Leitfaden

AWS Support

API-Version 2013-04-15

AWS Support: Leitfaden

Table of Contents

Erste Schritte mit AWS Support

AWS Support bietet eine Reihe von Plänen, die Zugriff auf Tools und Fachwissen bieten, die den Erfolg und die Funktionsfähigkeit Ihrer AWS Lösungen unterstützen. Alle Supportpläne bieten rund um die Uhr Zugriff auf Kundenservice, AWS Dokumentation, technische Dokumente und Support-Foren. Wenn Sie technischen Support und weitere Ressourcen für die Planung, Bereitstellung und Verbesserung Ihrer AWS Umgebung benötigen, können Sie einen Supportplan für Ihren AWS Anwendungsfall wählen.

Hinweise

- Informationen zum Erstellen eines Support-Falls in der AWS Management Console finden Sie unterErstellen eines Support-Falls.
- Weitere Informationen zu den verschiedenen AWS Support Plänen finden Sie unter AWS Support Tarife vergleichen undAWS Support Pläne ändern.
- Supportpläne bieten unterschiedliche Reaktionszeiten für Ihre Supportfälle. Siehe Auswahl eines Schweregrads und Reaktionszeiten.

Themen

Erstellung von Supportfällen und Fallmanagement

In der AWS Management Console können Sie drei Arten von Kundenfällen erstellen in AWS Support:

- Konto- und Rechnungs-Support-Fälle stehen allen AWS -Kunden zur Verfügung. Sie erhalten Hilfe bei Fragen zur Rechnungsstellung und zum Konto.

- Service-Limit-Erhöhungs-Anfragen stehen allen AWS -Kunden zur Verfügung. Weitere Informationen über die Standard-Service-Quotas, die früher als Limits bezeichnet wurden, finden Sie unter AWS -Service-Quotas in der Allgemeine AWS-Referenz.
- Technische Support-Fälle verbinden Sie für Hilfe bei servicebezogenen technischen Problemen und in einigen Fällen bei Anwendungen von Drittanbietern mit dem technischen Support. Wenn Sie Basic Support haben, können Sie keinen technischen Supportfall erstellen.

> Hinweise
>
> - Wie Sie Ihren Support-Plan ändern können, erfahren Sie unter AWS Support Pläne ändern.
> - Wie Sie Ihr Konto schließen können, erfahren Sie im AWS Billing Benutzerhandbuch unter Schließen eines Kontos.
> - Allgemeine Themen zur Problembehandlung für AWS-Services finden Sie unterRessourcen zur Fehlerbehebung.
> - Wenn Sie Kunde eines That sind AWS Partner , der Teil von ist AWS Partner Network, und den Resold Support nutzen, wenden Sie sich bei Fragen zur Abrechnung AWS Partner direkt an Sie. AWS Support kann Ihnen bei nicht technischen Problemen mit dem Resold Support nicht weiterhelfen, z. B. bei der Abrechnung und Kontoverwaltung. Weitere Informationen finden Sie unter den folgenden Themen:
>   - Wie AWS Partner die AWS Support Tarife in einer Organisation festlegen können
>   - AWS Partner-geführter Support

Erstellen eines Support-Falls

Sie können einen Supportfall im Support Center des AWS Management Console.

> Hinweise
>
> - Sie können sich als Root-Benutzer Ihres AWS Kontos oder als AWS Identity and Access Management (IAM-) Benutzer im Support Center anmelden. Weitere Informationen finden Sie unter Zugriff auf das AWS Support Center verwalten.

- Wenn Sie sich nicht im Support Center anmelden und einen Supportfall erstellen können, können Sie stattdessen die Seite Kontakt verwenden. Auf dieser Seite erhalten Sie Hilfe bei Fragen zur Rechnungsstellung und zum Konto.

So erstellen Sie einen Support-Fall

1. Melden Sie sich an der AWS Support Center Console an.

   > **Tip**
   >
   > In der AWS Management Console können Sie auch das Fragezeichensymbol ( ) und dann Support Center auswählen.

2. Wählen Sie Create case (Fall erstellen) aus.
3. Wählen Sie eine der folgenden Optionen:

   - Konto und Abrechnung
   - Technisch
   - Für Erhöhungen der Service Quota gehen Sie zu Sie wünschen eine Erhöhung des Servicelimits? und folgen anschließend den Anweisungen für Erstellen einer höheren Service Quota.

4. Wählen Sie den Service, die Kategorie und den Schweregrad aus.

   > **Tip**
   >
   > Sie können die empfohlenen Lösungen verwenden, die für häufig gestellte Fragen angezeigt werden.

5. Klicken Sie auf Next step (Nächster Schritt): Additional information (Zusätzliche Informationen)
6. Geben Sie auf der Seite Additional Information (Zusätzliche Informationen) für Subject (Betreff) einen Titel zu Ihrem Problem ein.
7. Befolgen Sie für Description (Beschreibung) die Anweisungen und beschreiben Sie Ihren Fall etwa wie folgt:

   - Fehlermeldungen, die Sie erhalten haben

- Von Ihnen befolgte Schritte zur Fehlerbehebung
- Wie Sie auf den Dienst zugreifen:
  - AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - API-Operationen

8. (Optional) Wählen Sie Attach files (Dateien anhängen), um Ihrem Fall relevante Dateien hinzuzufügen, z. B. Fehlerprotokolle oder Screenshots. Sie können bis zu 3 Dateien anfügen. Jede Datei kann bis zu 5 MB groß sein.
9. Klicken Sie auf Next step: Solve now or contact us (()Nächster Schritt): Jetzt lösen oder Support kontaktieren).
10. Wählen Sie auf der Seite Contact us (Kontakt) Ihre bevorzugte Sprache aus.
11. Wählen Sie Ihre bevorzugte Kontaktmethode. Sie können eine der folgenden Optionen wählen:

    a. Web: Erhalten Sie eine Antwort im Support-Center.

    b. Chat: Starten Sie einen Live-Chat mit einem Kundendienstmitarbeiter. Wenn Sie keine Verbindung zu einem Chat herstellen können, finden Sie weitere Informationen unter Fehlerbehebung.

    c. Phone (Telefon) – Erhalten Sie einen Anruf von einem Support-Agenten. Wenn Sie diese Option auswählen, geben Sie die folgenden Informationen ein:

       - Land oder Region
       - Phone number (Telefonnummer)
       - (Optional) Verlängerung

    > **Hinweise**
    >
    > - Die Kontaktoptionen hängen von der Art des Falls und Ihrem Support-Plan ab.
    > - Sie können Discard draft (Entwurf verwerfen) auswählen, um Ihren Support-Fallentwurf zu löschen.

12. (Optional) Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Support-Plan haben, sehen Sie die Option Additional Contacts (Weitere Kontakte). Sie können die E-Mail-Adressen der Personen eingeben, die benachrichtigt werden sollen, wenn sich der Status des Falls ändert. Wenn Sie als IAM-Benutzer angemeldet sind, schließen Sie Ihre E-Mail-Adresse mit

ein. Wenn Sie mit der E-Mail-Adresse und dem Passwort Ihres Stammkontos angemeldet sind, müssen Sie Ihre E-Mail-Adresse nicht mit einschließen.

> **Note**
>
> Beim Support-Plan „Basic“ ist das Feld Additional Contacts (Zusätzliche Kontakte) nicht verfügbar. Der im Abschnitt Alternate Contact (Stellvertretende Kontakte) auf der Seite My Account (Mein Konto) angegebene Kontakt für Operations (Operationen) erhält jedoch Kopien der Fallkorrespondenz, jedoch nur für die spezifischen Fallarten Konto und Abrechnung sowie Technik.

13. Überprüfen Sie Ihre Falldetails und wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

Beschreiben Ihres Problems

Die Beschreibung sollte so detailliert wie möglich sein. Schließen Sie relevante Ressourceninformationen zusammen mit allen weiteren Daten ein, die uns bei Ihrem Problem von Nutzen sein können. Für die Fehlersuche bei der Leistung sind beispielsweise Zeitstempel und Protokolle nützlich. Für Anforderungen von Funktionen oder allgemeine Anleitungsfragen, schließen Sie eine Beschreibung der Umgebung und des Zwecks mit ein. Befolgen Sie in allen Fällen die Description Guidance (Beschreibungsanleitung), welche in Ihrem Einreichformular des Falls erscheint.

Wenn Sie so viele Details wie möglich angeben, erhöhen Sie die Chancen, dass Ihr Fall schnell behoben werden kann.

Auswahl eines Schweregrads

Möglicherweise neigen Sie dazu, stets einen Supportfall mit dem höchsten Schweregrad zu erstellen, den Ihr Supportplan zulässt. Sie sollten die höchsten Schweregrade jedoch für Probleme auswählen, die nicht umgangen werden können oder sich direkt auf Produktionsanwendungen auswirken. Weitere Informationen dazu, wie Sie Ihre Services so erstellen, dass sich der Verlust einzelner Ressourcen nicht auf Ihre Anwendung auswirkt, finden Sie im technischem Papier zum Thema Entwicklung fehlertoleranter Anwendungen in AWS.

In der folgenden Tabelle werden Schweregrade, Reaktionszeiten und Beispielprobleme aufgeführt.

Hinweise

- Sie können den Schweregradcode für einen Supportfall nach der Erstellung nicht mehr ändern. Wenn sich Ihre Situation ändert, wenden Sie sich an den AWS Support Agenten für Ihren Support-Fall.
- Weitere Informationen zum Schweregrad finden Sie unter AWS Support -API-Referenz.

Schweregrad	Code für Schweregrad	Erstreaktionszeit	Beschreibung und Supportplan
General guidance (Allgemeine Anleitung)	`low`	24 Stunden	Sie haben eine allgemeine Entwicklungsfrage oder möchten eine Funktion anfordern. (*Entwickler-, Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan)
System impaired (System beeinträchtigt)	`normal`	12 Stunden	Nicht kritische Funktionen Ihrer Anwendung verhalten sich ungewöhnlich oder Sie haben eine dringende Entwicklungsfrage. (*Entwickler-, Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan)
Production system impaired (Produktionssystem beeinträchtigt)	`high`	4 Stunden	Wichtige Funktionen Ihrer Anwendung sind beeinträchtigt oder eingeschränkt. (Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan)
Production system down (Produktionssystem nicht mehr funktionsfähig)	`urgent`	1 Stunde	Ihr Geschäft wird erheblich beeinträchtigt. Wichtige Funktionen Ihrer Anwendung sind nicht verfügbar. (Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan)
Business-critical system down (Geschäftskritisches	`critical`	15 Minuten	Ihr Geschäft ist gefährdet. Kritische Funktionen Ihrer Anwendung sind nicht verfügbar (Enterprise-Supportplan). Beim Enterprise-On-Ramp-Supportplan sind es 30 Minuten.

Schweregrad	Code für Schweregrad	Erstreaktionszeit	Beschreibung und Supportplan
System nicht mehr funktionsfähig)			

Reaktionszeiten

Wir unternehmen alle erforderlichen Anstrengungen, um Ihre erste Anfrage innerhalb des angegebenen Zeitrahmens zu beantworten. Informationen zum Umfang des Supports für die einzelnen AWS Support Pläne finden Sie unter AWS Support Funktionen.

Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie rund um die Uhr technischen Support erhalten. *Für den "Developer"-Support werden Antwortziele für Supportfälle zu Geschäftszeiten berechnet. Geschäftszeiten sind im Allgemeinen als die Zeit von 08:00 bis 18:00 Uhr im Land des Kunden definiert, ausgenommen Feiertage und Wochenenden. Diese Zeiten können in Ländern mit mehreren Zeitzonen variieren. Diese Informationen über das Land des Kunden werden im Abschnitt Contact Information (Kontaktinformationen) auf der Seite My Account (Mein Konto) in der AWS Management Console angezeigt.

> **Note**
>
> Wenn Sie Japanisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Japanisch möglicherweise wie folgt verfügbar:
>
> - Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen oder wenn Sie einen Developer-Supportplan haben und technischen Support benötigen, steht Ihnen der Support auf Japanisch während der Geschäftszeiten in Japan zur Verfügung: 09:00 bis 18:00 Uhr japanische Standardzeit (GMT+9), außer an Feiertagen und Wochenenden.
> - Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Japanisch abrufen.
>
> Wenn Sie Chinesisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Chinesisch möglicherweise wie folgt verfügbar:

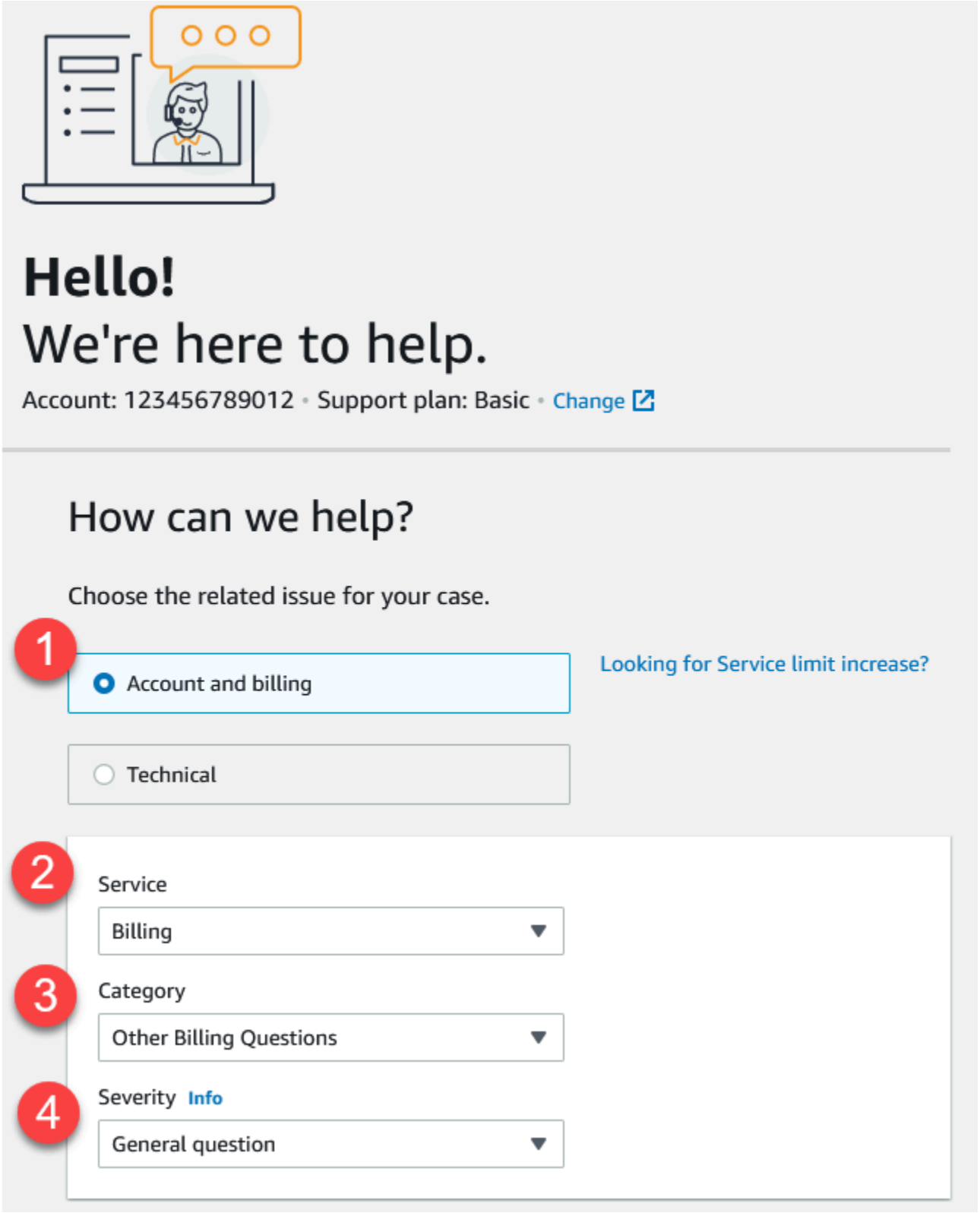
- Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen, steht Ihnen der Support auf Chinesisch von 09:00 bis 18:00 Uhr (GMT+8) zur Verfügung, ausgenommen an Feiertagen und Wochenenden.
- Wenn Sie einen Developer-Supportplan haben, steht Ihnen der technische Support auf Chinesisch während der Geschäftszeiten zur Verfügung, die als 8:00 bis 18:00 Uhr in Ihrem Land definiert sind, wie in Mein Konto eingestellt, ausgenommen Feiertage und Wochenenden. Diese Zeiten variieren möglicherweise in Ländern mit mehreren Zeitzonen.
- Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Chinesisch abrufen.

Wenn Sie Koreanisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Koreanisch möglicherweise wie folgt verfügbar:

- Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen, steht Ihnen der Support auf Koreanisch während der Geschäftszeiten in Korea von 09:00 bis 18:00 Uhr koreanischer Standardzeit (GMT+9) zur Verfügung, ausgenommen Feiertage und Wochenenden.
- Wenn Sie einen Developer-Supportplan haben, steht Ihnen der technische Support auf Koreanisch während der Geschäftszeiten zur Verfügung, die als 8:00 bis 18:00 Uhr in Ihrem Land definiert sind, wie in Mein Konto eingestellt, ausgenommen Feiertage und Wochenenden. Diese Zeiten variieren möglicherweise in Ländern mit mehreren Zeitzonen.
- Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Koreanisch abrufen.

