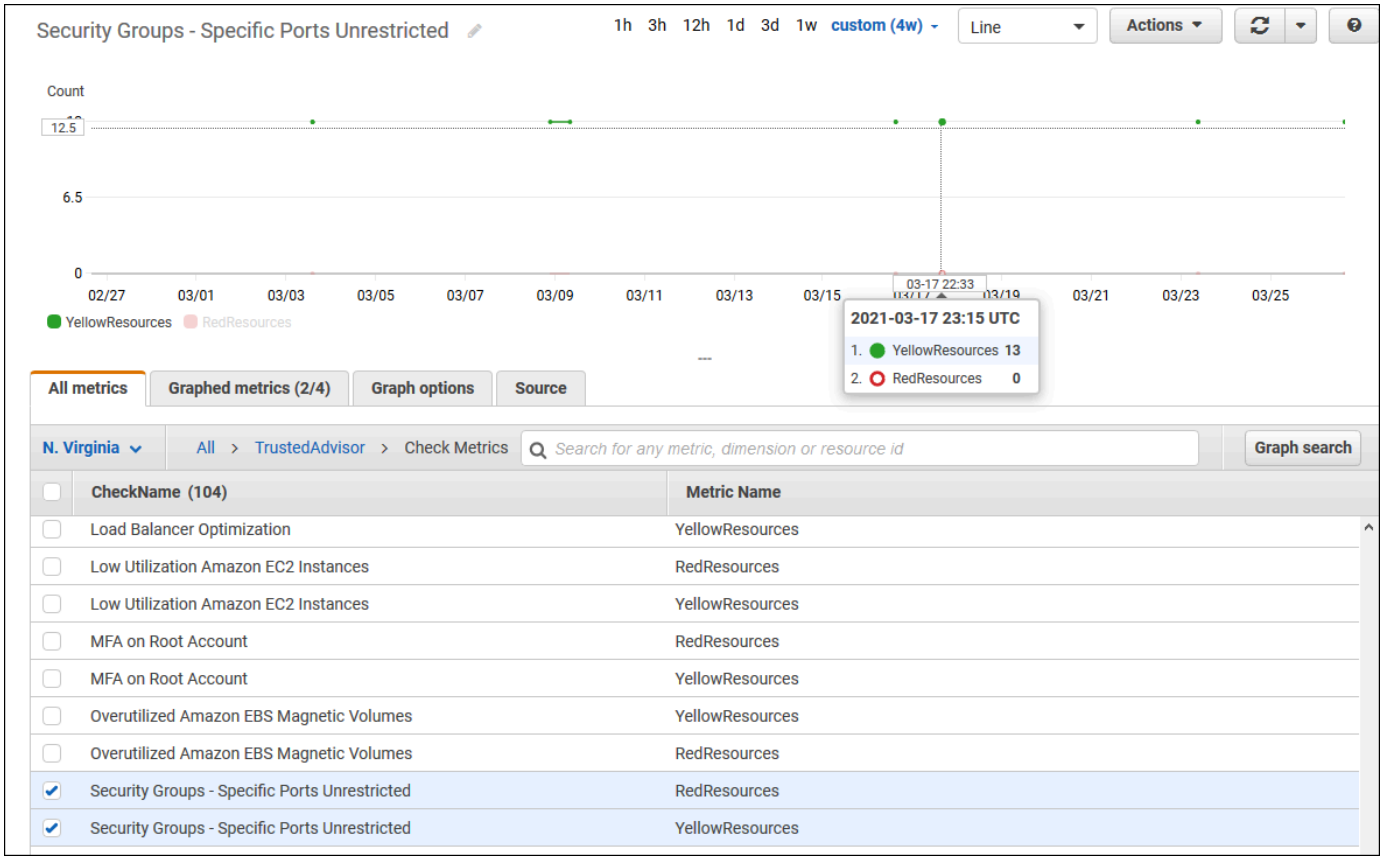
1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. リージョンセレクタを使用して、米国東部 (バージニア北部 ） AWS リージョンを選択します。
3. ナビゲーションペインで Metrics (メトリクス) を選択します。
4. メトリックの名前空間を入力します (**`TrustedAdvisor`** など)。
5. メトリクスのディメンションを選択します ([Check Metrics] など)。
6. [すべてのメトリクス] タブには、名前空間内のそのディメンションのメトリクスがすべて表示されます。以下の操作を行うことができます。

   a. テーブルを並べ替えるには、列見出しを選択します。

   b. メトリクスをグラフ表示するには、メトリクスの横にあるチェックボックスを選択します。すべてのメトリクスを選択するには、テーブルの見出し行にあるチェックボックスを選択します。

   c. メトリクスでフィルターするには、メトリクス名を選択し、[Add to search] (検索に追加) を選択します。

   次の例は、[セキュリティグループ - 開かれたポート] チェックの結果を示しています。このチェックでは、黄色の 13 個のリソースが識別されます。黄色のチェックを調査する Trusted Advisor ことをお勧めします。



7. (オプション) このグラフを CloudWatch ダッシュボードに追加するには、[Actions] (アクション)、[Add to dashboard] (ダッシュボードに追加) の順に選択します。

   メトリクスを表示するグラフの作成の詳細については、Amazon CloudWatch ユーザーガイドの「メトリクスのグラフ化」を参照してください。

Trusted Advisor メトリクスを表示する (CLI)

list-metrics AWS CLI コマンドを使用して、使用可能なメトリクスを表示できます Trusted Advisor。

Example : のすべてのメトリクスを一覧表示する Trusted Advisor

次の例では、すべてのメトリクスを表示するAWS/TrustedAdvisor名前空間を指定します Trusted Advisor。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