Beispiel: Erstellen eines Support-Falls für Konto und Abrechnung

Das folgende Beispiel ist ein Supportfall für ein Abrechnungs- und Kontoproblem.



1. Create case (Fall erstellen): Wählen Sie den zu erstellenden Falltyp aus. In diesem Beispiel lautet der Falltyp Account and Billing (Konto und Abrechnung).

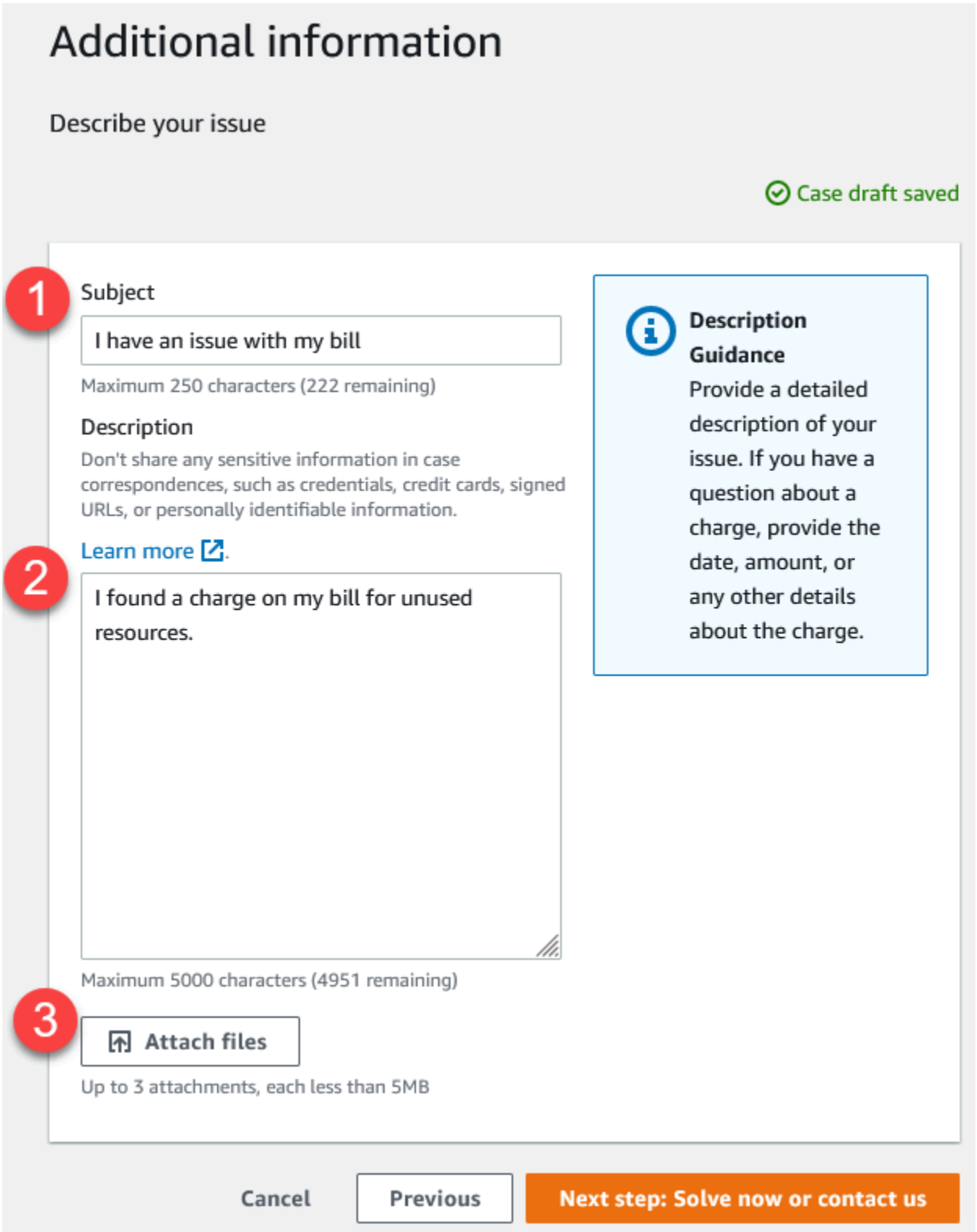
> **Note**
>
> Wenn Sie den Basis-Supportplan haben, können Sie keinen technischen Supportfall erstellen.

2. Service – Wenn sich Ihre Frage auf mehrere Services bezieht, wählen Sie den Service, der am ehesten zutrifft.
3. Category (Kategorie) – Wählen Sie die Kategorie aus, die diesem Anwendungsfall am besten entspricht. Wenn Sie eine Kategorie auswählen, werden Links zu Informationen, die Ihr Problem beheben könnten, unten angezeigt.
4. Severity (Schweregrad) –Kunden mit einem kostenpflichtigen Support-Plan können den Schweregrad General guidance (Allgemeine Anleitung) (Reaktionszeit von einem Tag) oder System impaired (System beeinträchtigt) (Reaktionszeit von 12 Stunden) auswählen. Kunden mit einem Support-Plan "Business" können auch Produktionssystem beeinträchtigt (Reaktionszeit von 4 Stunden) oder Produktionssystem ausgefallen (Reaktionszeit von einer Stunde) auswählen. Kunden mit einem Enterprise-On-Ramp- oder Enterprise-Supportplan können Business-critical system down (Geschäftskritisches System nicht mehr funktionsfähig) auswählen (Reaktionszeit von 15 Minuten für Enterprise-Support und 30 Minuten für Enterprise On-Ramp).

   Die Reaktionszeiten gelten für die erste Reaktion von AWS Support. Diese Reaktionszeiten gelten nicht für nachfolgende Reaktionen. Für Drittanbieter-Probleme können die Reaktionszeiten, je nach Verfügbarkeit des Fachpersonals, länger sein. Weitere Informationen finden Sie unter Auswahl eines Schweregrads.

   > **Note**
   >
   > Je nach Ihrer Kategorieauswahl werden Sie möglicherweise zur Eingabe weiterer Informationen aufgefordert.

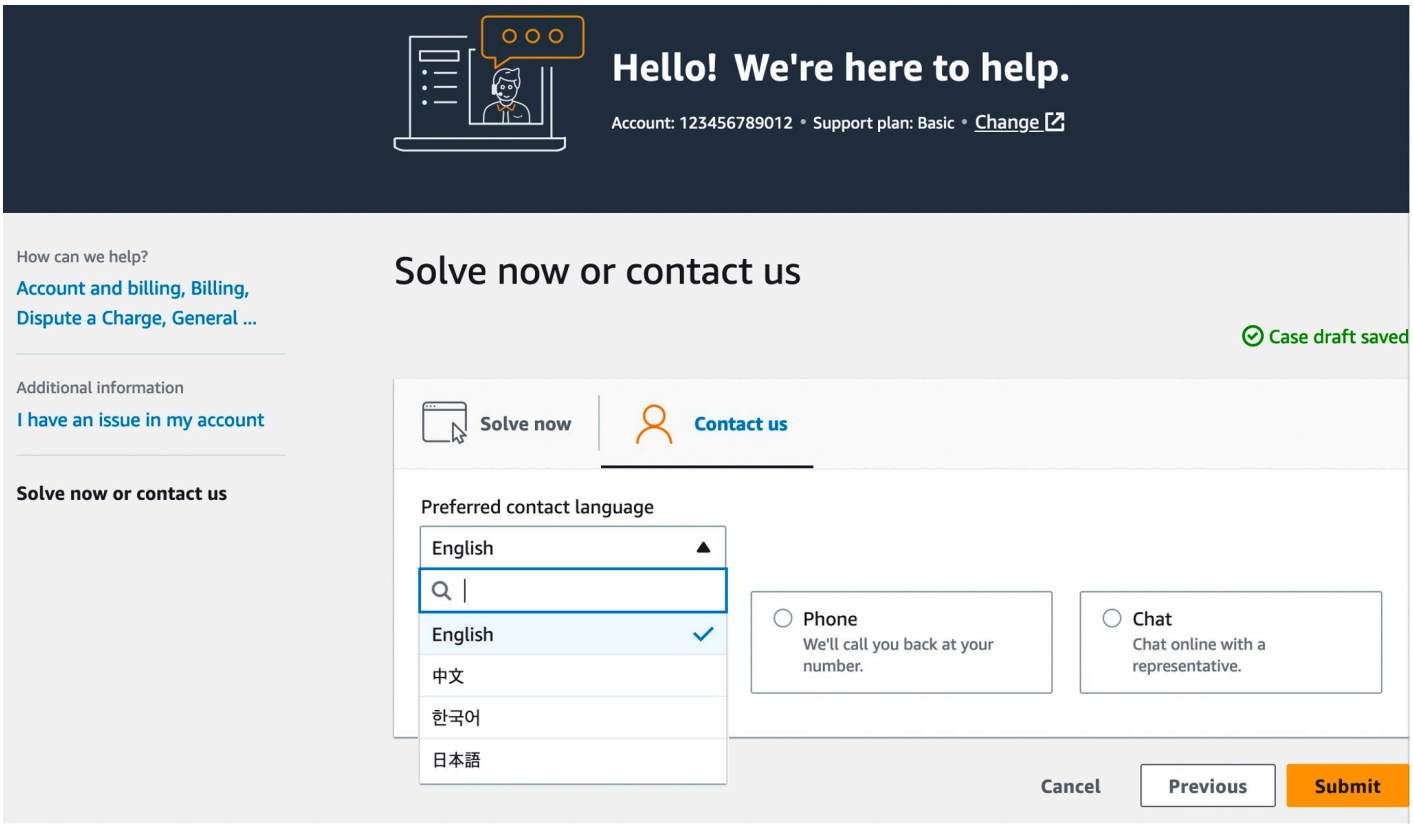
Nachdem Sie den Falltyp und die Klassifizierung angegeben haben, können Sie die Beschreibung und die Art der Kontaktaufnahme angeben.



1. Betreff – Geben Sie einen Titel ein, der Ihr Problem kurz beschreibt.

2. Description (Beschreibung) – Beschreiben Sie den Supportfall. Hierbei handelt es sich um die wichtigsten Informationen, die Sie dem AWS Support bereitstellen. Für einige Service- und Kategoriekombinationen wird eine Ansage mit zugehörigen Informationen angezeigt. Verwenden Sie diese Links, um Ihr Problem zu lösen. Weitere Informationen finden Sie unter Beschreiben Ihres Problems.
3. Attachments (Anhänge) – Hängen Sie Screenshots und andere Anhänge an, um Support-Mitarbeitern zu helfen, Ihren Fall schneller zu lösen. Sie können bis zu 3 Dateien anfügen. Jede Datei kann bis zu 5 MB groß sein.

Nachdem Sie Ihre Falldetails hinzugefügt haben, können Sie auswählen, wie Sie kontaktiert werden möchten.



1. Bevorzugte Kontaktsprache – Wählen Sie Ihre bevorzugte Sprache aus. Derzeit können Sie zwischen Chinesisch, Englisch, Japanisch und Koreanisch wählen. Die individuellen Kontaktoptionen in Ihrer bevorzugten Sprache werden in Ihrem Supportplan angezeigt.
2. Wählen Sie eine Kontaktmethode aus. Die Kontaktoptionen hängen von der Art des Falls und Ihrem Support-Plan ab.

- Wenn Sie Web auswählen, können Sie den Fortschritt des Falls im Support Center lesen und beantworten.
- Klicken Sie auf Chat (Chat) oder Phone (Telefon). Wenn Sie Telefon auswählen, werden Sie aufgefordert, eine Rückrufnummer anzugeben.

3. Klicken Sie auf die Schaltfläche Submit (Absenden), wenn Ihre Informationen vollständig und Sie bereit sind, den Fall zu erstellen.

> **Note**
>
> Wenn Sie Japanisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Japanisch möglicherweise wie folgt verfügbar:
>
> - Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen oder wenn Sie einen Developer-Supportplan haben und technischen Support benötigen, steht Ihnen der Support auf Japanisch während der Geschäftszeiten in Japan zur Verfügung: 09:00 bis 18:00 Uhr japanische Standardzeit (GMT+9), außer an Feiertagen und Wochenenden.
> - Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Japanisch abrufen.
>
> Wenn Sie Chinesisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Chinesisch möglicherweise wie folgt verfügbar:
>
> - Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen, steht Ihnen der Support auf Chinesisch von 09:00 bis 18:00 Uhr (GMT+8) zur Verfügung, ausgenommen an Feiertagen und Wochenenden.
> - Wenn Sie einen Developer-Supportplan haben, steht Ihnen der technische Support auf Chinesisch während der Geschäftszeiten zur Verfügung, die als 8:00 bis 18:00 Uhr in Ihrem Land definiert sind, wie in Mein Konto eingestellt, ausgenommen Feiertage und Wochenenden. Diese Zeiten variieren möglicherweise in Ländern mit mehreren Zeitzonen.
> - Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Chinesisch abrufen.
>
> Wenn Sie Koreanisch als Ihre bevorzugte Kontaktsprache für Supportfälle wählen, ist der Support auf Koreanisch möglicherweise wie folgt verfügbar:

- Wenn Sie den Kundenservice für nicht-technische Supportfälle benötigen, steht Ihnen der Support auf Koreanisch während der Geschäftszeiten in Korea von 09:00 bis 18:00 Uhr koreanischer Standardzeit (GMT+9) zur Verfügung, ausgenommen Feiertage und Wochenenden.
- Wenn Sie einen Developer-Supportplan haben, steht Ihnen der technische Support auf Koreanisch während der Geschäftszeiten zur Verfügung, die als 8:00 bis 18:00 Uhr in Ihrem Land definiert sind, wie in Mein Konto eingestellt, ausgenommen Feiertage und Wochenenden. Diese Zeiten variieren möglicherweise in Ländern mit mehreren Zeitzonen.
- Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie den technischen Support rund um die Uhr auf Koreanisch abrufen.

Fehlerbehebung

Wenn Sie bei beim Erstellen oder Verwalten Ihrer Supportfälle Schwierigkeiten haben, erhalten Sie in den folgenden Informationen zur Problembehandlung Unterstützung.

Ich möchte erneut einen Live-Chat für meinen Fall öffnen.

Wenn Sie auf Ihren vorhandenen Supportfall antworten, öffnet sich ein weiteres Chatfenster. Weitere Informationen finden Sie unter Aktualisieren eines vorhandenen Supportfalls.

Ich kann keine Verbindung zu einem Live-Chat herstellen.

Wenn Sie die Chat-Option ausgewählt haben, aber keine Verbindung zum Chatfenster herstellen können, müssen Sie die folgenden Überprüfungen durchführen:

- Stellen Sie sicher, dass Sie Ihren Browser so konfiguriert haben, dass Popupfenster im Support-Center zugelassen werden.

  > **Note**
  >
  > Überprüfen Sie die Einstellungen für Ihren Browser. Weitere Informationen finden Sie auf den Hilfeseiten für Chrome und Firefox.

- Vergewissern Sie sich, dass Sie Ihr Netzwerk so konfiguriert haben, dass Sie AWS Support nutzen können:

- Ihr Netzwerk kann auf den `*.connect.us-east-1.amazonaws.com`-Endpunkt zugreifen.

  > **Note**
  >
  > Für AWS GovCloud (US) ist der Endpunkt `*.connect-fips.us-east-1.amazonaws.com`.

- Ihre Firewall unterstützt WebSocket-Verbindungen.

Wenn Sie immer noch keine Verbindung zum Chatfenster herstellen können, wenden Sie sich per E-Mail oder Telefon an den AWS Support.

Erstellen einer höheren Service Quota

Fordern Sie höhere Service Quotas (früher als Limits bezeichnet) an, um die Leistung Ihres Services zu verbessern.

> **Note**
>
> Sie können Service Quotas auch verwenden, um Erhöhungen direkt für Ihre Services anzufordern. Derzeit unterstützen Service Quotas keine Service Quotas für alle Services. Weitere Informationen zu Service Quotas finden Sie unter Was sind Service Quotas? im Benutzerhandbuch für Service Quotas.

Erstellen Sie einen Supportfall zur Erhöhung der Service Quota wie folgt:

1. Melden Sie sich an der AWS Support Center Console an.

   > **Tip**
   >
   > In der AWS Management Console können Sie auch das Fragezeichen-Symbol ( ) und dann Support Center auswählen.

2. Wählen Sie Create case (Fall erstellen) aus.
3. Klicken Sie auf Sie wünschen eine Erhöhung des Servicelimits?

4. Folgen Sie den Anweisungen, um eine Erhöhung anzufordern. Die möglichen Optionen umfassen Folgendes:

   - Einschränkungstyp
   - Schweregrad

   > **Note**
   >
   > Je nach Ihrer Kategorieauswahl fordern die Eingabeaufforderungen möglicherweise weitere Informationen an.

5. Wählen Sie für Requests (Anforderungen) die Region aus.
6. Wählen Sie für Limit (Limit) die Art des Service-Limits aus.
7. Geben Sie unter New limit value (Neuer Grenzwert) den gewünschten Wert ein.
8. (Optional) Um eine weitere Erhöhung anzufordern, wählen Sie Add another request (Weitere Anforderung hinzufügen) aus.
9. Beschreiben Sie bei Case Description (Fallbeschreibung) den Supportfall.
10. Wählen Sie bei Contact Options (Kontaktoptionen) die bevorzugte Sprache und wie Sie kontaktiert werden möchten. Sie können eine der folgenden Optionen wählen:

    - Web: Erhalten Sie eine Antwort im Support-Center.
    - Chat: Starten Sie einen Live-Chat mit einem Kundendienstmitarbeiter. Wenn Sie keine Verbindung zu einem Chat herstellen können, finden Sie weitere Informationen unter Fehlerbehebung.
    - Phone (Telefon) – Erhalten Sie einen Anruf von einem Support-Agenten. Wenn Sie diese Option auswählen, geben Sie die folgenden Informationen ein:
      - Land/Region
      - Phone number (Telefonnummer)
      - (Optional) Verlängerung
11. Wählen Sie Submit (Absenden) aus. Ihre Fall-ID-Nummer und Übersicht werden angezeigt.

Aktualisierung, Lösung und Wiederaufnahme Ihres Falls

Nachdem Sie Ihren Supportfall erstellt haben, können Sie den Status Ihres Falles im Support Center verfolgen. Ein neuer Fall beginnt in dem Status Nicht zugeordnet. Wenn ein Supportagent mit der

Arbeit an einem Fall beginnt, ändert sich der Status in In Bearbeitung. Der Supportagent kann auf Ihren Fall antworten, um weitere Informationen anzufordern (Pending Customer Action) oder um Ihnen mitzuteilen, dass der Fall untersucht wird (Pending Amazon Action).

Wenn Ihr Fall aktualisiert wird, erhalten Sie eine E-Mail mit der Korrespondenz und einem Link zu dem Fall im Support Center. Verwenden Sie den Link in der E-Mail-Nachricht, um zum Support-Fall zu navigieren. Sie können auf Fallkorrespondenz nicht per E-Mail antworten.

Hinweise

- Sie müssen sich bei dem AWS-Konto anmelden, von dem der Supportfall übermittelt wurde. Wenn Sie sich als AWS Identity and Access Management (IAM-)Benutzer anmelden, müssen Sie über die erforderlichen Berechtigungen verfügen, um Supportfälle anzuzeigen. Weitere Informationen finden Sie unter Zugriff auf das AWS Support Center verwalten.
- Wenn Sie nicht innerhalb von ein paar Tagen auf den Fall reagieren, löst AWS Support den Fall automatisch auf.
- Supportfälle, die sich länger als 14 Tage im Status "gelöst" befinden, können nicht wieder geöffnet werden. Wenn Sie ein ähnliches Problem haben, das mit dem gelösten Fall zusammenhängt, können Sie einen verwandten Fall erstellen. Weitere Informationen finden Sie unter Erstellen eines Bezugsfalls.

Themen

Aktualisieren eines vorhandenen Supportfalls

Sie können Ihren Fall aktualisieren, um weitere Informationen für den Kundendienstmitarbeiter bereitzustellen. Sie haben beispielsweise die Möglichkeit, auf Korrespondenzen zu antworten, einen weiteren Live-Chat zu starten, zusätzliche E-Mail-Empfänger hinzuzufügen usw. Allerdings lässt

sich der Schweregrad eines Falles nicht aktualisieren, nachdem Sie ihn erstellt haben. Weitere Informationen finden Sie unter Auswahl eines Schweregrads.

So aktualisieren Sie einen vorhandenen Supportfall

1. Melden Sie sich an der AWS Support Center Console an.

   > **Tip**
   >
   > In der AWS Management Console können Sie auch das Fragezeichen-Symbol () und dann Support Center auswählen.

2. Wählen Sie unter Open support cases (Offene Supportfälle) die Option Subject (Betreff) für den Supportfall aus.
3. Wählen Sie Reply (Antworten) aus. Im Bereich Correspondence (Korrespondenz) können Sie außerdem die folgenden Änderungen vornehmen:
   - Angeben von Informationen, die der Kundendienstmitarbeiter angefordert hat
   - Hochladen von Dateianlagen
   - Ändern der bevorzugten Kontaktmethode
   - Hinzufügen von E-Mail-Adressen, um Fallaktualisierungen zu erhalten
4. Wählen Sie Submit (Absenden) aus.

> **Tip**
>
> Wenn Sie das Chatfenster geschlossen haben und einen weiteren Live-Chat starten möchten, fügen Sie Ihrem Supportfall eine Antwort hinzu. Wählen Sie hierfür Chat und dann Submit (Absenden) aus. Ein neues Popup-Chatfenster wird geöffnet.

Lösung eines Supportfalls

Wenn Sie mit der Antwort zufrieden sind oder Ihr Problem gelöst ist, können Sie den Fall im Support Center auflösen.

So lösen Sie einen Supportfall

1. Melden Sie sich an der AWS Support Center Console an.

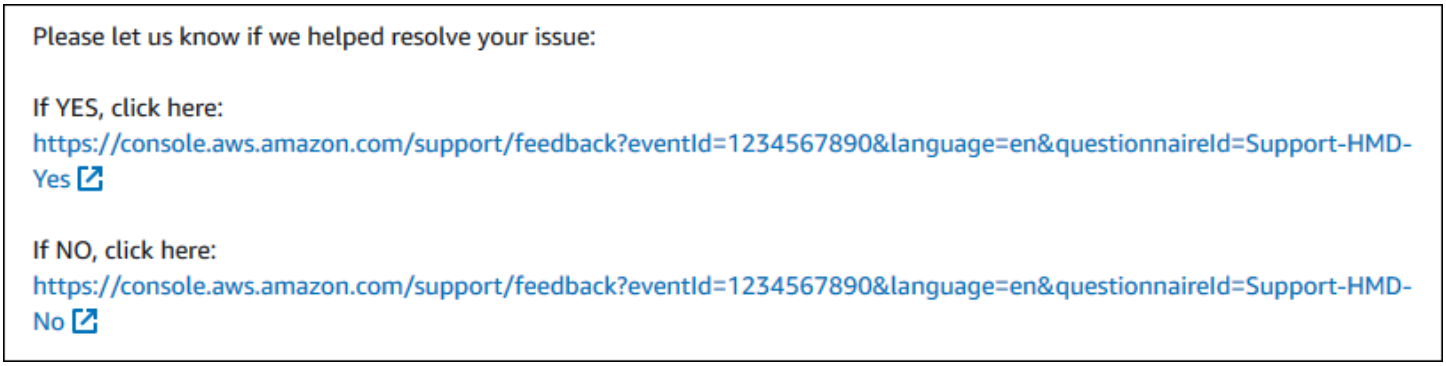
> **Tip**
>
> In der AWS Management Console können Sie auch das Fragezeichen-Symbol ( ) und dann Support Center auswählen.

2. Wählen Sie unter Offene Supportfälle den Betreff des Supportfalls, den Sie lösen möchten.
3. (Optional) Wählen Sie Antworten und geben Sie im Abschnitt Korrespondenz an, warum Sie den Fall lösen, und wählen Sie dann Senden. Sie können z. B. Informationen darüber eingeben, wie Sie das Problem selbst behoben haben, falls Sie diese Informationen in Zukunft benötigen.
4. Wählen Sie Resolve case (Fall lösen).
5. Wählen Sie OK im Dialogfeld, um den Fall zu lösen.

> **Note**
>
> Wenn AWS Support Ihren Fall für Sie gelöst hat, können Sie den Feedback-Link verwenden, um weitere Informationen über Ihre Erfahrungen mit AWS Support zu geben.

Example : Feedback-Links

Der folgende Screenshot zeigt die Feedback-Links in der Korrespondenz eines Falls im Support Center.



Wiederaufnahme eines gelösten Falls

Wenn das gleiche Problem erneut auftritt, können Sie den ursprünglichen Fall erneut öffnen. Geben Sie an, wann das Problem erneut aufgetreten ist und welche Schritte zur Fehlerbehebung Sie unternommen haben. Geben Sie alle zugehörigen Fallnummern an, damit der Support-Mitarbeiter auf frühere Korrespondenz verweisen kann.

> **Hinweise**
>
> - Sie können Ihren Support-Fall bis zu 14 Tage nach der Behebung Ihres Problems erneut öffnen. Allerdings können Sie einen Fall, der länger als 14 Tage inaktiv war, nicht wieder aufnehmen. Sie können einen neuen Fall oder einen verwandten Fall anlegen. Weitere Informationen finden Sie unter Erstellen eines Bezugsfalls.
> - Wenn Sie einen bestehenden Fall wieder öffnen, der andere Informationen als Ihr aktuelles Problem enthält, kann der Support-Mitarbeiter Sie auffordern, einen neuen Fall zu erstellen.

So öffnen Sie einen gelösten Fall wieder

1. Melden Sie sich an der AWS Support Center Console an.

   > **Tip**
   >
   > In der AWS Management Console können Sie auch das Fragezeichen-Symbol () und dann Support Center auswählen.

2. Wählen Sie Alle Fälle anzeigen und wählen Sie dann den Betreff oder die Fall-ID des Supportfalls, den Sie wieder öffnen möchten.
3. Wählen Sie Fall wieder öffnen.
4. Unter Korrespondenz, für Antworten, geben Sie die Falldetails ein.
5. (Optional) Wählen Sie Dateien auswählen, um Dateien an Ihren Fall anzuhängen. Sie können bis zu 3 Dateien anfügen.
6. Wählen Sie für Kontaktmethoden eine der folgenden Optionen:
   - Web – Lassen Sie sich per E-Mail und über das Support Center benachrichtigen.
   - Chat – Chatten Sie online mit einem Support-Mitarbeiter.

- Fon – Erhalten Sie einen Anruf von einem Support-Agenten.

7. (Optional) Geben Sie unter Zusätzliche Kontakte die E-Mail-Adressen anderer Personen ein, die Korrespondenz zu Ihrem Fall erhalten sollen.
8. Überprüfen Sie Ihre Falldetails und wählen Sie Senden.

Erstellen eines Bezugsfalls

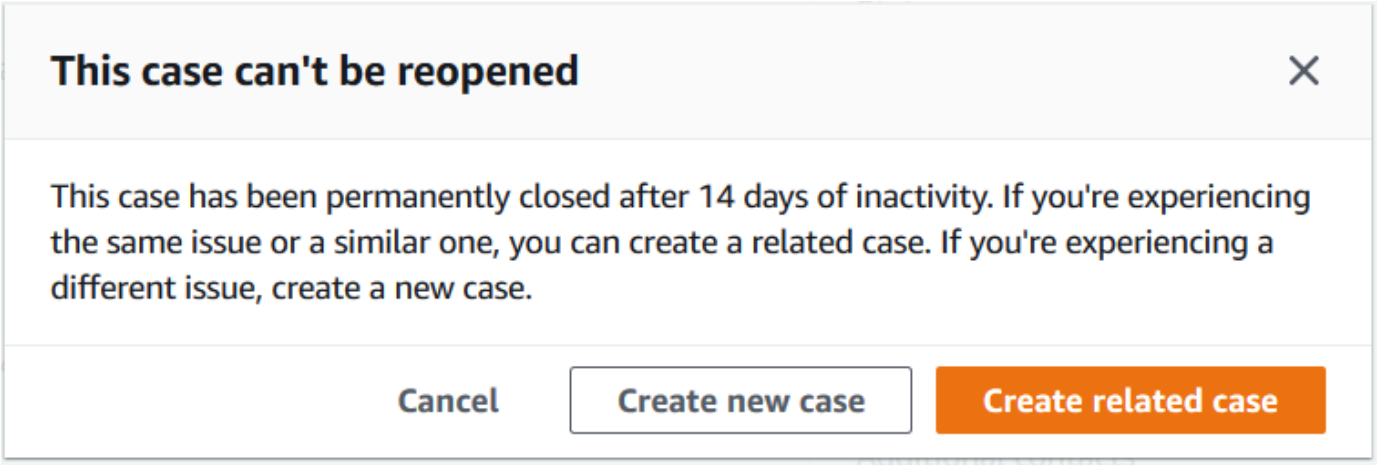
Nach 14 Tagen Inaktivität können Sie einen gelösten Fall nicht wieder öffnen. Wenn Sie ein ähnliches Problem haben, das mit dem gelösten Fall zusammenhängt, können Sie einen verwandten Fall erstellen. Dieser verwandte Fall enthält einen Link zu dem zuvor gelösten Fall, so dass der Support-Agent die früheren Falldetails und die Korrespondenz einsehen kann. Wenn Sie ein anderes Problem haben, empfehlen wir Ihnen, einen neuen Fall zu erstellen.

So erstellen Sie einen verwandten Fall

1. Melden Sie sich an der AWS Support Center Console an.

   > **Tip**
   >
   > In der AWS Management Console können Sie auch das Fragezeichen-Symbol () und dann Support Center auswählen.

2. Wählen Sie Alle Fälle anzeigen und wählen Sie dann den Betreff oder die Fall-ID des Supportfalls, den Sie wieder öffnen möchten.
3. Wählen Sie Fall wieder öffnen.
4. Wählen Sie iVerwandten Fall erstellen im Dialogfeld. Die Informationen des vorherigen Falles werden automatisch dem zugehörigen Fall hinzugefügt. Wenn Sie ein anderes Problem haben, wählen Sie Neuen Fall anlegen.

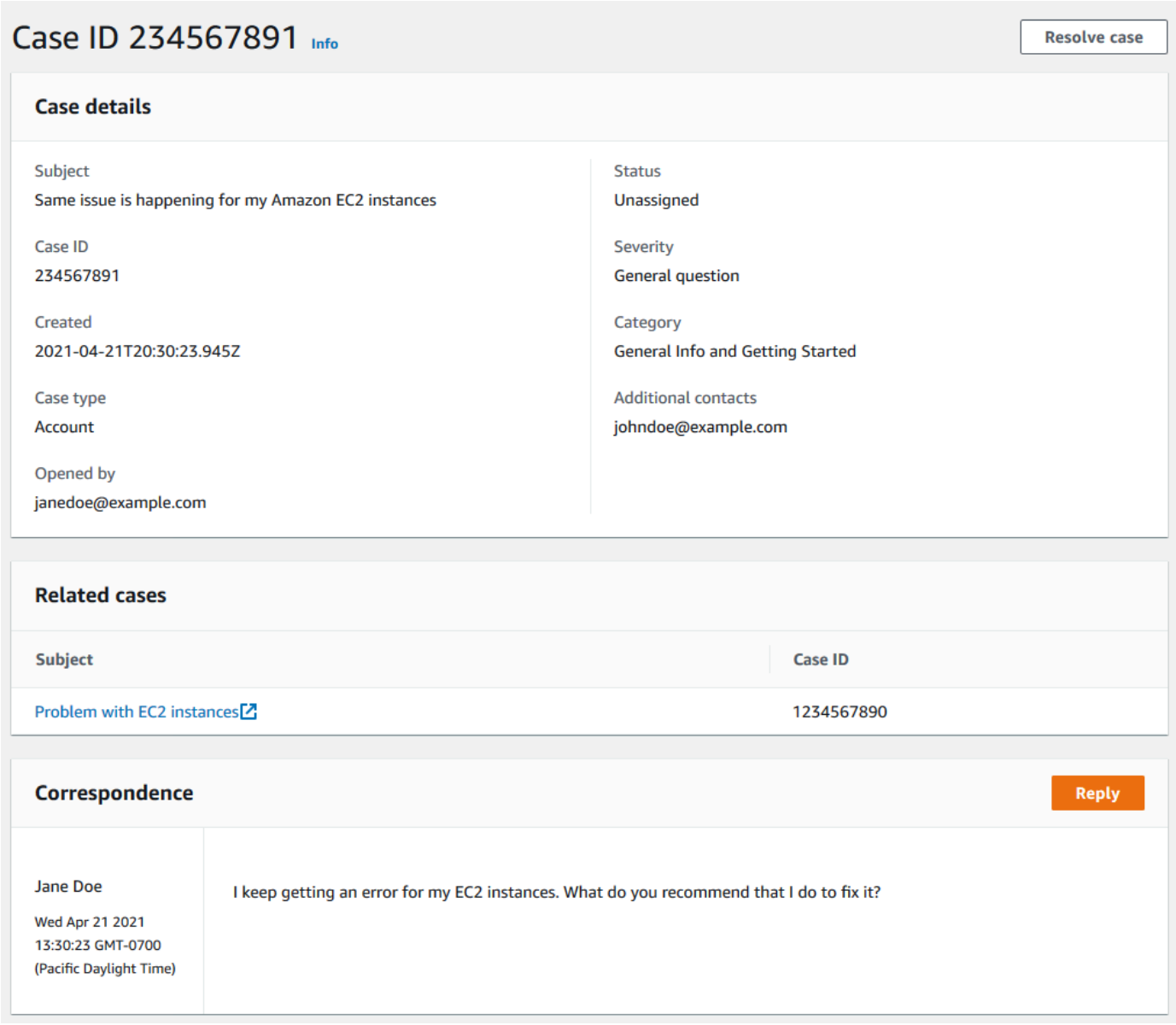


5. Führen Sie die gleichen Schritte aus, um Ihren Fall zu erstellen. Siehe Erstellen eines Support-Falls.

> **Note**
>
> Standardmäßig hat Ihr zugehöriger Fall denselben Typ, dieselbe Kategorie und denselben Schweregrad wie der vorherige Fall. Sie können die Falldetails nach Bedarf aktualisieren.