出力は次のようになります。

```
{
```

```
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
```

```
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : ディメンションのすべてのメトリクスの一覧表示

次の例では、指定した AWS リージョンで使用可能なメトリクスを表示する AWS/TrustedAdvisor 名前空間と Region ディメンションを指定します。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

出力は次のようになります。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
```

```
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
```

```
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example : 特定のメトリクス名のメトリクスの一覧表示

次の例では、この指定のメトリクスの結果だけを表示する AWS/TrustedAdvisor 名前空間と RedResources メトリクス名を指定します。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

出力は次のようになります。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
```

```
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Trusted Advisor メトリクスとディメンション

CloudWatch アラームとグラフに使用できる Trusted Advisor メトリクスとディメンションについては、次の表を参照してください。

Trusted Advisor チェックレベルのメトリクス

Trusted Advisor チェックには次のメトリクスを使用できます。

メトリクス	説明
RedResources	赤色の状態のリソースの数 (アクションが推奨されます)。
YellowResources	黄色の状態のリソースの数 (調査が推奨されます)。

Trusted Advisor サービスクォータレベルのメトリクス

AWS のサービス クォータには次のメトリクスを使用できます。

メトリクス	説明
ServiceLimitUsage	サービスクォータ (以前の名称は制限) に対するリソース使用状況の割合。

チェックレベルメトリクスのディメンション

Trusted Advisor チェックには次のディメンションを使用できます。

ディメンション	説明
CheckName	Trusted Advisor チェックの名前。 すべてのチェック名は、Trusted Advisor コンソールまたは AWS Trusted Advisor チェックリファレンス に表示されます。

サービスクォータメトリクスのディメンション

Trusted Advisor サービスクォータメトリクスには、次のディメンションを使用できます。

ディメンション	説明
Region	サービスクォータ AWS リージョン の 。
ServiceName	AWS のサービスの名前。
ServiceLimit	サービスクォータの名前。 Service Quotas の詳細については、「AWS 全般のリファレンス」の「AWS のサービス クォータ」を参照してください。

を使用した AWS Trusted Advisor コンソールアクションのログ記録 AWS CloudTrail

Trusted Advisor は、ユーザー AWS CloudTrail、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています Trusted Advisor。CloudTrail は、

のアクションをイベント Trusted Advisor としてキャプチャします。キャプチャされた呼び出しには、 Trusted Advisor コンソールからの呼び出しが含まれます。証跡を作成する場合は、 イベントなど、Amazon Simple Storage Service (Amazon S3) バケットへの CloudTrail イベントの継続的な配信を有効にすることができます Trusted Advisor。証跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを表示できます。CloudTrail によって収集された情報を使用して、リクエストの実行元の IP アドレス Trusted Advisor、リクエストの実行者、リクエストの実行日時などの詳細を確認できます。

CloudTrail を設定して有効にする方法などの詳細については、AWS CloudTrail 「ユーザーガイド」を参照してください。

Trusted Advisor CloudTrail の情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。 Trusted Advisor コンソール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、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。 AWS アカウントで最近のイベントを表示、検索、ダウンロードできます。詳細については、「Viewing Events with CloudTrail Event History」を参照してください。

のイベントなど、 AWS アカウントのイベントの継続的な記録については Trusted Advisor、証跡を作成します。証跡により、ログファイルを CloudTrail で 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、すべての AWS リージョンに証跡が適用されます。証跡は、 AWS パーティション内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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 証跡の作成の概要
- CloudTrail がサポートするサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- CloudTrail ログファイルの複数のリージョンからの受け取り、複数のアカウントから CloudTrail ログファイルを受け取る

Trusted Advisor は、 Trusted Advisor コンソールアクションのサブセットを CloudTrail ログファイルのイベントとしてログ記録することをサポートしています。CloudTrail は、以下のアクションをログに記録します。

- `BatchUpdateRecommendationResourceExclusion`

- CreateEngagement
- CreateEngagementAttachment
- CreateEngagementCommunication
- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization
- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements

- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences
- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

Trusted Advisor コンソールアクションの完全なリストについては、「」を参照してくださいTrusted Advisor アクション。

> **Note**
>
> CloudTrail は、 Trusted Advisor API AWS サポート リファレンスの API オペレーションもログに記録します。詳細については、「を使用した AWS サポート API コールのログ記録 AWS CloudTrail」を参照してください。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。

- 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 エレメント」を参照してください。

例: Trusted Advisor ログファイルエントリ

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Example : RefreshCheck のログエントリ

次の例は、Amazon S3 バケットのバージョニングチェック (ID R365s2Qddf) の `RefreshCheck` アクションを示す CloudTrail のログエントリを示しています。


```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:06:33Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"RefreshCheck",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.136",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "checkId":"R365s2Qddf"
        },
```

```
        "responseElements":{
        "status":{
        "checkId":"R365s2Qddf",
        "status":"enqueued",
        "millisUntilNextRefreshable":3599993
        }
        },
        "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
        "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : UpdateNotificationPreferences のログエントリ

以下の例は、UpdateNotificationPreferences アクションを示す CloudTrail ログエントリです。

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2020-10-21T22:06:18Z"
        }
        }
        },
        "eventTime":"2020-10-21T22:09:49Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"UpdateNotificationPreferences",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.34.167",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "contacts":[
```

```
        {
        "id":"billing",
        "type":"email",
        "active":false
        },
        {
        "id":"operational",
        "type":"email",
        "active":false
        },
        {
        "id":"security",
        "type":"email",
        "active":false
        }
        ],
        "language":"en"
        },
        "responseElements":null,
        "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
        "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

Example : GenerateReport のログエントリ

以下の例は、GenerateReport アクションを示す CloudTrail ログエントリです。このアクションにより、 AWS 組織のレポートが作成されます。

```
{
        "eventVersion":"1.04",
        "userIdentity":{
        "type":"IAMUser",
        "principalId":"AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/janedoe",
        "accountId":"123456789012",
        "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
        "userName":"janedoe",
        "sessionContext":{
        "attributes":{
        "mfaAuthenticated":"false",
```

```
        "creationDate":"2020-11-03T13:03:10Z"
        }
        }
        },
        "eventTime":"2020-11-03T13:04:29Z",
        "eventSource":"trustedadvisor.amazonaws.com",
        "eventName":"GenerateReport",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"100.127.36.171",
        "userAgent":"signin.amazonaws.com",
        "requestParameters":{
        "refresh":false,
        "includeSuppressedResources":false,
        "language":"en",
        "format":"JSON",
        "name":"organizational-view-report",
        "preference":{
        "accounts":[

        ],
        "organizationalUnitIds":[
        "r-j134"
        ],
        "preferenceName":"organizational-view-report",
        "format":"json",
        "language":"en"
        }
        },
        "responseElements":{
        "status":"ENQUEUED"
        },
        "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
        "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
        }
```