6. Überprüfen Sie Ihre Falldetails und wählen Sie Senden.

   Nachdem Sie Ihren Fall erstellt haben, erscheint der vorherige Fall im Abschnitt Verwandte Fälle, wie im folgenden Beispiel.



Fallverlauf

Sie können Informationen über den Verlauf eines Falles bis zu 24 Monate nach der Erstellung eines Falles einsehen.

AWS Support Empfehlungen

> **Note**
>
> AWS Support Recommendations wird im Sinne der Servicebedingungen als „ AWS Vorschau-Service“ bereitgestellt. Der Vorschau-Service kann geändert und storniert werden. Weitere Informationen.

AWS Support Recommendations bietet Ihnen personalisierte Unterstützung bei der Problembehebung bei Konto- und technischen Problemen während der Bearbeitung von Kundenvorgängen in der AWS Support Mittelkonsole. AWS Support Recommendations basiert auf den Falldetails und dem angemeldeten Konto, um Ihnen maßgeschneiderte Lösungen zur Lösung Ihres Problems anbieten zu können.

Um Probleme zu analysieren, fragt AWS Support Recommendations Informationen wie AccountID, AWS Ressourcen-IDs oder die Fehlermeldung im Rahmen der genehmigten Richtlinien/ Benutzerberechtigungen ab. Weitere Informationen.

Themen

Zugriff auf AWS Support Empfehlungen verwalten

> **Note**
>
> AWS Support Recommendations wird im Sinne der Servicebedingungen als „ AWS Vorschau-Service“ bereitgestellt. Der Vorschau-Service kann geändert und storniert werden. Weitere Informationen.

Sie können AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf AWS Support Empfehlungen in der AWS Support Center-Konsole während der Erstellung von Kundenvorgängen zu verwalten.

Themen

- AWS Support Empfehlungen und Aktionen.
- Beispiel für IAM-Richtlinien für Empfehlungen AWS Support

AWS Support Empfehlungen und Aktionen.

Sie können in einer IAM-Richtlinie AWS Support Empfehlungsaktionen angeben, um vollen Zugriff zu gewähren, vollständigen Zugriff zu verweigern oder den Zugriff auf bestimmte Aktionen bereitzustellen/zu verweigern.

Aktion	Beschreibung
`StartSupportTroubleshooting`	Initiieren Sie eine geführte Sitzung zur Problembehandlung, um bei der Diagnose und Lösung von Konto- oder technischen Problemen während der Bearbeitung von Kundenvorgängen in der AWS Support Center-Konsole zu helfen.
`GetSupportTroubleshootingResponse`	Ruft den aktuellen Status und die Ausgabe einer Sitzung zur Problembehandlung ab, die mit gestartet wurde StartSupportTroubleshooting. Beinhaltet interaktive Anfragen nach weiteren Informationen und Empfehlungen zur Lösung des Problems auf der Grundlage früherer Antworten.

Beispiel für IAM-Richtlinien für Empfehlungen AWS Support

Sie können die folgenden Beispielrichtlinien verwenden, um den Zugriff auf AWS Support Empfehlungen zu verwalten.

Voller Zugriff auf AWS Support Empfehlungen

Die folgende Richtlinie gewährt Benutzern vollen Zugriff auf AWS Support Empfehlungen.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportrecommendations:StartSupportTroubleshooting",
                "supportrecommendations:GetSupportTroubleshootingResponse"
            ],
            "Resource": "*"
        }
    ]
}
```

Zugriff auf AWS Support Empfehlungen verweigern

Die folgende Richtlinie erlaubt Benutzern keinen Zugriff auf AWS Support Empfehlungen.

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

Überwachung und Protokollierung von AWS Support Empfehlungen

> **Note**
>
> AWS Support Recommendations wird als „Vorschau-Service“ im Sinne der AWS Servicebedingungen bereitgestellt. Der Vorschau-Service kann geändert und storniert werden. Weitere Informationen.

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Support Recommendations und Ihren anderen AWS Lösungen. AWS bietet das folgende Überwachungstool, um AWS Support Empfehlungen zu verfolgen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Themen

AWS Support Recommendations-Anrufe protokollieren mit AWS CloudTrail

> **Note**
>
> AWS Support Recommendations wird im Sinne der Servicebedingungen als „ AWS Vorschau-Service“ bereitgestellt. Der Vorschau-Service kann geändert und storniert werden. Weitere Informationen.

AWS Support Recommendations ist in einen Dienst integriert, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen bereitstellt. AWS CloudTrail CloudTrail erfasst API-Aufrufe für AWS Support Empfehlungen als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Support Center-Konsole und Code-Aufrufe an die AWS Support Empfehlungen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für AWS Support Empfehlungen. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen.

Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an AWS Support Recommendations, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

AWS Support Informationen zu Empfehlungen finden Sie in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn in AWS Support Recommendations unterstützte Ereignisse vorkommen, wird diese Aktivität zusammen mit anderen CloudTrail AWS Serviceereignissen in der Ereignishistorie als Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Support Empfehlungen, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AWS Support Recommendations-Anrufe werden von protokolliert CloudTrail. Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Sie können auch AWS Support Recommendations-Protokolldateien aus mehreren AWS Regionen und mehreren AWS Konten in einem einzigen Amazon S3 S3-Bucket zusammenfassen.

Die Einträge in der AWS Support Recommendations-Protokolldatei verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Sie enthält Informationen über den angeforderten Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Example : Protokolleintrag für **`StartSupportTroubleshooting`**

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für den `StartSupportTroubleshooting` Vorgang.


```
{
    "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 : Protokolleintrag für **`GetSupportTroubleshootingResponse`**

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für den `GetSupportTroubleshootingResponse` Vorgang.


```
{
    "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"
}
```


Verwendung AWS Support mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK for C++	AWS SDK for C++ Code-Beispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK for Go	AWS SDK for Go Code-Beispiele
AWS SDK for Java	AWS SDK for Java Code-Beispiele
AWS SDK for JavaScript	AWS SDK for JavaScript Code-Beispiele
AWS SDK for Kotlin	AWS SDK for Kotlin Code-Beispiele
AWS SDK for .NET	AWS SDK for .NET Code-Beispiele
AWS SDK for PHP	AWS SDK for PHP Code-Beispiele
AWS Tools for PowerShell	Tools für PowerShell Codebeispiele
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) Code-Beispiele
AWS SDK for Ruby	AWS SDK for Ruby Code-Beispiele
AWS SDK for Rust	AWS SDK for Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK for Swift	AWS SDK for Swift Code-Beispiele

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Über die AWS Support-API

Die AWS Support-API bietet Zugriff auf einige der Funktionen des AWSSupport-Centers.

Die API bietet zwei verschiedene Gruppen von Operationen:

- Support-Fallverwaltung Operationen zur Verwaltung des gesamten Lebenszyklus Ihrer AWS Supportfälle, von der Erstellung eines Falls bis zu seiner Lösung
- AWS Trusted Advisor Operationen zur AWS Trusted Advisor Zugangsprüfung

> **Note**
>
> Sie benötigen einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan zur Nutzung der AWS Support-API. Weitere Informationen finden Sie unter AWS Support.

Weitere Informationen zu den Operationen und Datentypen, die von AWS Support bereitgestellt werden, finden Sie in der AWS SupportAPI-Referenz.

Themen

Support-Fallverwaltung

Mit der API können Sie die folgenden Aufgaben durchführen:

- Öffnen eines Support-Falls.
- Abrufen einer Liste und detaillierter Informationen über die letzten Support-Fälle.
- Filtern Sie Ihre Suche nach Support-Fällen durch Daten- und Fall-IDs, einschließlich Fällen, die behoben wurden.

- Hinzufügen der Kommunikations- und Dateianlagen zu Ihren Fällen und Hinzufügen der E-Mail-Empfänger für die Fallkorrespondenz. Sie können bis zu 3 Dateien anfügen. Jede Datei kann bis zu 5 MB groß sein.
- Lösen Ihrer Fälle.

Die AWS Support API unterstützt die CloudTrail Protokollierung für Support-Case-Management-Operationen. Weitere Informationen finden Sie unter Protokollierung von AWS Support-API-Aufrufen mit AWS CloudTrail.

Codebeispiele, die zeigen, wie der gesamte Lebenszyklus eines Support-Falls verwaltet werden kann, finden Sie unter Codebeispiele für AWS Support mithilfe von AWS SDKs.

AWS Trusted Advisor

Mit den Trusted Advisor Vorgängen können Sie die folgenden Aufgaben durchführen.

- Holen Sie sich die Namen und Kennungen für die Trusted Advisor Prüfungen
- Anfordern, dass eine Trusted Advisor-Prüfung für Ihr AWS Konto und Ihre Ressourcen ausgeführt wird.
- Erhalten Sie Zusammenfassungen und detaillierte Informationen zu Ihren Trusted Advisor Prüfungsergebnissen
- Aktualisieren Sie Ihre Trusted Advisor Prüfungen
- Abrufen des Status jeder Trusted Advisor Prüfung

Die AWS Support API unterstützt die CloudTrail Protokollierung von Trusted Advisor Vorgängen. Weitere Informationen finden Sie unter AWS Trusted Advisor-Informationen in der CloudTrail Protokollierung.

Sie können Amazon CloudWatch Events verwenden, um zu überwachen, ob sich Ihre Prüfergebnisse für geändert habenTrusted Advisor. Weitere Informationen finden Sie unter AWS Trusted AdvisorPrüfergebnisse mit Amazon überwachen EventBridge.

Ein Beispiel für Java-Code, der die Verwendung der Trusted Advisor Operationen demonstriert, finden Sie unter Trusted Advisor Als Webservice verwenden.

Endpunkte

AWS Support ist ein globaler Service. Das bedeutet, dass jeder Endpunkt, den Sie verwenden, Ihre Supportfälle in der Support Center Console aktualisiert.

Wenn Sie beispielsweise den USA Ost (Nord-Virginia) verwenden, um einen Fall zu erstellen, können Sie den Endpunkt USA West (Oregon) oder Europa (Irland) oder Europa (Irland) verwenden, um demselben Fall eine Entsprechung hinzuzufügen.

Sie können die folgenden Endpunkte für die AWS Support-API verwenden:

- USA Ost (Nord-Virginia) – https://support.us-east-1.amazonaws.com
- USA West (Oregon) – https://support.us-west-2.amazonaws.com
- Europa (Irland) – https://support.eu-west-1.amazonaws.com

Important

- Wenn Sie den CreateCaseVorgang aufrufen, um Test-Supportfälle zu erstellen, empfehlen wir Ihnen, eine Betreffzeile anzugeben, z. B. TEST CASE-Please ignore. Wenn Sie mit Ihrem Test-Supportfall fertig sind, rufen Sie den ResolveCaseBetrieb an, um das Problem zu lösen.
- Um die AWS Trusted Advisor-Operationen in der AWS Support-API aufzurufen, müssen Sie den Endpunkt USA Ost (Nord-Virginia) verwenden. Derzeit unterstützen die Endpunkte USA West (Oregon) und Europa (Irland) die Trusted Advisor-Operationen nicht.

Weitere Informationen über AWS-Endpunkte finden Sie unter AWS Support-Endpunkte und -Kontingente im Allgemeine Amazon Web Services-Referenz.

Unterstützung inAWS-SDKs

Die AWS Command Line Interface (AWS CLI), und die AWS Software Development Kits (SDKs) enthalten Unterstützung für die AWS Support-API.

Um eine Liste der Sprachen zu erhalten, die die AWS Support API unterstützen, wählen Sie einen Namen für den Vorgang aus CreateCase, z. B., und wählen Sie im Abschnitt Siehe auch Ihre bevorzugte Sprache aus.

AWS Support Pläne

Sie können Ihre AWS Support Pläne für Ihr Konto je nach Ihren Geschäftsanforderungen ändern.

Themen

Merkmale der AWS Support Pläne

AWS Support bietet fünf Supportpläne an:

- Basic
- Developer
- Geschäft
- Enterprise On-Ramp
- Enterprise

Der Basic-Support bietet Unterstützung bei Konto- und Abrechnungsfragen sowie bei der Erhöhung von Servicekontingenten. Die anderen Tarife bieten eine Reihe von Fällen mit technischem Support zu pay-by-the-month Preisen und ohne langfristige Verträge.

Alle AWS Kunden haben automatisch rund um die Uhr Zugriff auf diese Funktionen des Basic Support:

- O ne-on-one Antworten auf Fragen zum Konto und zur Abrechnung
- Support-Foren
- Prüfungen des Servicezustands
- Dokumentation, technische Unterlagen und Leitfäden für bewährte Verfahren

Kunden mit einem Developer Support-Plan haben Zugang zu diesen zusätzlichen Funktionen:

- Anleitungen für bewährte Methoden
- Kundenseitige Diagnose-Tools

- Unterstützung bei der Bausteinarchitektur: Anleitung zur gemeinsamen Nutzung von AWS Produkten, Funktionen und Diensten
- Unterstützt eine unbegrenzte Anzahl von Supportanfragen, die von jedem Benutzer mit entsprechenden Berechtigungen geöffnet werden können.

Zusätzlich haben Kunden mit einem Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan Zugriff auf die folgenden Funktionen:

- Hinweise zu Anwendungsfällen — Welche AWS Produkte, Funktionen und Dienste Sie verwenden sollten, um Ihre spezifischen Anforderungen am besten zu erfüllen.
- AWS Trusted Advisor— Eine Funktion von AWS Support, die Kundenumgebungen untersucht und Möglichkeiten identifiziert, Geld zu sparen, Sicherheitslücken zu schließen und die Zuverlässigkeit und Leistung des Systems zu verbessern. Sie können auf alle Trusted Advisor Schecks zugreifen.
- Die AWS Support API für die Interaktion mit dem Support Center und Trusted Advisor. Sie können die AWS Support -API verwenden, um die Verwaltung von Support-Fällen und Trusted Advisor -Vorgänge zu automatisieren.
- Support für Software anderer Hersteller – Hilfe für Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Betriebssysteme und Konfiguration. Hilft auch bei der Leistung der beliebtesten Softwarekomponenten von Drittanbietern AWS. Support für Software von Drittanbietern ist für Kunden mit Support-Plänen auf Basic- oder Developer-Stufe nicht verfügbar.
- Unterstützt eine unbegrenzte Anzahl von AWS Identity and Access Management (IAM-) Benutzern, die technische Supportfälle eröffnen können.

Zusätzlich haben Kunden mit einem Enterprise-On-Ramp- oder Enterprise-Supportplan Zugriff auf die folgenden Funktionen:

- Anleitung zur Anwendungsarchitektur – Hilfreiche Informationen dazu, wie Services speziell für Ihre Anwendungsfälle, Workloads oder Anwendungen ineinander greifen.
- Infrastructure Event Management – Kurzfristige Interaktion mit AWS Support , um eine fundierte Kenntnis Ihres Anwendungsfalls zu erhalten. Stellen Sie nach der Analyse Architektur- und Skalierungsanleitungen für eine Veranstaltung bereit.
- Technical Account Manager – Arbeiten Sie für Ihre spezifischen Anwendungsfälle und Anwendungen mit einem Technical Account Manager (TAM) zusammen.
- Direkte Fallweiterleitung an speziell geschulte Techniker.
- Geschäftsberichte des Managements.

Weitere Informationen zu den Funktionen und Preisen der einzelnen AWS Support Supportpläne finden Sie unter AWS SupportTarife vergleichen. Einige Funktionen, wie z. B. Telefon- und Chat-Support rund um die Uhr, sind nicht in allen Sprachen verfügbar.

AWS Support Pläne ändern

Sie können die AWS Support Plans-Konsole verwenden, um Ihren Supportplan für Sie zu ändern AWS-Konto. Um Ihren Supportplan zu ändern, müssen Sie über AWS Identity and Access Management (IAM-) Berechtigungen verfügen oder sich als Root-Benutzer bei Ihrem Konto anmelden. Weitere Informationen finden Sie unter Zugriff auf Pläne verwalten AWS Support und AWS verwaltete Richtlinien für AWS Support Pläne.

So ändern Sie Ihren Supportplan

1. Melden Sie sich unter https://console.aws.amazon.com/support/plans/home in der AWS Support Plans-Konsole an.
2. (Optional) Vergleichen Sie auf der Seite AWS Support Plans die Support-Pläne. Weitere Informationen zur Preisgestaltung finden Sie auf der Seite mit den Preisdetails.
3. (Optional) Wählen Sie unter AWS Support pricing example (-Preisbeispiel) die Option See examples (Beispiele anzeigen) und wählen Sie dann eine der Support-Plan-Optionen aus, um die geschätzten Kosten anzuzeigen.
4. Wenn Sie sich für einen Plan entscheiden, wählen Sie Review downgrade (Downgrade prüfen) oder Review upgrade (Upgrade prüfen) für den von Ihnen gewünschten Plan.

   > **Hinweise**
   >
   > - Wenn Sie sich für einen kostenpflichtigen Support-Plan anmelden, müssen Sie mindestens ein einmonatiges Abonnement von AWS Support abschließen. Weitere Informationen finden Sie unter AWS Support – Häufig gestellte Fragen.
   > - Wenn Sie über einen Enterprise On-Ramp- oder Enterprise Support-Plan verfügen, wenden Sie sich im Dialogfeld Change plan confirmation (Plan-Bestätigung ändern) an AWS Support, um Ihren Support-Plan zu ändern.

5. Im Dialogfeld Change plan confirmation (Plan-Bestätigung ändern) können Sie die Support-Elemente erweitern, um die Funktionen anzuzeigen, die Sie zu Ihrem Konto hinzufügen oder entfernen möchten.

Unter Pricing (Preisgestaltung) können Sie die voraussichtlichen einmaligen Gebühren für den neuen Support-Plan anzeigen.

6. Wählen Sie Accept and agree (Akzeptieren und zustimmen).

Ähnliche Informationen

Weitere Informationen zu AWS Support Plänen finden Sie in den AWS Support häufig gestellten Fragen. Sie können auch in der Support-Plans-Konsole Contact us (Kontakt) auswählen.

Wie Sie Ihr Konto schließen können, erfahren Sie im AWS Billing Benutzerhandbuch unter Schließen eines Kontos.

AWS Trusted Advisor

Trusted Advisor stützt sich auf bewährte Methoden, die sich aus der Betreuung von Hunderttausenden von AWS Kunden ergeben haben. Trusted Advisor überprüft Ihre - AWS Umgebung und gibt dann Empfehlungen, wenn sich Möglichkeiten ergeben, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen.

Wenn Sie über einen Basic- oder Developer-Supportplan verfügen, können Sie die Trusted Advisor Konsole verwenden, um auf alle Prüfungen in der Kategorie Service Limits und auf sechs Prüfungen in der Kategorie Sicherheit zuzugreifen.

Wenn Sie über einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan verfügen, können Sie die Trusted Advisor Konsole und die AWS Trusted Advisor API verwenden, um auf alle Trusted Advisor Prüfungen zuzugreifen. Sie können Amazon CloudWatch Events auch verwenden, um den Status von Trusted Advisor Prüfungen zu überwachen. Weitere Informationen finden Sie unter AWS Trusted AdvisorPrüfergebnisse mit Amazon überwachen EventBridge.

Sie können auf Trusted Advisor in der zugreifen AWS Management Console. Weitere Informationen zum Steuern des Zugriffs auf die Trusted Advisor Konsole finden Sie unter Zugriff verwalten auf AWS Trusted Advisor.

Weitere Informationen finden Sie unter Trusted Advisor.

Themen

- Protokoll ändern für AWS Trusted Advisor

Erste Schritte mit Trusted Advisor -Empfehlungen

Sie können die Seite mit den Trusted Advisor Empfehlungen der Trusted Advisor Konsole verwenden, um die Prüfergebnisse für Sie zu überprüfen AWS-Konto und dann die empfohlenen Schritte zur Behebung von Problemen zu befolgen. Zum Beispiel Trusted Advisor könnte er Ihnen empfehlen, ungenutzte Ressourcen zu löschen, um Ihre monatliche Rechnung zu senken, wie z. B. eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance.

Sie können die AWS Trusted Advisor API auch verwenden, um Operationen an Ihren Trusted Advisor Schecks durchzuführen. Weitere Informationen finden Sie in der AWS Trusted Advisor API Reference.

Themen

- Melden Sie sich bei der Trusted Advisor Konsole an
- Ansicht der Prüfungskategorien
- Besondere Prüfungen anzeigen
- Ihre Prüfungen filter
- Ergebnisse der Prüfung aktualisieren
- Herunterladen der Prüfungsergebnisse
- Organisationsansicht
- Präferenzen

Melden Sie sich bei der Trusted Advisor Konsole an

Sie können die Schecks und den Status der einzelnen Schecks in der Trusted Advisor Konsole einsehen.

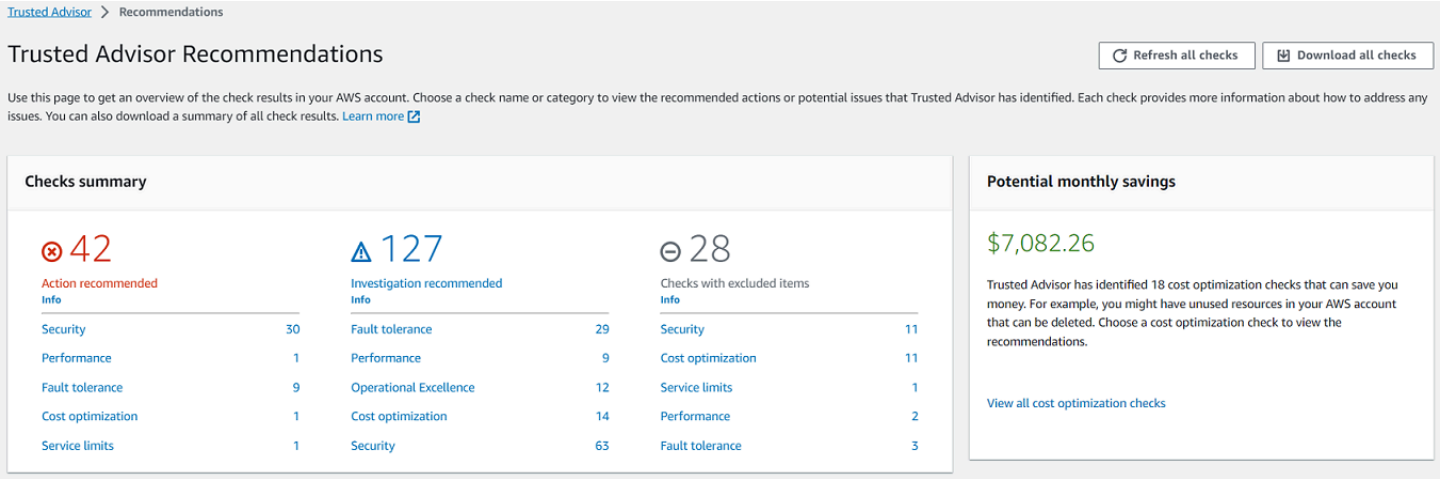
> **Note**
>
> Sie benötigen AWS Identity and Access Management (IAM-) Berechtigungen, um auf die Trusted Advisor Konsole zugreifen zu können. Weitere Informationen finden Sie unter Zugriff verwalten auf AWS Trusted Advisor.

Um sich bei der Trusted Advisor Konsole anzumelden

1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Auf der Trusted Advisor -Empfehlungsseite können Sie die Zusammenfassung für jede Prüfungskategorie einsehen:
   - Aktion empfohlen (rot) — Trusted Advisor empfiehlt eine Aktion für die Prüfung. Eine Prüfung, die ein Sicherheitsproblem für Ihre IAM-Ressourcen feststellt, kann beispielsweise dringende Maßnahmen empfehlen.
   - Empfohlene Untersuchung (Gelb) – Trusted Advisor stellt ein mögliches Problem bei der Prüfung fest. Eine Prüfung, bei der ein Kontingent für eine Ressource erreicht wird, könnte zum Beispiel Empfehlungen zum Löschen ungenutzter Ressourcen geben.
   - Prüfungen mit ausgeschlossenen Elemente (grau) – Die Anzahl der Prüfungen, bei denen Elemente ausgeschlossen wurden, z. B. Ressourcen, die bei einer Prüfung nicht berücksichtigt werden sollen. Dabei kann es sich beispielsweise um Amazon EC2-Instances handeln, die bei der Prüfung nicht berücksichtigt werden sollen.
3. Auf der Seite Trusted Advisor -Empfehlungen können Sie folgende Aktionen ausführen:
   - Um alle Prüfungen in Ihrem Konto zu aktualisieren, wählen Sie Alle Prüfungen aktualisieren.
   - Um eine .xls-Datei zu erstellen, die alle Prüfungsergebnisse enthält, wählen Sie Alle Prüfungen herunterladen.
   - Wählen Sie unter Zusammenfassung der Prüfungen eine Prüfungskategorie, z. B. Sicherheit, um die Ergebnisse anzuzeigen.
   - Unter Potenzielle monatliche Ersparnis können Sie sehen, wie viel Sie für Ihr Konto sparen können, und welche Prüfungen zur Kostenoptimierung empfohlen werden.
   - Unter Letzte Änderungen können Sie die Änderungen der letzten 30 Tage am Status der Prüfungen einsehen. Wählen Sie den Namen einer Prüfung, um die neuesten Ergebnisse für diese Prüfung anzuzeigen, oder wählen Sie das Pfeilsymbol, um die nächste Seite anzuzeigen.

Example : Trusted Advisor Empfehlungen

Das folgende Beispiel zeigt eine Zusammenfassung der Ergebnisse der Prüfung für AWS-Konto.



Ansicht der Prüfungskategorien

Sie können die Prüfungsbeschreibungen und -ergebnisse für die folgenden Prüfungskategorien einsehen:

- Kostenoptimierung – Empfehlungen, mit denen Sie möglicherweise Geld sparen können. Diese Prüfungen zeigen ungenutzte Ressourcen und Möglichkeiten zur Senkung Ihrer Rechnung auf.
- Leistung – Empfehlungen, die die Geschwindigkeit und Reaktionsfähigkeit Ihrer Anwendungen verbessern können.
- Sicherheit — Empfehlungen für Sicherheitseinstellungen, die Ihre AWS Lösung sicherer machen können.
- Fehlertoleranz — Empfehlungen, die dazu beitragen, die Stabilität Ihrer AWS Lösung zu erhöhen. Diese Prüfungen zeigen Redundanzdefizite und überbeanspruchte Ressourcen auf.
- Service-Limits – Prüft die Nutzung Ihres Kontos und ob sich Ihr Konto dem Limit (auch als Kontingent bezeichnet) für AWS -Dienste und -Ressourcen nähert oder es überschreitet.
- Operational Excellence — Empfehlungen, die Ihnen helfen, Ihre AWS Umgebung effektiv und skalierbar zu betreiben.

So zeigen Sie die Prüfungskategorien an

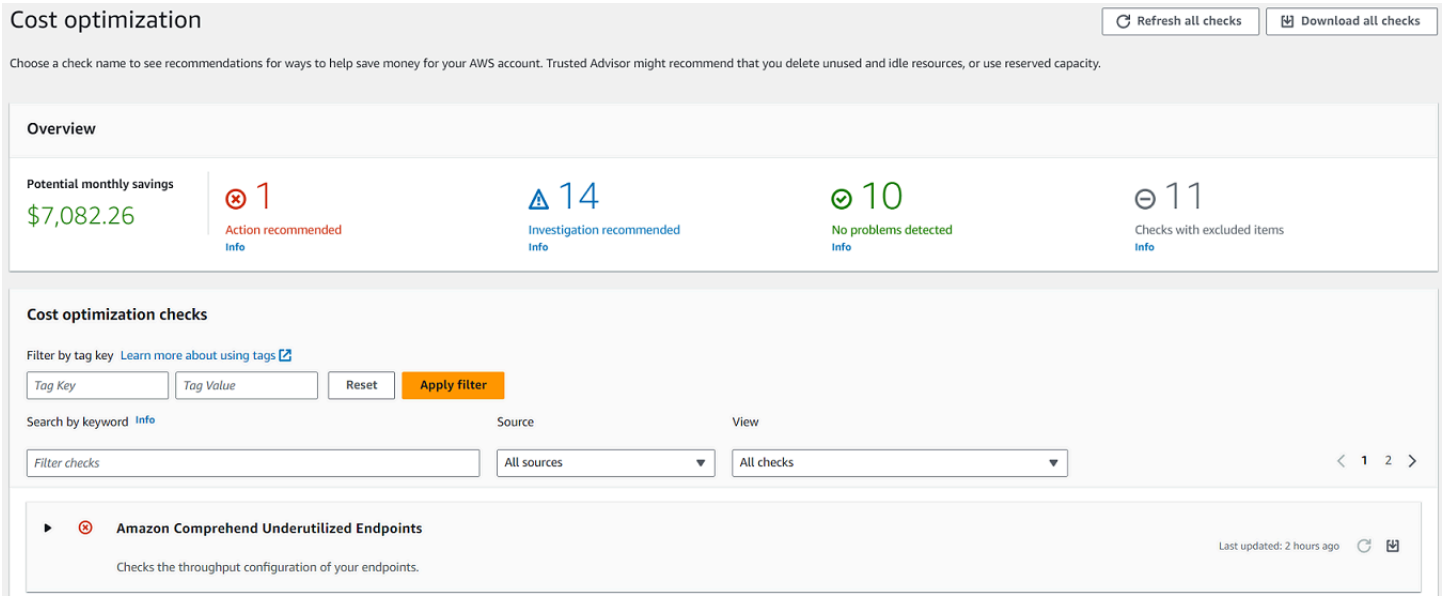
1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Wählen Sie im Navigationsbereich die Kategorie Prüfung.
3. Auf der Kategorieseite können Sie die Zusammenfassung für jede Prüfungskategorie einsehen:

- Aktion empfohlen (rot) — Trusted Advisor empfiehlt eine Aktion für die Prüfung.
- Empfohlene Untersuchung (Gelb) – Trusted Advisor stellt ein mögliches Problem bei der Prüfung fest.
- Keine Probleme erkannt (grün) — Trusted Advisor Es wird kein Problem für die Prüfung erkannt.
- Ausgeschlossene Elemente (Grau) – Die Anzahl der Prüfungen, bei denen Elemente ausgeschlossen wurden, z. B. Ressourcen, die bei einer Prüfung nicht berücksichtigt werden sollen.

4. Wählen Sie für jede Prüfung das Aktualisierungssymbol (), um diese Prüfung zu aktualisieren.
5. Wählen Sie das Download-Symbol (), um eine .xls-Datei zu erstellen, die die Ergebnisse dieser Prüfung enthält.

Example : Kategorie Kostenoptimierung

Das folgende Beispiel zeigt 10 (grüne) Schecks, bei denen es keine Probleme gibt.



Besondere Prüfungen anzeigen

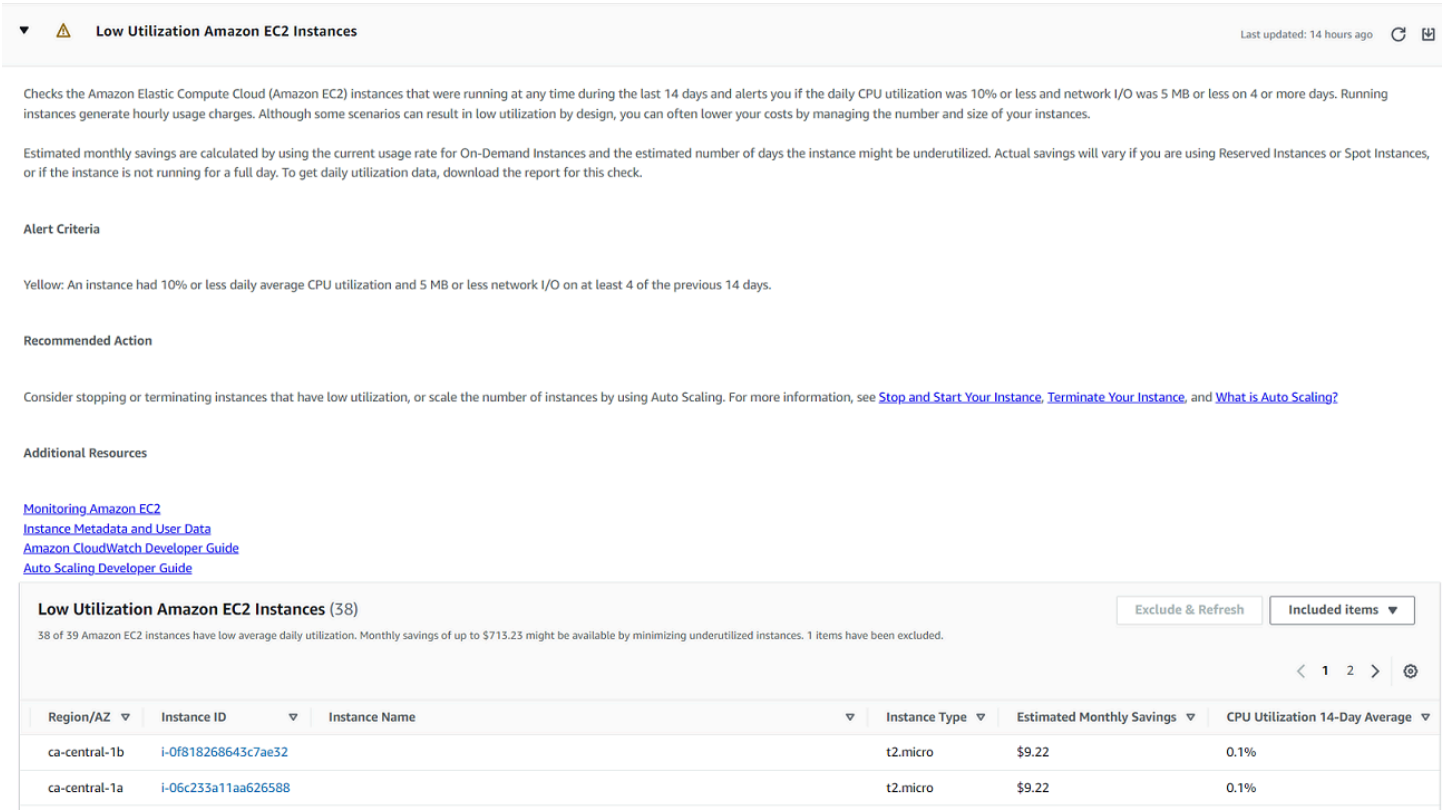
Erweitern Sie eine Prüfung, um die vollständige Prüfungsbeschreibung, die betroffenen Ressourcen, alle empfohlenen Schritte und Links zu weiteren Informationen anzuzeigen.