トラブルシューティングリソース

一般的なトラブルシューティングの質問に対する回答については、AWS サポート ナリッジセンターを参照してください。

Windows の場合、Amazon EC2 は EC2Rescue を提供します。EC2Rescue を使用すると、Windows インスタンスを調べて、一般的な問題の特定、ログファイルの収集、問題の サポート トラブルシューティングに役立てることができます。EC2Rescue を使用して、動作していないインスタンスのブートボリュームを分析することもできます。詳細については、How can I use EC2Rescue to troubleshoot and fix common issues on my EC2 Windows instance? を参照してください。

サービス固有のトラブルシューティング

ほとんどの AWS のサービス ドキュメントには、 に連絡する前に開始できるトラブルシューティングトピックが含まれています AWS サポート。次の表は、サービスごとに並べたトラブルシューティングトピックのリンク一覧です。

> **Note**
>
> 次の表は、最も一般的なサービスの一覧です。トラブルシューティングに関する他のトピックを検索するには、AWS ドキュメントのランディングページにある検索用のテキストボックスを使用します。

サービス	リンク
Amazon Web Services	AWS Signature Version 4 エラーのトラブルシューティング
Amazon API Gateway	HTTP API の問題のトラブルシューティング
Amazon AppStream	Amazon AppStream のトラブルシューティング
Amazon Athena	Athena でのトラブルシューティング
Amazon Aurora MySQL	Amazon Aurora のトラブルシューティング
Amazon Aurora PostgreSQL	Amazon Aurora のトラブルシューティング

サービス	リンク
Amazon EC2 Auto Scaling	Auto Scaling のトラブルシューティング
AWS Certificate Manager (ACM)	トラブルシューティング
AWS CloudFormation	AWS CloudFormation のトラブルシューティング
Amazon CloudFront	トラブルシューティング | RTMP ディストリビューションをトラブルシューティングする
AWS CloudHSM	トラブルシューティング
Amazon CloudSearch	Amazon CloudSearch のトラブルシューティング
AWS CodeDeploy	AWS CodeDeploy のトラブルシューティング
Amazon CloudWatch	https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-metric-streams-troubleshoot.html のトラブルシューティング
AWS Database Migration Service	での移行タスクのトラブルシューティング AWS Database Migration Service
AWS Data Pipeline	トラブルシューティング
AWS Direct Connect	AWS Direct Connect のトラブルシューティング
AWS Directory Service	AWS Directory Service 管理に関する問題のトラブルシューティング
Amazon DynamoDB	トラブルシューティング | SSL/TLS 接続の確立に関する問題のトラブルシューティング
AWS Elastic Beanstalk	トラブルシューティング

サービス	リンク
Amazon Elastic Compute Cloud (Amazon EC2)	インスタンスのトラブルシューティング | Windows インスタンスのトラブルシューティング | VM Import/Export のトラブルシューティング | API リクエストエラーのトラブルシューティング
Amazon エラスティックコンテナサービス (Amazon ECS)	Amazon ECS のトラブルシューティング
Amazon エラスティックKubernetesサービス (Amazon EKS)	Amazon EKS のトラブルシューティング
エラスティックロードバランシング	Application Load Balancer のトラブルシューティング | Classic Load Balancer のトラブルシューティングを行う
Amazon ElastiCache (Memcached)	アプリケーションのトラブルシューティング
Amazon ElastiCache (Redis OSS)	アプリケーションのトラブルシューティング
Amazon EMR	クラスターをトラブルシューティングする
AWS Flow Framework	Troubleshooting and Debugging Tips
AWS Glue	トラブルシューティング AWS Glue
AWS Glue DataBrew	AWS Glue DataBrewでのアイデンティティとアクセスに関するトラブルシューティング
AWS GovCloud (US)	トラブルシューティング
AWS Identity and Access Management (IAM)	IAM のトラブルシューティング
Amazon Keyspaces (Apache Cassandra 向け)	Amazon Keyspaces (Apache Cassandra 向け) のトラブルシューティング

サービス	リンク
Amazon Kinesis Data Streams	Amazon Kinesis Data Streams プロデューサーのトラブルシューティング | Amazon Kinesis Data Streams コンシューマーのトラブルシューティング
Amazon Managed Service for Apache Flink	パフォーマンスのトラブルシューティング|SQL アプリケーション用 Amazon Managed Service for Apache Flink のトラブルシューティング
Amazon Data Firehose	Amazon Data Firehose のトラブルシューティング
AWS Lambda	CloudWatch を使用した AWS Lambda 関数のトラブルシューティングとモニタリング
Amazon OpenSearch Service	Amazon OpenSearch Service のトラブルシューティング
AWS OpsWorks	デバッグとトラブルシューティングのガイド
Amazon Personalize	トラブルシューティング
Amazon QLDB	Amazon QLDB のトラブルシューティング
Amazon QuickSight	Amazon QuickSight のトラブルシューティング | スキップされた行のエラーのトラブルシューティング
AWS Resource Access Manager (AWS RAM)	AWS RAMの問題のトラブルシューティング
Amazon Redshift	クエリのトラブルシューティング | データロードのトラブルシューティング | Amazon Redshift における接続の問題のトラブルシューティング | Amazon Redshift 監査ログ作成のトラブルシューティング | Amazon Redshift Spectrum でのクエリのトラブルシューティング
Amazon Relational Database Service (Amazon RDS)	トラブルシューティング | Amazon RDS 上のアプリケーションのトラブルシューティング | Amazon RDS Custom の DB に関する問題のトラブルシューティング
Amazon Route 53	Amazon Route 53 のトラブルシューティング

サービス	リンク
Amazon SageMaker AI	エラーのトラブルシューティング | Amazon SageMaker AI Studio のトラブルシューティング
Amazon Silk	トラブルシューティング
Amazon Simple Email Service (Amazon SES)	Amazon SES のトラブルシューティング
Amazon Simple Storage Service (Amazon S3)	トラブルシューティング
Amazon Simple Workflow Service (Amazon SWF)	AWS Java 用 フローフレームワーク: トラブルシューティングとデバッグのヒント | AWS Ruby 用 フローフレームワーク: ワークフローのトラブルシューティングとデバッグ
AWS Storage Gateway	ゲートウェイのトラブルシューティング
AWS Systems Manager	SSM エージェントのトラブルシューティング
Amazon Virtual Private Cloud (Amazon VPC)	トラブルシューティング
AWS Virtual Private Network (AWS VPN)	カスタマーゲートウェイデバイスのトラブルシューティング
AWS WAF	AWS WAF 保護のテストとチューニング
Amazon WorkMail	Amazon WorkMail ウェブアプリケーションのトラブルシューティング
Amazon WorkSpaces	Amazon WorkSpaces に関する問題のトラブルシューティング | Amazon WorkSpaces クライアントに関する問題のトラブルシューティング