So zeigen Sie eine bestimmte Prüfung an

1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Wählen Sie im Navigationsbereich eine Prüfungskategorie aus.
3. Wählen Sie den Namen der Prüfung, um die Beschreibung und die folgenden Details anzuzeigen:
   - Alarmkriterien – Beschreibt den Schwellenwert, ab dem eine Prüfung ihren Status ändert.
   - Empfohlene Aktion – Beschreibt die empfohlenen Maßnahmen für diese Prüfung.
   - Weitere Ressourcen – Listet die zugehörige AWS Dokumentation auf.
   - Eine Tabelle, in der die betroffenen Posten in Ihrem Konto aufgeführt sind. Sie können diese Elemente in die Prüfung einbeziehen oder ausschließen.
4. (Optional) Sie können Elemente ausschließen, damit sie nicht in den Prüfungsergebnissen erscheinen:
   a. Markieren Sie einen Artikel und wählen Sie Ausschließen & Aktualisieren.
   b. Um alle ausgeschlossenen Artikel anzuzeigen, wählen Sie Ausgeschlossene Artikel.
5. (Optional) Um Elemente einzuschließen, damit die Prüfung sie erneut auswertet:
   a. Wählen Sie Ausgeschlossene Elemente, markieren Sie ein Element und wählen Sie dann Einschließen & Aktualisieren.
   b. Um alle enthaltenen Elemente anzuzeigen, wählen Sie Enthaltene Elemente.
6. Wählen Sie das Symbol Einstellungen ().
   Im Dialogfeld Präferenzen können Sie die Anzahl der Elemente oder die anzuzeigenden Eigenschaften angeben und dann Bestätigen wählen.

Example : Kostenoptimierungsprüfung

Die folgende Prüfung für Amazon-EC2-Instances mit niedriger Auslastung listet die betroffenen Instances des Kontos auf. Diese Prüfung identifiziert 38 Amazon EC2-Instances mit geringer Auslastung und empfiehlt Ihnen, die Ressourcen zu stoppen oder zu beenden.



Ihre Prüfungen filter

Auf den Seiten der Prüfungskategorien können Sie angeben, welche Prüfergebnisse Sie sehen möchten. Sie können zum Beispiel nach Prüfungen filtern, bei denen Fehler in Ihrem Konto festgestellt wurden, damit Sie dringende Probleme zuerst untersuchen können.

Wenn Sie Schecks haben, mit denen Artikel in Ihrem Konto bewertet werden, z. B. AWS Ressourcen, können Sie Tag-Filter verwenden, um nur Artikel mit dem angegebenen Tag anzuzeigen.

So filtern Sie Ihre Prüfungen

1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Wählen Sie im Navigationsbereich oder auf der Trusted Advisor -Empfehlungsseite die Prüfungskategorie.

3. Für Nach Schlüsselwort suchen ein Schlüsselwort aus dem Schecknamen oder der Beschreibung eingeben, um Ihre Ergebnisse zu filtern.
4. Geben Sie in der Liste View (Ansicht) an, welche Prüfungen angezeigt werden sollen:
   - Alle Prüfungen – Liste aller Prüfungen für diese Kategorie.
   - Empfohlene Aktion – Listen Sie Prüfungen auf, die Ihnen Maßnahmen empfehlen. Diese Prüfungen sind rot hervorgehoben.
   - Empfohlene Untersuchung – Listen Sie die Prüfungen auf, die Ihnen empfehlen, mögliche Maßnahmen zu ergreifen. Diese Prüfungen sind gelb hervorgehoben.
   - Keine Probleme erkannt – Listen Sie Prüfungen auf, bei denen es keine Probleme gibt. Diese Prüfungen sind grün hervorgehoben.
   - Prüfungen mit ausgeschlossenen Elementen – Listen Sie die Prüfungen auf, die Sie angegeben haben, um Elemente von den Prüfungsergebnissen auszuschließen.
5. Wenn Sie Ihren AWS Ressourcen, wie Amazon EC2 EC2-Instances oder AWS CloudTrail Trails, Tags hinzugefügt haben, können Sie Ihre Ergebnisse filtern, sodass bei den Prüfungen nur Elemente angezeigt werden, die das angegebene Tag haben.

   Geben Sie für Filter nach Tag einen Tag-Schlüssel und einen Wert ein, und wählen Sie dann Filter anwenden.
6. In der Tabelle für die Prüfung werden in den Prüfergebnissen nur die Positionen angezeigt, die den angegebenen Schlüssel und Wert haben.
7. Um den Filter nach Tags zu löschen, wählen Sie Zurücksetzen.

Ähnliche Informationen

Weitere Informationen zum Trusted Advisor Markieren von finden Sie in den folgenden Themen:

- AWS Support aktiviert Tagging-Funktionen für Trusted Advisor
- Markieren von AWS -Ressourcen in Allgemeine AWS-Referenz.

Ergebnisse der Prüfung aktualisieren

Sie können die Prüfungen aktualisieren, um die neuesten Ergebnisse für Ihr Konto zu erhalten. Wenn Sie einen Developer- oder Basic Support-Plan haben, können Sie sich bei der Trusted Advisor Konsole anmelden, um die Checks zu aktualisieren. Wenn Sie einen Business-, Enterprise On-

Ramp- oder Enterprise Support-Plan haben, aktualisiert die Schecks in Ihrem Konto Trusted Advisor automatisch wöchentlich.

Um Schecks zu aktualisieren Trusted Advisor

1. Navigieren Sie zur AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.
2. Wählen Sie auf der Seite Trusted Advisor Empfehlungen oder einer Scheckkategorie die Option Alle Checks aktualisieren aus.

Sie können bestimmte Prüfungen auch auf die folgenden Arten auffrischen:

- Wählen Sie das Aktualisierungssymbol
  ( )
  für eine einzelne Prüfung.
- Verwenden Sie die API-Operation RefreshTrustedAdvisorCheck.

> **Hinweise**
>
> - Trusted Advisor aktualisiert einige Prüfungen automatisch mehrmals täglich, z. B. bei Problemen mit AWS Well-Architected hohem Risiko für Zuverlässigkeitsprüfungen. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Für diese automatisch aktualisierten Prüfungen können Sie das Aktualisierungssymbol
>   ( )
>   auswählen, um Ihre Ergebnisse manuell zu aktualisieren.
> - Wenn Sie AWS Security Hub die Option für Ihr Konto aktiviert haben, können Sie die Security Hub-Steuerelemente nicht über die Trusted Advisor Konsole aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie Ihre Security Hub-Ergebnisse.

Herunterladen der Prüfungsergebnisse

Sie können die Prüfergebnisse herunterladen, um sich Trusted Advisor in Ihrem Konto einen Überblick zu verschaffen. Sie können die Ergebnisse für alle Prüfungen oder für eine bestimmte Prüfung herunterladen.

Um Prüfergebnisse aus den Trusted Advisor Empfehlungen herunterzuladen

1. Navigieren Sie zur AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.
   - Um alle Prüfungsergebnisse herunterzuladen, wählen Sie in Trusted Advisor -Empfehlungen oder auf einer Prüfungskategorieseite die Option Alle Prüfungen herunterladen.
   - Um ein Prüfungsergebnis für eine bestimmte Prüfung herunterzuladen, wählen Sie den Namen der Prüfung aus und klicken Sie dann auf das Download-Symbol ( )
2. Speichern oder öffnen Sie die .xls-Datei. Die Datei enthält dieselben zusammenfassenden Informationen wie die Trusted Advisor Konsole, z. B. den Namen der Prüfung, die Beschreibung, den Status, die betroffenen Ressourcen und so weiter.

Organisationsansicht

Sie können die Funktion zur Ansicht der Organisation einrichten, um einen Bericht für alle Mitgliedskonten in Ihrer AWS Organisation zu erstellen. Weitere Informationen finden Sie unter Organisationsansicht für AWS Trusted Advisor.

Präferenzen

Auf der Seite Trusted Advisor verwalten können Sie Trusted Advisor deaktivieren.

Auf der Seite Notifications (Benachrichtigungen)können Sie Ihre wöchentlichen E-Mail-Nachrichten für die Prüfzusammenfassung konfigurieren. Siehe Einrichten von Benachrichtigungseinstellungen.

Auf der Seite Ihre Organisation können Sie den vertrauenswürdigen Zugriff mit aktivieren oder deaktivieren AWS Organizations. Dies ist für das Feature Organisationsansicht für AWS Trusted Advisor, Trusted Advisor Priority und Trusted Advisor Engage erforderlich.

Einrichten von Benachrichtigungseinstellungen

Geben Sie an, wer die wöchentlichen Trusted Advisor E-Mail-Nachrichten mit den Prüfergebnissen erhalten kann und in welcher Sprache. Sie erhalten einmal pro Woche eine E-Mail-Benachrichtigung über die Zusammenfassung Ihrer Schecks für Trusted Advisor Empfehlungen.

Die E-Mail-Benachrichtigungen für Trusted Advisor Empfehlungen enthalten keine Ergebnisse für Trusted Advisor Priority. Weitere Informationen finden Sie unter Verwalten von Benachrichtigungen der Trusted Advisor-Priorität.

So richten Sie Benachrichtigungseinstellungen ein

1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Notifications (Benachrichtigungen).
3. Für Empfehlungen, wählen Sie aus, wer über Ihre Prüfungsergebnisse benachrichtigt werden soll. Sie können Kontakte auf der Seite mit den Kontoeinstellungen in der AWS Billing and Cost Management Konsole hinzufügen und entfernen.
4. Wählen Sie unter Language (Sprache) die Sprache für die E-Mail-Nachricht aus.
5. Wählen Sie Save your preferences (Ihre Präferenzen speichern) aus.

Organisationssicht einrichten

Wenn Sie Ihr Konto mit einrichten AWS Organizations, können Sie Berichte für alle Mitgliedskonten in Ihrer Organisation erstellen. Weitere Informationen finden Sie unter Organisationsansicht für AWS Trusted Advisor.

Deaktivieren Trusted Advisor

Wenn Sie diesen Dienst deaktivieren, Trusted Advisor wird Ihr Konto nicht überprüft. Jeder, der versucht, auf die Trusted Advisor Konsole zuzugreifen oder die API-Operationen zu verwenden, erhält die Fehlermeldung „Zugriff verweigert“.

Um zu deaktivieren Trusted Advisor

1. Melden Sie sich unter https://console.aws.amazon.com/trustedadvisor/home bei der Trusted Advisor Konsole an.
2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Manage Trusted Advisor (verwalten) aus.
3. Deaktivieren Sie unter Trusted Advisor die Option Enabled (Aktiviert). Diese Aktion ist Trusted Advisor für alle Schecks in Ihrem Konto deaktiviert.
4. Anschließend können Sie die AWSServiceRoleForTrustedAdvisor Trusted Advisor manuell aus Ihrem Konto löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle für Trusted Advisor.

Ähnliche Informationen

Weitere Informationen zu Trusted Advisor finden Sie in den folgenden Themen:

- Wie fange ich an zu verwenden Trusted Advisor?
- AWS Trusted Advisor Referenz überprüfen

Erste Schritte mit der Trusted Advisor API

Die AWS Trusted Advisor API-Referenz richtet sich an Programmierer, die detaillierte Informationen zu den Trusted Advisor API-Vorgängen und Datentypen benötigen. Diese API bietet Zugriff auf Trusted Advisor Empfehlungen für Ihr Konto oder alle Konten innerhalb Ihrer AWS Organisation. Die Trusted Advisor API verwendet HTTP-Methoden, die Ergebnisse im JSON-Format zurückgeben.

> **Note**
>
> - Sie müssen über einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan verfügen, um die Trusted Advisor API nutzen zu können
> - Wenn Sie die AWS Trusted Advisor API von einem Konto aus aufrufen, für das es keinen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan gibt, erhalten Sie die Ausnahme „Zugriff verweigert“. Weitere Informationen zur Änderung Ihres Supportplans finden Sie unter AWS Support.

Sie können die AWS Trusted Advisor API verwenden, um eine Liste mit Prüfungen und deren Beschreibungen, Empfehlungen und Ressourcen für Empfehlungen abzurufen. Sie können auch den Lebenszyklus von Empfehlungen aktualisieren. Verwenden Sie die folgenden API-Operationen, um Empfehlungen zu verwalten:

- Verwenden Sie die ListRecommendationResourcesAPI-Operationen ListChecksListRecommendationsGetRecommendation,, und, um Empfehlungen und die entsprechenden Konten und Ressourcen anzuzeigen.
- Verwenden Sie den UpdateRecommendationLifecycleAPI-Vorgang, um den Lebenszyklus einer Empfehlung zu aktualisieren, die von Trusted Advisor Priority verwaltet wird.
- Verwenden Sie den BatchUpdateRecommendationResourceExclusionAPI-Vorgang, um eine oder mehrere Ressourcen in Ihre Trusted Advisor Ergebnisse ein- oder auszuschließen.

- Die UpdateOrganizationRecommendationLifecycleAPI-Aufrufe ListOrganizationRecommendationsGetOrganizationRecommendationListOrganizationRecommendationRe ListOrganizationRecommendationAccounts, und unterstützen nur Empfehlungen, die von Trusted Advisor Priority verwaltet werden. Diese Empfehlungen werden auch als priorisierte Empfehlungen bezeichnet. Sie können Ihre priorisierten Empfehlungen von einem Verwaltungs- oder delegierten Administratorkonto aus anzeigen und verwalten, wenn Sie Trusted Advisor Priority aktiviert haben. Wenn Priority nicht aktiviert ist, erhalten Sie bei Anfragen die Ausnahme „Zugriff verweigert“.

Weitere Informationen finden Sie AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

Informationen zur Authentifizierung von Anfragen finden Sie im Signaturprozess für Signature Version 4.

Trusted Advisor Als Webservice verwenden

> **Note**
>
> Trusted Advisor Operationen werden 2024 nicht von der AWS Trusted Advisor Support-API unterstützt. Bitte verwenden Sie die neue AWS Trusted Advisor API, um programmgesteuert auf bewährte Verfahren und Empfehlungen zuzugreifen.

Der AWS Support Dienst ermöglicht es Ihnen, Anwendungen zu schreiben, die interagieren mit. AWS Trusted Advisor In diesem Thema erfahren Sie, wie Sie eine Liste von Trusted Advisor Prüfungen abrufen, eine davon aktualisieren und anschließend die detaillierten Ergebnisse der Prüfung abrufen. Diese Aufgaben werden in Java dargestellt. Weitere Informationen zum Support für andere Sprachen finden Sie unter Tools für Amazon Web Services.

Themen

Rufen Sie die Liste der verfügbaren Trusted Advisor Prüfungen ab

Der folgende Java-Codeausschnitt erstellt eine Instanz eines AWS Support Clients, mit der Sie alle Trusted Advisor API-Operationen aufrufen können. Als Nächstes ruft der Code die Liste der Trusted Advisor Prüfungen und ihrer entsprechenden `CheckId` Werte ab, indem er die DescribeTrustedAdvisorChecksAPI-Operation aufruft. Anhand dieser Informationen können Sie Benutzeroberflächen erstellen, mit denen Benutzer die Prüfung auswählen können, die sie ausführen oder aktualisieren möchten.

```
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());
    }
}
```

Aktualisieren Sie die Liste der verfügbaren Trusted Advisor Prüfungen

Der folgende Java-Codeausschnitt erstellt eine Instanz eines AWS Support Clients, den Sie zum Aktualisieren Trusted Advisor von Daten verwenden können.

```
// 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());
}
```

Fragen Trusted Advisor Sie nach Statusänderungen ab

Nachdem Sie die Anfrage zur Ausführung einer Trusted Advisor Prüfung zur Generierung der neuesten Statusdaten eingereicht haben, verwenden Sie den DescribeTrustedAdvisorCheckRefreshStatusesAPI-Vorgang, um den Status der Ausführung der Prüfung und die Verfügbarkeit neuer Daten für die Prüfung abzufragen.