ドキュメント履歴

次の表は、 AWS サポート サービスの最終リリース以降のドキュメントの重要な変更点を示しています。

- AWS サポート API バージョン: 2013-04-15
- AWS サポート アプリ API バージョン： 2021-08-20

次の表は、2021 年 5 月 10 日以降の AWS サポート および AWS Trusted Advisor ドキュメントの重要な更新を示しています。RSS フィードにサブスクライブすると、更新に関する通知を受け取ることができます。

変更	説明	日付
のカテゴリレベルのメトリクスへの参照を削除 Trusted Advisor	のカテゴリレベルのメトリクス Trusted Advisor は廃止されました。カテゴリレベルのメトリクスへの参照は、AWS Trusted Advisor メトリクスをモニタリングする Amazon CloudWatch アラームの作成から削除されます。	2025 年 1 月 27 日
のドキュメントを更新しました Trusted Advisor	AWS CloudTrail 管理イベントのログ記録と Amazon RDS 継続的バックアップが有効になっていないという 2 つの新しいチェックが追加されました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2024 年 12 月 23 日
のドキュメントを更新しました Trusted Advisor	Auto Scaling グループのリソースを更新しました。詳細については、AWS Trusted	2024 年 12 月 23 日

	Advisor「チェックの変更ログ」を参照してください。	
のドキュメントを更新しました Trusted Advisor	IAM Access Analyzer の外部アクセスチェックを更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 12 月 23 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2024 年 11 月 25 日
のドキュメントを更新しました Trusted Advisor	1 つの新しい Trusted Advisor チェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 11 月 22 日
AWS パートナー主導サポートの AWS マネージドポリシーに関するドキュメントを追加しました	新しい AWS 管理ポリシー のドキュメントを追加しましたAWSPartnerLedSupportReadOnlyAccess 。詳細については、「 AWSAWS パートナー主導サポートの マネージドポリシー」を参照してください。	2024 年 11 月 22 日

のドキュメントを更新しました Trusted Advisor	3 Trusted Advisor checks を更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 11 月 7 日
AWS サポート プランのドキュメントを更新しました	Logging サポート Plans API コールの AWS CloudTrailページに `ListSupportPlanModifiers` オペレーションの新しいログ例を追加しました。	2024 年 11 月 6 日
`AWSTrustedAdvisorServiceRolePolicy` のドキュメントの更新	新しいセキュリティチェックをオンボード`elasticloadbalancing:DescribeRules` するための新しい IAM アクション `elasticloadbalancing:DescribeListeners` と を追加しました。詳細については、「AWS マネージドポリシーAWSTrustedAdvisorServiceRolePolicy」を参照してください。	2024 年 10 月 30 日
のドキュメントを更新しました Trusted Advisor	4 つの新しい Trusted Advisor チェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 10 月 11 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2024 年 10 月 8 日
のドキュメントを更新しました Trusted Advisor	障害耐性の柱の下に 1 つのコスト最適化チェックを移動しました。1 セキュリティチェックと 1 耐障害性チェックを更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 10 月 2 日
AWS Trusted Advisor Engage セクションを更新しました	AWS Trusted Advisor Engage セクションを更新して AWS 、カウントダウンを参照しました。詳細については、「Get started with AWS Trusted Advisor Engage (プレビュー)」を参照してください。	2024 年 9 月 16 日

AWS サポート プランのドキュメントを更新しました	サポートプラン修飾子のリストを表示するための新しいアクセス許可と CloudTrail ドキュメントを追加しました。詳細については、「 AWS サポート プランへのアクセスの管理」、「 プランAWS の管理ポリシー」、「 を使用した AWS サポート プラン API コールのログ記録」を参照してください。 AWS サポート AWS CloudTrail	2024 年 9 月 9 日
のドキュメントを更新しました Trusted Advisor	Trusted Advisor は 8 月 23 日に 9 件の新しいチェックを追加しました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2024 年 8 月 23 日
のドキュメントを更新しました Trusted Advisor	1 Trusted Advisor Operational Excellence チェックを更新し、1 つの新しい Trusted Advisor セキュリティチェックを追加しました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2024 年 8 月 22 日
のドキュメントを更新しました Trusted Advisor	6 Trusted Advisor Security チェックを更新しました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2024 年 8 月 20 日

のドキュメントを更新しました Trusted Advisor	2 Trusted Advisor checks を更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 8 月 12 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2024 年 8 月 5 日
のドキュメントを更新しました Trusted Advisor	9 Trusted Advisor Checks を更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 7 月 21 日

AWSTrustedAdvisorServiceRolePolicy のドキュメントの更新	新しいチェックをオンボードするためにsqs:GetQueueAttributes cloudwatch:ListMetrics dax:DescribeClusters 、新しい IAM アクションec2:DescribeNatGateways access-analyzer:ListAnalyzers 、ec2:DescribeRouteTables 、、、ec2:DescribeVpcEndpoints 、、ec2:GetManagedPrefixListEntries elasticloadbalancing:DescribeTargetHealth 、、iam:ListSAMLProviders kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall を追加しました。詳細については、「AWS マネージドポリシーAWSTrustedAdvisorServiceRolePolicy」を参照してください。	2024 年 6 月 11 日
AWS サポート 推奨事項のドキュメントを追加	AWS サポート 推奨事項のドキュメントを追加しました。	2024 年 5 月 22 日
AWS サポート 推奨事項のドキュメントを追加	AWS サポート 推奨事項のドキュメントを追加しました。	2024 年 5 月 20 日

ドキュメントから 5 つの AWS Trusted Advisor チェックを削除	廃止された 5 つの AWS Trusted Advisor チェックを削除しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 5 月 15 日
ドキュメントに 1 つの新しい AWS Trusted Advisor セキュリティチェックを追加	ドキュメントに 1 つの新しい AWS Trusted Advisor セキュリティチェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 5 月 15 日
ドキュメントから 3 つの耐障害性チェックを削除	廃止された 3 つの耐障害性チェックを削除しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 4 月 25 日
障害耐性とセキュリティチェックのドキュメントを更新	1 つの新しい耐障害性チェックを追加しました。1 つの耐障害性と 1 つのセキュリティチェックを更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 3 月 29 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2024 年 3 月 22 日
サポート プランのドキュメントを更新	サポート プランの機能の更新。詳細については、「 サポート プラン」を参照してください。	2024 年 3 月 11 日
のドキュメントを更新しました Trusted Advisor	耐障害性チェックを 1 つ追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 2 月 29 日
のドキュメントを更新しました Trusted Advisor	耐障害性チェックを 1 つ追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 1 月 31 日

AWSTrustedAdvisorServiceRolePolicy のドキュメントの更新	新しいチェックをオンボードoutposts:ListAssets outposts:ListOutposts するためにcloudtrail:GetTrail 、新しい IAM cloudtrail:ListTrails アクション cloudtrail:GetEventSelectors 、、outposts:GetOutpost 、、 を追加しました。詳細については、「AWS マネージドポリシーAWSTrustedAdvisorServiceRolePolicy」を参照してください。	2024 年 1 月 18 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2024 年 1 月 17 日
のドキュメントを更新しました Trusted Advisor	タイトルと説明を修正するために 1 つの耐障害性チェックを更新しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2024 年 1 月 8 日

のドキュメントを更新しました Trusted Advisor	1 つのセキュリティチェックを更新し、非推奨期間の変更が反映されるようにしました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2023 年 12 月 21 日
のドキュメントを更新しました Trusted Advisor	2 つのセキュリティチェックと 2 つのパフォーマンスチェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2023 年 12 月 20 日
のドキュメントを更新しました Trusted Advisor	1 つのセキュリティチェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2023 年 12 月 15 日
Trusted Advisor Engage のドキュメントを更新しました	Trusted Advisor Engage のドキュメントを更新し、E メール通知のオプションを変更しました。	2023 年 12 月 14 日
Trusted Advisor Engage のドキュメントを更新しました	Trusted Advisor Engage のドキュメントを更新し、スケジュールされたエンゲージメントを変更しました。	2023 年 12 月 11 日
のドキュメントを更新しました Trusted Advisor	2 つの新しい耐障害性チェックと 1 つのコスト最適化チェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2023 年 12 月 7 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 12 月 6 日
の AWS 管理ポリシーを更新しました Trusted Advisor	AWSTrustedAdvisorPriorityFullAccess および AWSTrustedAdvisorPriorityReadOnlyAccess AWS マネージドポリシーを更新して、ステートメント IDs。詳細については、「AWS Trusted AdvisorのAWS マネージドポリシー」を参照してください。	2023 年 12 月 6 日
のドキュメントを更新しました Trusted Advisor	に 3 つの新しい耐障害性チェックを追加しました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2023 年 11 月 17 日
のドキュメントを更新しました Trusted Advisor	Amazon RDS に 37 個の新しいチェックを追加しました。詳細については、AWS Trusted Advisor 「チェックの変更ログ」を参照してください。	2023 年 11 月 15 日

AWSTrustedAdvisorServiceRolePolicy のドキュメントの更新	新しいチェックをオンボードするための新しい IAM アクション ec2:DescribeRegions 、s3:GetLifecycleConfiguration 、ecs:DescribeTaskDefinition および ecs:ListTaskDefinitions が追加されました。詳細については、「AWS マネージドポリシーAWSTrustedAdvisorServiceRolePolicy」を参照してください。	2023 年 11 月 9 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 10 月 27 日
のドキュメントを更新しました Trusted Advisor	から統合された 64 の新しいチェックを追加しました AWS Config。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2023 年 10 月 26 日
のドキュメントを更新しました Trusted Advisor	に 6 つの新しい耐障害性チェックを追加しました Trusted Advisor。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 10 月 12 日

AWSTrustedAdvisorServiceRolePolicy のドキュメントの更新	新しい耐障害性チェックをオンボードするための新しい IAM アクション route53resolver:ListResolverEndpoints 、route53resolver:ListResolverEndpointIpAddresses 、ec2:DescribeSubnets 、kafka:ListClustersV2 、kafka:ListNodes が追加されました。詳細については、「AWS マネージドポリシーAWSTrustedAdvisorServiceRolePolicy」を参照してください。	2023 年 9 月 14 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 8 月 28 日
のドキュメントを更新しました Trusted Advisor	1 つの新しいサービス制限チェックが追加されましたAWS Lambda。詳細については、「チェックの変更ログAWS Trusted Advisor」を参照してください。	2023 年 8 月 17 日

のドキュメントを更新しました Trusted Advisor	Lambda の新しい耐障害性チェックを 1 つ追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 8 月 3 日
Trusted Advisor Engage のドキュメントを更新しました	エンゲージメントを作成および編集するためのフォームを変更して Trusted Advisor Engage ドキュメントを更新しました。のサービスコントロールポリシーの例を含むページを追加しました AWS Trusted Advisor。	2023 年 7 月 27 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 6 月 26 日
のドキュメントを更新しました Trusted Advisor	Amazon MQ に関する耐障害性チェックを新たに 2 つ追加しました。Amazon Elastic File System に関する新しい耐障害性チェックを 1 つと新しいパフォーマンスチェックを 1 つ追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 6 月 1 日

のドキュメントを更新しました Trusted Advisor	新しい耐障害性チェックを NAT ゲートウェイ用に 2 つ追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 5 月 16 日
AWS サポート プランのドキュメントを更新しました	サポートプランのスケジュールを作成するための新しいアクセス許可と CloudTrail ドキュメントを追加しました。詳細については、AWS サポート 「プランへのアクセスの管理」、AWSAWS サポート 「プランの 管理ポリシー」、「 を使用した AWS サポート プラン API コールのログ記録 AWS CloudTrail」を参照してください。	2023 年 5 月 8 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 5 月 2 日