Der folgende Java-Codeausschnitt ruft den Status der angeforderten Prüfung in dem folgenden Abschnitt ab, indem er den Wert verwendet, welcher der `CheckId`-Variable entspricht. Darüber hinaus demonstriert der Code mehrere andere Verwendungsmöglichkeiten des Trusted Advisor Dienstes:

1. Sie können `getMillisUntilNextRefreshable` aufrufen, indem Sie Objekte, die in der `DescribeTrustedAdvisorCheckRefreshStatusesResult`-Instance enthalten sind, durchlaufen. Sie können den zurückgegebenen Wert verwenden, um zu testen, ob der Code mit der Aktualisierung der Prüfung fortgesetzt werden soll.
2. Wenn `timeUntilRefreshable` null entspricht, können Sie eine Aktualisierung der Prüfung anfordern.
3. Durch die Verwendung des zurückgegebenen Status können Sie weiterhin Statusänderungen abrufen. Der Codeausschnitt legt das Abrufintervall auf empfohlene zehn Sekunden fest. Wenn der Status entweder `enqueued` oder `in_progress` ist, kehrt die Schleife zurück und fordert einen anderen Status an. Wenn der Aufruf `successful` zurückgibt, wird die Schleife beendet.
4. Schließlich gibt der Code eine Instance eines `DescribeTrustedAdvisorCheckResultResult`-Datentyps zurück, den Sie verwenden können, um die Informationen der Prüfung zu durchlaufen.

Hinweis: Verwenden Sie eine einzelne Aktualisierungsanforderung, bevor Sie den Status der Anforderung abfragen.

```
// 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.
}
```

Fordern Sie ein Trusted Advisor Prüfergebnis an

Nachdem Sie die Prüfung für die gewünschten detaillierten Ergebnisse ausgewählt haben, reichen Sie mithilfe der DescribeTrustedAdvisorCheckResult API-Operation eine Anfrage ein.

> **Tip**
>
> Die Namen und Beschreibungen der Trusted Advisor Prüfungen können sich ändern. Wir empfehlen Ihnen, die Prüfungs-ID in Ihrem Code anzugeben, um eine Prüfung eindeutig zu identifizieren. Sie können die DescribeTrustedAdvisorChecksAPI-Operation verwenden, um die Scheck-ID abzurufen.

Der folgende Java-Codeausschnitt verwendet die `DescribeTrustedAdvisorChecksResult`-Instance, auf welche die Variable `result` verweist, die im vorhergehenden Codeausschnitt erhalten wurde. Nachdem Sie die Anforderung zum Ausführen des Ausschnitts gesendet haben, sendet der Ausschnitt, anstatt eine Prüfung interaktiv über eine Benutzeroberfläche zu definieren, eine Anforderung für die erste Prüfung in der Liste, die ausgeführt werden soll. Dabei wird in jedem `result.getChecks().get(0)`-Aufruf als Indexwert 0 angegeben. Als Nächstes definiert der Code eine Instance von `DescribeTrustedAdvisorCheckResultRequest`, die er an eine Instance von `DescribeTrustedAdvisorCheckResultResult` mit dem Namen `checkResult` weiterleitet. Sie können die Mitgliedsstrukturen dieses Datentyps verwenden, um die Ergebnisse der Prüfung anzuzeigen.

```
// 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();
}
```

Hinweis: Beim Anfordern eines Trusted Advisor Prüfergebnisses werden keine aktualisierten Ergebnisdaten generiert.

Details eines Trusted Advisor Schecks anzeigen

Der folgende Java-Codeausschnitt wiederholt die `DescribeTrustedAdvisorCheckResultResult` Instanz, die im vorherigen Abschnitt zurückgegeben wurde, um eine Liste der Ressourcen zu erhalten, die durch die Prüfung gekennzeichnet wurden. Trusted Advisor

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

Organisationsansicht für AWS Trusted Advisor

In der Organisationsansicht können Sie die Trusted Advisor Prüfungen für alle Konten in Ihrem AWS Organizations ansehen. Nachdem Sie diese Funktion aktiviert haben, können Sie Berichte erstellen, um die Ergebnisse der Prüfungen für alle Mitgliedskonten in Ihrer Organisation zusammenzufassen. Der Bericht enthält eine Zusammenfassung der Prüfungsergebnisse und Informationen über die betroffenen Ressourcen für jedes Konto. Mit den Berichten können Sie zum Beispiel feststellen, welche Konten in Ihrer Organisation AWS Identity and Access Management (IAM) mit der Prüfung

"IAM-Nutzung" verwenden oder ob Sie mit der Prüfung "Amazon S3 Bucket Permissions" empfohlene Aktionen für Amazon-Simple-Storage-Service(Amazon S3)-Buckets haben.

Themen

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, um die Organisationssicht zu aktivieren:

- Ihre Konten müssen Mitglieder einer AWSOrganisation sein.
- Ihre Organization muss alle Funktionen für Organizations aktiviert haben. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.
- Das Management-Konto in Ihrer Organisation muss über einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan verfügen. Sie finden Ihren Förderplan im AWS Support Zentrum oder auf der Seite Supportpläne. Siehe Pläne AWS Supportvergleichen.
- Sie müssen sich als Benutzer mit dem Verwaltungskonto anmelden (oder eine entsprechende Rolle annehmen). Unabhängig davon, ob Sie sich als IAM-Benutzer oder als IAM-Rolle anmelden, müssen Sie über eine Richtlinie mit den erforderlichen Berechtigungen verfügen. Siehe Verwendung von IAM-Richtlinien, um den Zugriff auf die Organisationssicht zu ermöglichen.

Aktivieren der Organisationsansicht

Nachdem Sie die Voraussetzungen erfüllt haben, gehen Sie wie folgt vor, um die Organisationssicht zu aktivieren. Nachdem Sie diese Funktion aktiviert haben, geschieht Folgendes:

- Trusted Advisor ist als vertrauenswürdiger Dienst in Ihrer Organisation aktiviert. Weitere Informationen finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs mit anderen AWS Diensten im AWS Organizations Benutzerhandbuch.
- Die `AWSServiceRoleForTrustedAdvisorReporting` dienstverknüpfte Rolle wird für Sie im Verwaltungskonto in Ihrer Organisation erstellt. Diese Rolle umfasst die Berechtigungen, die Trusted Advisor erforderlich sind, um Organizations in Ihrem Namen anzurufen. Diese dienstverknüpfte Rolle ist gesperrt, und Sie können sie nicht manuell löschen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Trusted Advisor.

Sie aktivieren die Organisationsansicht über die Trusted Advisor-Konsole.

So aktivieren Sie die Organisationssicht

1. Melden Sie sich als Administrator mit dem Verwaltungskonto der Organisation an und öffnen Sie die AWS Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor.
2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Your organization (Meine Organisation) aus.
3. Aktivieren Sie unter Enable trusted access with AWS Organizations (Vertrauenswürdigen Zugriff mit aktivieren) die Option Enabled (Aktiviert).

> **Note**
>
> Das Aktivieren der Organisationsansicht für das Verwaltungskonto bietet nicht die gleichen Prüfungen für alle Mitgliedskonten. Wenn Ihre Mitgliedskonten beispielsweise alle über Basic Support verfügen, stehen diesen Konten nicht die gleichen Prüfungen zur Verfügung wie Ihrem Verwaltungskonto. Die AWS Support-Plan bestimmt, welche Trusted Advisor-Prüfungen für ein Konto verfügbar sind.

Trusted Advisor- Prüfungen aktualisieren

Bevor Sie einen Bericht für Ihre Organisation erstellen, empfehlen wir Ihnen, die Status Ihrer Trusted Advisor Prüfungen zu aktualisieren. Sie können einen Bericht herunterladen, ohne Ihre Trusted Advisor-Prüfungen zu aktualisieren, aber Ihr Bericht enthält möglicherweise nicht die neuesten Informationen.

Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, werden die Prüfungen in Ihrem Konto von Trusted Advisor automatisch wöchentlich aktualisiert.

> **Note**
>
> Wenn Sie in Ihrem Unternehmen über Konten mit einem Entwickler- oder Basis-Supportplan verfügen, muss sich ein Benutzer für diese Konten bei der Trusted Advisor-Konsole anmelden, um die Prüfungen zu aktualisieren. Sie können die Prüfungen für alle Konten nicht über das Verwaltungskonto der Organisation aktualisieren.

So aktualisieren Sie Trusted Advisor Prüfungen

1. Navigieren Sie zur AWS Trusted Advisor-Konsole auf https://console.aws.amazon.com/trustedadvisor.
2. Wählen Sie auf der Seite Trusted Advisor-Empfehlungen die Option Alle Prüfungen aktualisieren. Dadurch werden alle Prüfungen auf Ihrem Konto aktualisiert.

Sie können bestimmte Prüfungen auch auf die folgenden Arten auffrischen:

- Verwenden Sie den API-Vorgang RefreshTrustedAdvisorCheck.
- Wählen Sie das Aktualisierungssymbol
  ()
  für eine einzelne Prüfung.

Berichte für die Organisationsansicht erstellen

Nachdem Sie die Organisationssicht aktiviert haben, können Sie Berichte erstellen, mit denen Sie die Trusted Advisor Prüfungsergebnisse für Ihre Organisation einsehen können.

Sie können bis zu 50 Berichte erstellen. Wenn Sie Berichte erstellen, die dieses Kontingent überschreiten, löscht Trusted Advisor den frühesten Bericht. Sie können gelöschte Berichte nicht wiederherstellen.

So erstellen Sie Berichte zur Organisationssicht

1. Melden Sie sich beim Management-Konto der Organisation an und öffnen Sie die AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.

2. Wählen Sie im Navigationsbereich Organisationssicht.
3. Wählen Sie Create report (Bericht erstellen) aus.
4. Standardmäßig enthält der Bericht alle AWS Regionen, Prüfungskategorien, Prüfungen und Ressourcenstatus. Auf der Seite Bericht erstellen können Sie die Filteroptionen verwenden, um Ihren Bericht anzupassen. Sie können zum Beispiel die Option Alle für Region deaktivieren und dann die einzelnen Regionen angeben, die in den Bericht aufgenommen werden sollen.

   a. Geben Sie einen Namen für den Bericht ein.
   b. Wählen Sie für Format JSON oder CSV.
   c. Geben Sie bei Region die AWS Regionen an oder wählen Sie Alle.
   d. Wählen Sie unter Prüfungskategorie die gewünschte Prüfungskategorie oder wählen Sie Alle.
   e. Wählen Sie unter Prüfungen die spezifischen Prüfungen für diese Kategorie oder wählen Sie Alle.

      > **Note**
      >
      > Der Filter der Prüfungskategorie hat Vorrang vor dem Filter Prüfungen. Wenn Sie z. B. die Kategorie Sicherheit und dann den Namen einer bestimmten Prüfung auswählen, enthält Ihr Bericht alle Prüfungsergebnisse für diese Kategorie.
      > Um einen Bericht nur für bestimmte Prüfungen zu erstellen, behalten Sie den Standardwert Alle für die Prüfungskategorie bei und wählen Sie dann die Namen der Prüfungen aus.

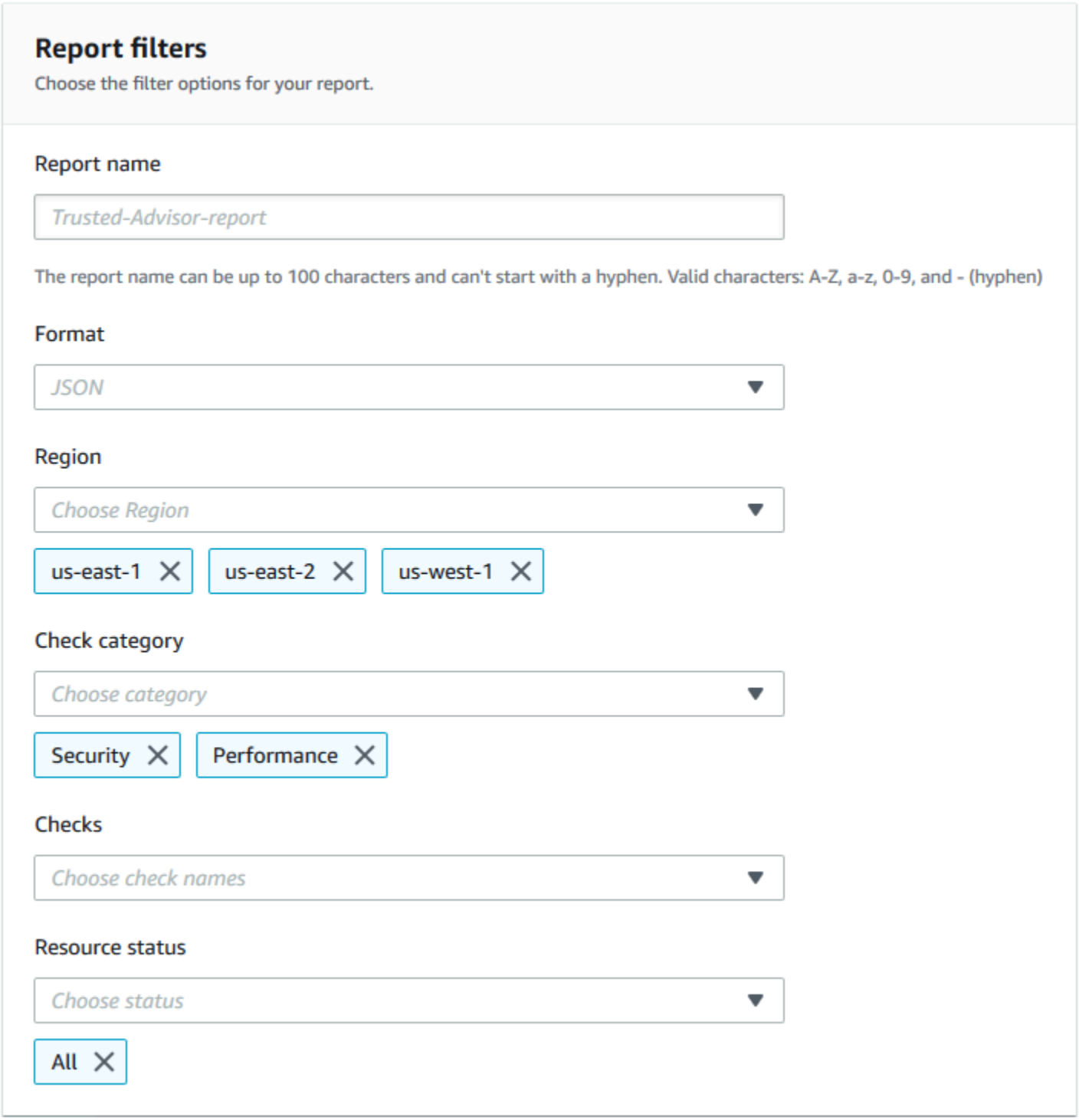
   f. Wählen Sie unter Ressourcenstatus den zu filternden Status, z. B. Warnung, oder wählen Sie Alle.
5. Wählen Sie unter AWS Organisation die Organisationseinheiten (OEs) aus, die in Ihrem Bericht enthalten sein sollen. Weitere Informationen über OUs finden Sie unter Verwaltung von Organisationseinheiten im AWS OrganizationsBenutzerhandbuch.
6. Wählen Sie Create report (Bericht erstellen) aus.