Trusted Advisor Engage と Trusted Advisor Priority のドキュメントを更新	Trusted Advisor Engage と Trusted Advisor Priority の前提条件を明確にしました。Trusted Advisor Engage の使用や、 Trusted Advisorへの信頼できるアクセスの有効化が行える IAM ポリシーの例を追加しました。	2023 年 4 月 28 日
のドキュメントを更新しました Trusted Advisor	AWS Resilience Hub と Incident Manager の 2 つの新しい耐障害性チェックを追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 4 月 27 日
Trusted Advisor Engage のドキュメントを追加	AWS Trusted Advisor Engage を使用すると、すべてのプロアクティブなエンゲージメントを簡単に確認、リクエスト、追跡し、進行中のエンゲージメントについて AWS アカウント チームと通信できるため、 AWS サポート プランを最大限に活用できます。詳細については、「AWS Trusted Advisor Engage の使用を開始する」を参照してください。	2023 年 4 月 6 日
のドキュメントを更新しました Trusted Advisor	Amazon ECS の耐障害性チェックを新たに 2 つ追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2023 年 3 月 30 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 3 月 16 日
Trusted Advisor Priority のドキュメントを追加しました	Trusted Advisor Priority コンソールを更新しました。 • [了解] ボタンと [無視] ボタンが [確認] ボタンと [却下] ボタンに置き換えられました。 • レコメンデーションを確認、解決、却下、または再開するために役職や名前を入力する必要はありません。 詳細については、Trusted Advisor 「優先度の開始方法」を参照してください。	2023 年 2 月 16 日
のコード例を更新 サポート	Software AWS Development Kit (SDK) サポート で を使用する方法を示す .NET、Java、および Kotlin コード例を追加しました。詳細については、「SDK サポート を使用するためのコード例 AWS SDKs」を参照してください。	2023 年 1 月 16 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2023 年 1 月 10 日
AWS サポート アプリのドキュメントを更新しました	フィルターオプションを使用するか、ケース ID で検索することにより、Slack でサポートケースを検索できます。詳細については、「Slack でのサポートケースの検索」を参照してください。	2022 年 12 月 29 日
AWS サポート アプリのドキュメントを更新しました	Terraform を使用して、 AWS サポート アプリのリソースを作成することもできます。詳細については、「Terraform を使用して AWS サポート アプリリソースを作成する」を参照してください。	2022 年 12 月 22 日
のドキュメントを更新しました Trusted Advisor	Amazon MemoryDB、Amazon ElastiCache、 AWS CloudHSM向けの 3 つの新しい耐障害性チェックを追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2022 年 12 月 15 日

Slack の AWS サポート アプリのドキュメントを更新しました	次のオプションでライブチャットサポートをリクエストできるようになりました。 • アカウントおよび請求サポートケース • テクニカルサポートケースの日本語サポート。 • 詳細については、「Slack チャンネルでのサポートケースの作成」を参照してください。	2022 年 12 月 14 日
のドキュメントを更新しました AWS サポート	サポート API の新しいエンドポイ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 サポート API について」を参照してください。	2022 年 12 月 14 日
Slack の AWS サポートアプリに使用する AWS CloudFormation テンプレートのドキュメントを追加しました	CloudFormation テンプレートを使用して、 AWS アカウント の Slack 設定ワークスペースとチャネルを作成できます AWS Organizations。詳細については、「 を使用した AWS サポート アプリリソースの作成 AWS CloudFormation」を参照してください。	2022 年 12 月 5 日
のドキュメントを更新しました Trusted Advisor	の 2 つの新しい耐障害性チェックを追加しました AWS Resilience Hub。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2022 年 11 月 17 日

で AWS Security Hub の検出結果に関するドキュメントを追加しました Trusted Advisor	Security Hub コントロールからの検出結果は、より Trusted Advisor 迅速に から削除されます。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2022 年 11 月 17 日
のドキュメントを更新しました AWS Trusted Advisor	Trusted Advisor 推奨事項のドキュメントを追加しました。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2022 年 11 月 16 日
Slack の AWS サポート アプリのドキュメントを更新しました	日本語サポートのドキュメントを追加しました。詳細については、「Slack チャンネルでのサポートケースの作成」を参照してください。	2022 年 11 月 11 日
AWS サポート プランのドキュメントを更新しました	組織がサポートプランにアクセスできるようにするためのトラブルシューティングの情報を追加しました。詳細については、「トラブルシューティング」を参照してください。	2022 年 11 月 9 日
Slack の AWS サポート アプリのドキュメントを更新しました	`supportapp` アクセス許可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 サポート 「アプリが Slack に接続するために必要なアクセス許可」を参照してください。	2022 年 11 月 1 日

Slack の AWS サポート アプリのドキュメントを更新しました	`RegisterSlackWorkspaceForOrganization` API オペレーションを使用して、 AWS アカウントの Slack ワークスペースを登録できます。この API を呼び出すには、 AWS Organizationsの組織に属している必要があります。詳細については、「Slack API リファレンスのAWS サポート アプリ」を参照してください。	2022 年 10 月 19 日
`AWSSupportServiceRolePolicy` のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 10 月 4 日

サポートプランのドキュメントの更新	AWS Identity and Access Management (IAM) を使用して、 のサポートプランを変更するアクセス許可を管理できるようになりました AWS アカウント。詳細については、以下の各トピックを参照してください。 • AWS サポート プランのアクセスの管理 • AWSAWS サポート プランの マネージドポリシー • AWS サポート プランの変更 • を使用した AWS サポート Plans API コールのログ記録 AWS CloudTrail	2022 年 9 月 29 日
Slack の AWS サポート アプリのドキュメントを更新しました	AWS サポート アプリで使用するパブリックチャネルまたはプライベートチャネルを設定する方法に関するドキュメントを追加しました。詳細については、「Configuring a Slack channel」(Slack チャンネルの設定) を参照してください。	2022 年 9 月 22 日
のドキュメントを更新しました AWS サポート	サポートケースのセキュリティに関する新しいセクションを追加しました。詳細については、AWS サポート「ケースのセキュリティ」を参照してください。	2022 年 9 月 9 日

のドキュメントを更新しました Trusted Advisor	Amazon EC2 の新しいセキュリティチェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2022 年 9 月 1 日
Slack の AWS サポート アプリのドキュメントを更新しました	以下のトピックを参照してください。 AWS サポート アプリを使用して、Slack チャネルでサポートケースの管理、サービスクォータの引き上げのリクエスト、サポートエージェントとの直接チャットを行うことができます。詳細については、「AWS サポート App in Slack ドキュメント」を参照してください。 AWS マネージドポリシーを IAM ロールにアタッチして、AWS サポート アプリを使用できます。詳細については、AWS「Slack の AWS サポート アプリの マネージドポリシー」を参照してください。 AWS サポート アプリの新しい API リファレンス。「AWS サポート アプリ API リファレンス」を参照してください。	2022 年 8 月 24 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 8 月 17 日
Trusted Advisor Priority のドキュメントを追加しました	Trusted Advisor Priority では、以下の機能のサポートが追加されています。 • 委任された管理者 • レコメンデーションの概要に関する日次および週次のメール通知 • 解決済みまたは却下済みのレコメンデーションの再オープン • AWS マネージドポリシー 詳細については、Trusted Advisor 「優先度の開始方法」を参照してください。	2022 年 8 月 17 日
のドキュメントを更新しました Trusted Advisor	Trusted Advisor コンソールの環境設定ページが更新されました。詳細については、「 の開始方法 AWS Trusted Advisor」を参照してください。	2022 年 7 月 15 日

のドキュメントを更新しました Trusted Advisor	チェックを更新して、次の情報を含めてください。 • [Alert Criteria] (アラート条件) • [Recommended Action] (推奨されるアクション) • その他のリソース • [Report columns] (レポート列) 詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。	2022 年 7 月 7 日
のドキュメントを更新しました AWS サポート	サポートケースの管理方法を説明するドキュメントを追加しました。 • Updating an existing support case (既存のサポートケースの更新) • トラブルシューティング	2022 年 6 月 28 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための許可を更新しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 6 月 23 日

のドキュメントを更新しました Trusted Advisor	Trusted Advisor は、ソースとなる追加の AWS Foundational Security Best Practices セキュリティ標準コントロールをサポートします AWS Security Hub。詳細については、AWS Trusted Advisor チェックの変更ログを参照してください。	2022 年 6 月 23 日
のドキュメントを更新しました Trusted Advisor	サービスクォータの引き上げをリクエストする方法に関する情報を追加しました。詳細については、「サービス制限」を参照してください。	2022 年 6 月 21 日
のドキュメントを更新しました AWS サポート	Support Center コンソールでケースの作成エクスペリエンスが更新されました。詳細については、サポートケースとケース管理の作成を参照してください。	2022 年 5 月 18 日
のドキュメントを更新しました Trusted Advisor	Amazon EBS および AWS Lambdaのチェックを 4 つ追加しました。詳細については、「オプトイン AWS Compute Optimizer して Trusted Advisor チェックを追加する」を参照してください。	2022 年 5 月 4 日

AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 4 月 27 日
公開アクセスキーチェックのドキュメントが更新されました	このチェックは自動的に更新されます。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2022 年 4 月 25 日
のドキュメントを更新しました Trusted Advisor	耐障害性カテゴリの AWS Direct Connect チェックが更新されます。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2022 年 3 月 29 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 3 月 14 日

Trusted Advisor Priority のドキュメントを追加しました	Trusted Advisor Priority を使用して、テクニカルアカウントマネージャー (TAM) からの優先順位付きレコメンデーションのリストを表示できます。詳細については、Trusted Advisor 「優先度の開始方法」を参照してください。	2022 年 2 月 28 日
での Amazon EventBridge の使用に関するドキュメントを更新しました Trusted Advisor	EventBridge ルールを作成して、 Trusted Advisor チェックの変更をモニタリングできます。詳細については、「EventBridge での AWS Trusted Advisor チェック結果のモニタリング」を参照してください。	2022 年 2 月 21 日
Amazon EventBridge を使用して AWS サポート ケースをモニタリングするための新しいドキュメント	EventBridge ルールを作成して、サポートケースに関する通知をモニタリングおよび受信できます。詳細については、「EventBridge での サポート ケースのモニタリング」を参照してください。	2022 年 2 月 21 日
AWSSupportServiceRolePolicy のドキュメントの更新	請求サービス、管理サービス、およびサポートサービスをサービスにリンクされたロールに提供するための新しい許可を追加しました。詳細については、「AWS マネージドポリシーAWSSupportServiceRolePolicy」を参照してください。	2022 年 2 月 17 日

との統合に関するドキュメントを追加 AWS Security Hub	Trusted Advisor コンソールで、 AWS Foundational Security Best Practices セキュリティ標準の一部である Security Hub コントロールの結果を表示できるようになりました。詳細については、「 AWS Trusted Advisor コンソールでの AWS Security Hub コントロールの表示」を参照してください。	2022 年 1 月 18 日
のドキュメントを更新しました Trusted Advisor	Microsoft SQL Server を実行している Amazon EC2 インスタンスの 3 つの新しいチェックを追加しました。 • Amazon EC2 インスタンスの統合 (Microsoft SQL Server 向け) • 過剰にプロビジョニングされた Amazon EC2 インスタンス (Microsoft SQL サーバー向け) • Microsoft SQL Server を使用した Amazon EC2 インスタンスのサポートの終了 詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。	2021 年 12 月 20 日

のドキュメントを更新しました Trusted Advisor	Trusted Advisor に 4 つの新しいチェックが追加されましたAWS Well-Architected • コスト最適化に関する AWS Well-Architected のリスクの高い問題 • パフォーマンスに関する AWS Well-Architected のリスクの高い問題 • セキュリティに関する AWS Well-Architected のリスクの高い問題 • 信頼性に関する AWS Well-Architected のリスクの高い問題 詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。	2021 年 12 月 20 日
更新版	Enterprise On-Ramp Support プランをお持ちの場合は、すべての Trusted Advisor チェックと AWS サポート API にアクセスできます。	2021 年 11 月 24 日
のドキュメントを更新しました Trusted Advisor	Trusted Advisor はAmazon Comprehend の 2 つの新しいチェックを追加しました。詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。	2021 年 9 月 29 日

のドキュメントを更新しました Trusted Advisor	Amazon OpenSearch Service Reserved Instance Optimization のチェック名が更新されました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2021 年 9 月 8 日
Trusted Advisor チェックのドキュメントを更新しました	すべての Trusted Advisor チェックのリファレンストピックを追加しました。詳細については、AWS Trusted Advisor チェックリファレンスを参照してください。	2021 年 9 月 1 日
Trusted Advisor 管理ポリシーのドキュメントを更新しました	Trusted Advisor 管理ポリシーのドキュメントを更新しました。詳細については、「AWSAWS サポート およびの マネージドポリシー AWS Trusted Advisor」を参照してください。	2021 年 8 月 10 日
のドキュメントを更新しました Trusted Advisor	Trusted Advisor コンソールのドキュメントを更新しました。詳細については、「 の開始方法 AWS Trusted Advisor」を参照してください。	2021年7月16日

サポート ケース作成に関するドキュメントの更新	完全に終了したケースに関連するサポートケースを作成する方法に関するドキュメントが追加されました。詳細については、「解決済みのケースを再開する」および「関連ケースの作成」を参照してください。	2021 年 6 月 8 日
のドキュメントを更新しました Trusted Advisor	Trusted Advisor は、Amazon Elastic Block Store (Amazon EBS) ボリュームストレージの 2 つの新しいチェックを追加しました。詳細については、AWS Trusted Advisor「チェックの変更ログ」を参照してください。	2021 年 6 月 8 日
更新版	以下のトピックが更新されました。 • AWS Trusted Advisor「メトリクスをモニタリングするための Amazon CloudWatch アラームの作成」トピックの手順を更新し、内容を追加しました。 • AWS サポート API の Service Quotas セクションを追加しました。	2021 年 5 月 12 日

以前の更新

変更	説明	日付
のドキュメントを更新しました Trusted Advisor	チェック結果のフィルター、更新、およびダウンロードに関するドキュメントが追加されました。詳細については、次のセクションを参照してください。 • チェックのフィルター • チェック結果の更新 • 結果のダウンロード	2021 年 3 月 16 日
AWS 管理ポリシーに関するドキュメントを更新しました	AWSSupportServiceRolePolicy AWS 管理ポリシーに関する情報を追加しました。詳細については、「AWS サポート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。	2021 年 3 月 16 日
のチェックを追加 AWS Lambda	に Lambda の 4 つの AWS Trusted Advisor チェックを追加しましたの変更ログ AWS Trusted Advisor。	2021 年 3 月 8 日
Amazon Elastic Block Store の更新されたサービスの制限チェック	の Amazon EBS の 5 つの AWS Trusted Advisor チェックを更新しましたの変更ログ AWS Trusted Advisor。	2021 年 3 月 5 日
CloudTrail ログに関するドキュメントの更新	CloudTrail は、 AWS サポート プラン変更時のコンソールアクションのログをサポートします。詳細については、「サポート プランへの変更のログ記録」を参照してください。	2021 年 2 月 9 日
のドキュメントを更新しました Trusted Advisor	「Trusted Advisor Recommendations の開始方法」トピックが更新されました。	2021 年 1 月 29 日

変更	説明	日付
Trusted Advisor レポートのドキュメントを更新しました	他の AWS サービスで Trusted Advisor レポートを使用するためのトラブルシューティングセクションを追加しました。	2020 年 12 月 4 日
AWS CloudTrail ログ記録 AWS Trusted Advisor のサポートを追加	CloudTrail は、 Trusted Advisor コンソールアクションのサブセットのログ記録をサポートしています。詳細については、「を使用した AWS Trusted Advisor コンソールアクションのログ記録 AWS CloudTrail」を参照してください。	2020 年 11 月 23 日
変更ログのトピックの追加	の AWS Trusted Advisor チェックとカテゴリの変更を表示しますの変更ログ AWS Trusted Advisor。	2020 年 11 月 18 日
組織単位のサポートの追加	組織単位 (OUs) の Trusted Advisor チェックのレポートを作成できるようになりました。詳細については、「組織ビューレポートを作成する」を参照してください。	2020 年 11 月 17 日
AWS CloudTrail トピックでログ記録を更新	Trusted Advisor API オペレーションのログエントリの例を追加しました。「AWS Trusted Advisor CloudTrail ログ記録の情報」を参照してください。	2020 年 10 月 22 日
AWS サポート クォータの追加	サポートの現在のクォータと制限に関する情報が追加されました。「AWS 全般のリファレンス」の「サポート エンドポイントとクォータ」を参照してください。	2020 年 8 月 4 日
の組織ビュー AWS Trusted Advisor	の一部であるアカウントの Trusted Advisor チェックのレポートを作成できるようになりました AWS Organizations。「の組織ビュー AWS Trusted Advisor」を参照してください。	2020 年 7 月 17 日

変更	説明	日付
セキュリティと AWS サポート	AWS サポート と Trusted Advisor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更新しました。「のセキュリティ AWS サポート」を参照してください。	2020 年 5 月 5 日
セキュリティと AWS サポート	AWS サポート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。	2020 年 1 月 10 日
ウェブサービス Trusted Advisor としての の使用	Trusted Advisor チェックのリストを取得した後に Trusted Advisor データを更新する手順を更新しました。	2018 年 11 月 1 日
サービスにリンクされたロールの使用	新しいセクションを追加。	2018 年 7 月 11 日
はじめに: トラブルシューティング	Route 53 と AWS Certificate Managerのトラブルシューティングリンクが追加されました。	2017 年 9 月 1 日
ケース管理の例: ケースの作成	Basic Support プランユーザーのための CC ボックスに関する注記を追加。	2017 年 8 月 1 日
CloudWatch Events による Trusted Advisor チェック結果のモニタリング	新しいセクションを追加。	2016 年 11 月 18 日
ケース管理	ケース重大度レベルの名前を更新。	2016 年 10 月 27 日
を使用した AWS サポート 通話のログ記録 AWS CloudTrail	新しいセクションを追加。	2016 年 4 月 21 日
はじめに: トラブルシューティング	さらにトラブルシューティングリンクを追加。	2015 年 5 月 19 日
はじめに: トラブルシューティング	さらにトラブルシューティングリンクを追加。	2014 年 11 月 18 日

変更	説明	日付
はじめに: ケース管理	AWS Management Consoleで Service Catalog を反映するように更新。	2014 年 10 月 30 日
AWS サポート ケースの有効期間のプログラミング	ケースの履歴取得時に、ケースに添付ファイルを追加したり、ケース通信を省略するための、新しい API 要素に関する情報を追加。	2014 年 7 月 16 日
アクセス AWS サポート	アクセス方法として、指定サポート担当者を削除。	2014 年 5 月 28 日
概要	「はじめに」セクションを追加。	2013 年 12 月 13 日
初版発行	新しい AWS サポート サービスがリリースされました。	2013 年 4 月 30 日

AWS 用語集

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

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