Example : Berichtsfilteroptionen erstellen

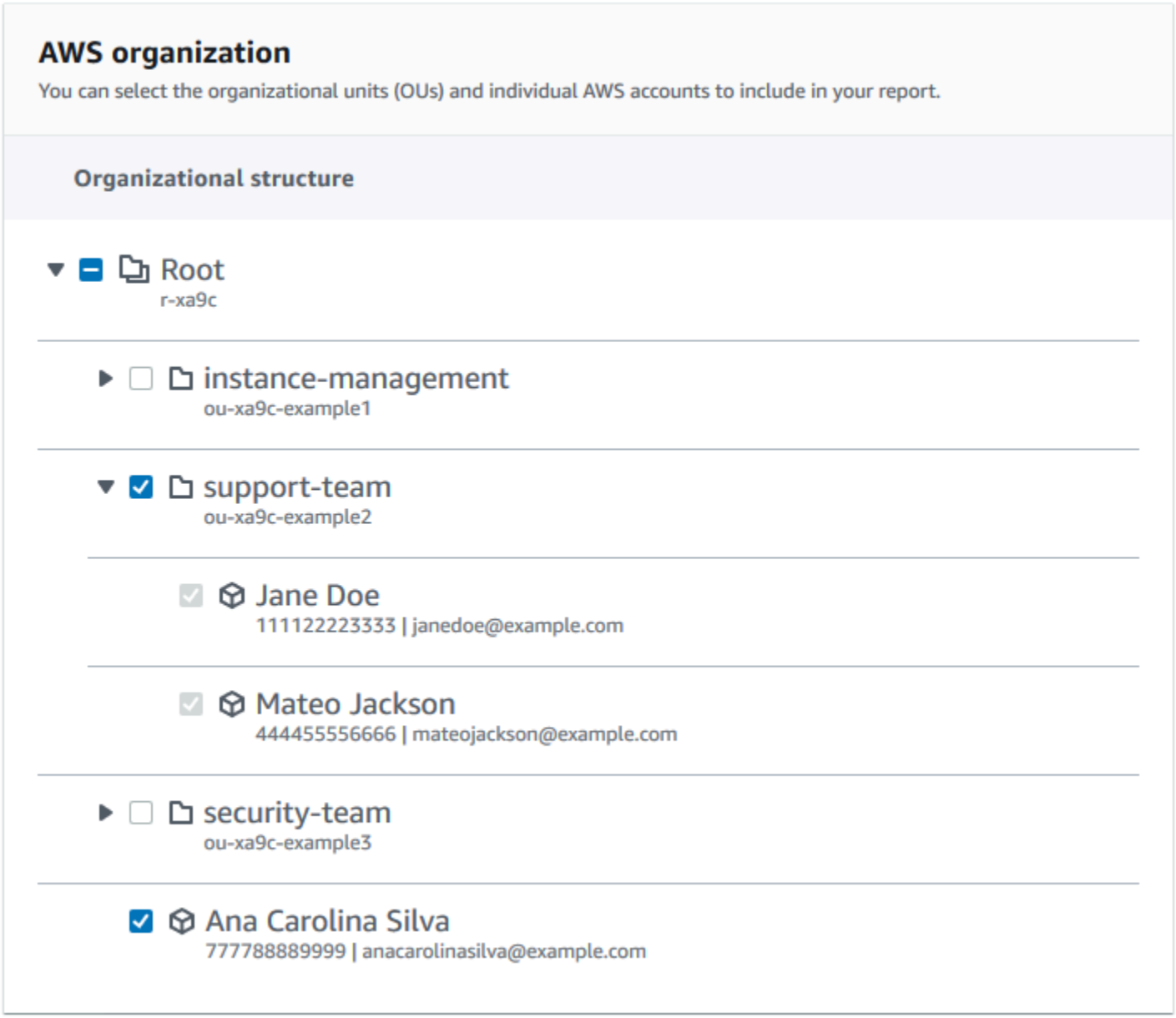
Das folgende Beispiel erstellt einen JSON-Bericht für Folgendes:

- Drei AWS Regionen

- Alle Sicherheits- und Leistungsprüfungen



Im folgenden Beispiel enthält der Bericht die OE Support-Team und ein AWS Konto, die Teil der Organisation sind.



Hinweise

- Die Zeit, die für die Erstellung des Berichts benötigt wird, hängt von der Anzahl der Konten im Unternehmen und der Anzahl der Ressourcen in jedem Konto ab.
- Sie können nicht mehr als einen Bericht auf einmal erstellen, es sei denn, der aktuelle Bericht läuft bereits seit mehr als 6 Stunden.
- Aktualisieren Sie die Seite, wenn der Bericht nicht auf der Seite angezeigt wird.

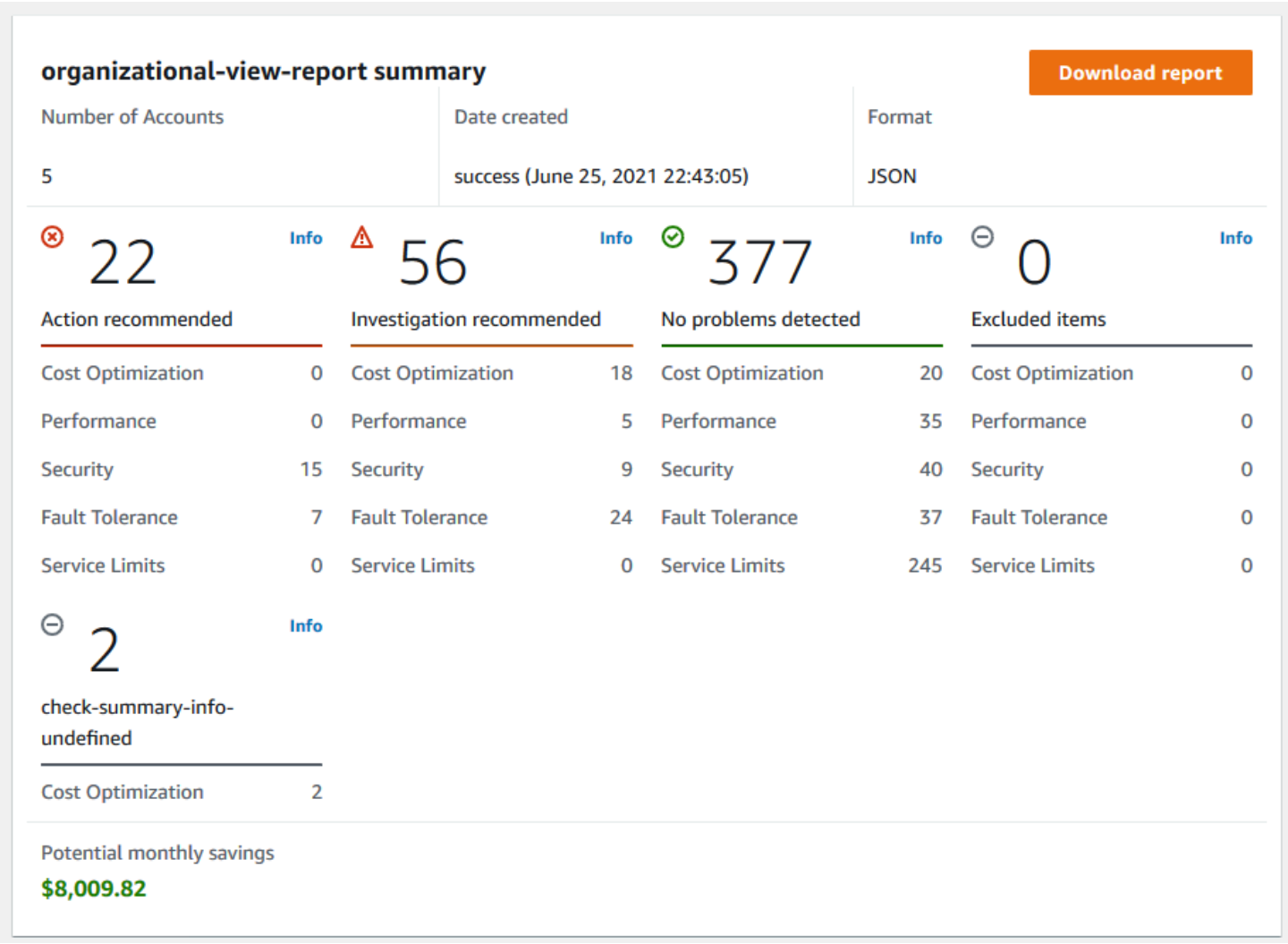
Zusammenfassung des Berichts anzeigen

Nachdem der Bericht fertig ist, können Sie die Zusammenfassung des Berichts in der Trusted Advisor Konsole einsehen. Auf diese Weise können Sie sich schnell einen Überblick über die Ergebnisse Ihrer Prüfungen in Ihrem Unternehmen verschaffen.

So zeigen Sie die Zusammenfassung des Berichts an

1. Melden Sie sich beim Management-Konto der Organisation an und öffnen Sie die AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.
2. Wählen Sie im Navigationsbereich Organisationssicht.
3. Wählen Sie den Namen des Berichts.
4. Auf der Seite Zusammenfassung können Sie den Status der Prüfungen für jede Kategorie einsehen. Sie können auch Bericht herunterladen wählen.

Example : Zusammenfassung des Berichts für eine Organisation



Bericht zur Organisationssicht herunterladen

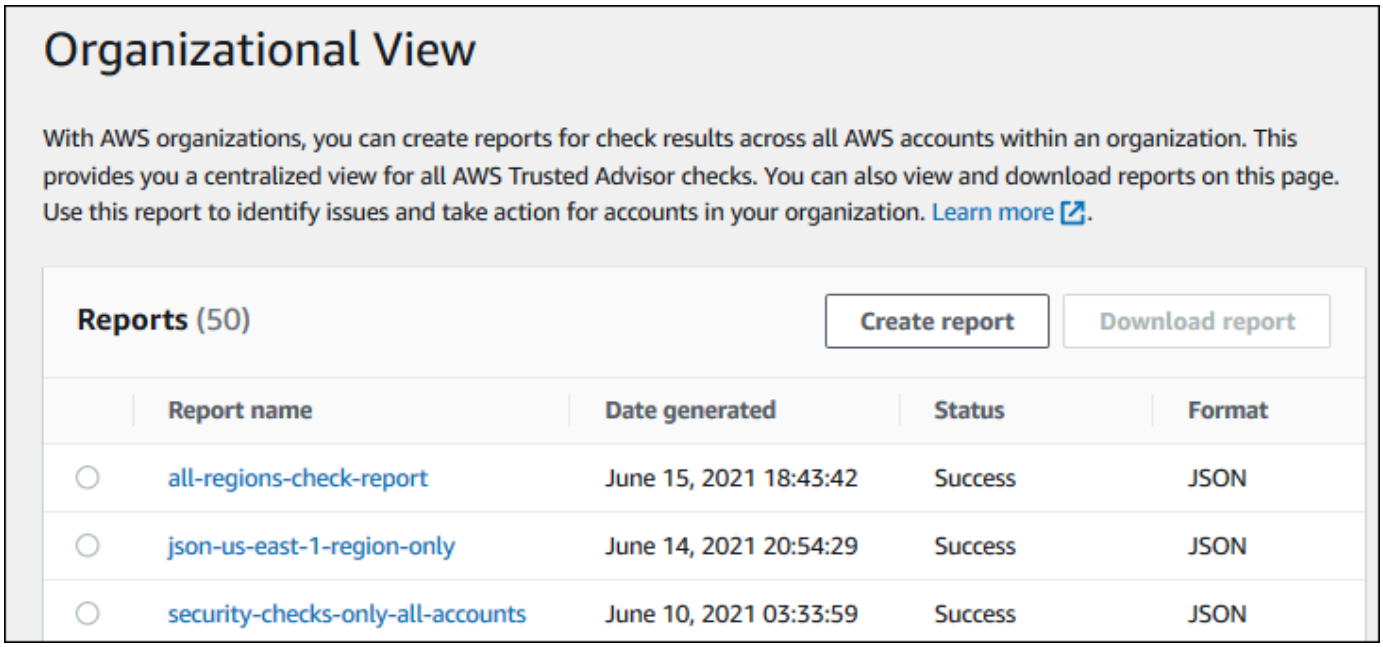
Wenn Ihr Bericht fertig ist, laden Sie ihn von der Trusted Advisor Konsole herunter. Der Bericht ist eine .zip-Datei, die drei Dateien enthält:

- `summary.json` – Der Bericht ist eine .zip-Datei, die drei Dateien enthält:
- `schema.json` – Enthält das Schema für die angegebenen Prüfungen im Bericht.
- Eine Ressourcendatei (.json oder .csv) - Enthält detaillierte Informationen über den Status der Prüfungen von Ressourcen in Ihrer Organisation.

So laden Sie einen Bericht zur Organisationssicht herunter

1. Melden Sie sich beim Management-Konto der Organisation an und öffnen Sie die AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.
2. Wählen Sie im Navigationsbereich Organisationssicht.

   Auf der Seite Organisationsansicht werden die verfügbaren Berichte zum Herunterladen angezeigt.
3. Wählen Sie einen Bericht aus, wählen Sie Bericht herunterladen und speichern Sie dann die Datei. Sie können immer nur einen Bericht auf einmal herunterladen.



4. Entpacken Sie die Datei.
5. Öffnen Sie die `.json` Datei mit einem Texteditor oder die `.csv` Datei einem Tabellenkalkulationsprogramm.

> **Note**
>
> Sie erhalten möglicherweise mehrere Dateien, wenn Ihr Bericht 5 MB oder größer ist.

Example : summary.json Datei

Die `summary.json` Datei zeigt die Anzahl der Konten in der Organisation und den Status der Prüfungen in jeder Kategorie.

Trusted Advisor verwendet den folgenden Farbcode für Prüfungsergebnisse:

- `Green` – Trusted Advisor stellt keine Probleme bei der Prüfung fest.
- `Yellow` – Trusted Advisor stellt ein mögliches Problem bei der Prüfung fest.
- `Red` – Trusted Advisor stellt einen Fehler fest und empfiehlt eine Maßnahme für die Prüfung.
- `Blue` – Trusted Advisor kann den Status der Prüfung nicht feststellen.

Im folgenden Beispiel sind zwei Prüfungen `Red`, eine ist `Green` und eine ist `Yellow`.


```
{
    "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 Datei

Die `schema.json` Datei enthält das Schema für die Prüfungen im Bericht. Das folgende Beispiel enthält die IDs und Eigenschaften für die Prüfungen IAM Passwortrichtlinie (Yw2K9puPzl) und IAM Key Rotation (DqdJqYeRm5).

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

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

Example : resources.csv Datei

Die `resources.csv` Datei enthält Informationen über Ressourcen in der Organisation. Dieses Beispiel zeigt einige der Datenspalten, die in dem Bericht erscheinen, wie z. B. die Folgende:

- Konten-ID des betroffenen Kontos
- Die Trusted Advisor Prüfung der ID
- Die Ressourcen-ID.
- Zeitstempel des Berichts
- Der vollständige Name der Trusted Advisor Prüfung
- Die Trusted Advisor Prüfungskategorie
- Die Konto-ID der übergeordneten Organisationseinheit (OU) oder des Stammkontos

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	wAvASS3YOwy6WWxlBHf	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	H7lgTzjTYb	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

Die Ressourcendatei enthält nur dann Einträge, wenn ein Prüfungsergebnis auf Ressourcenebene vorliegt. Es kann sein, dass Sie Prüfungen im Bericht aus folgenden Gründen nicht sehen:

- Einige Prüfungen, wie z. B. MFA on Root-Konto, haben keine Ressourcen und werden nicht im Bericht angezeigt. Prüfungen ohne Ressourcen erscheinen stattdessen in der `summary.json` Datei.
- Einige Prüfungen zeigen nur Ressourcen an, wenn sie `Red` oder `Yellow` sind. Wenn alle Ressourcen `Green` sind, erscheinen sie möglicherweise nicht in Ihrem Bericht.
- Wenn ein Konto nicht für einen Dienst aktiviert ist, der die Prüfung erfordert, erscheint die Prüfung möglicherweise nicht im Bericht. Wenn Sie beispielsweise keine Amazon Elastic Compute Cloud Reserved Instances in Ihrem Unternehmen verwenden, wird die Prüfung des Ablaufs der Amazon EC2 Reserved Instance Lease nicht in Ihrem Bericht erscheinen.
- Das Konto hat die Ergebnisse der Prüfung nicht aufgefrischt. Dies kann passieren, wenn sich Benutzer mit einem Basic- oder Developer-Supportplan zum ersten Mal bei der Trusted Advisor Konsole anmelden. Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, kann es bis zu einer Woche nach der Anmeldung des Kontos dauern, bis die Benutzer die Prüfungsergebnisse sehen. Weitere Informationen finden Sie unter Trusted Advisor- Prüfungen aktualisieren.
- Wenn nur das Managementkonto der Organisation Empfehlungen für Prüfungen aktiviert hat, enthält der Bericht keine Ressourcen für andere Konten in der Organisation.

Für die Ressourcendatei können Sie eine gängige Software wie Microsoft Excel verwenden, um das .csv-Dateiformat zu öffnen. Sie können die .csv-Datei für eine einmalige Analyse aller Prüfungen über alle Konten in Ihrer Organisation verwenden. Wenn Sie Ihren Bericht in einer Anwendung verwenden möchten, können Sie ihn stattdessen als .json-Datei herunterladen.

Das .json-Dateiformat bietet mehr Flexibilität als das .csv-Dateiformat für fortgeschrittene Anwendungsfälle wie Aggregation und erweiterte Analysen mit mehreren Datensätzen. Sie können zum Beispiel eine SQL-Schnittstelle mit einem AWS Dienst wie Amazon Athena verwenden, um Abfragen zu Ihren Berichten durchzuführen. Sie können auch Amazon QuickSight verwenden, um Dashboards zu erstellen und Ihre Daten zu visualisieren. Weitere Informationen finden Sie unter Verwendung anderer AWS Dienste zur Anzeige von Trusted Advisor Berichten.

Organisationssicht deaktivieren

Gehen Sie wie folgt vor, um die Organisationssicht zu deaktivieren. Sie müssen sich beim Verwaltungskonto der Organisation anmelden oder eine Rolle mit den erforderlichen Berechtigungen

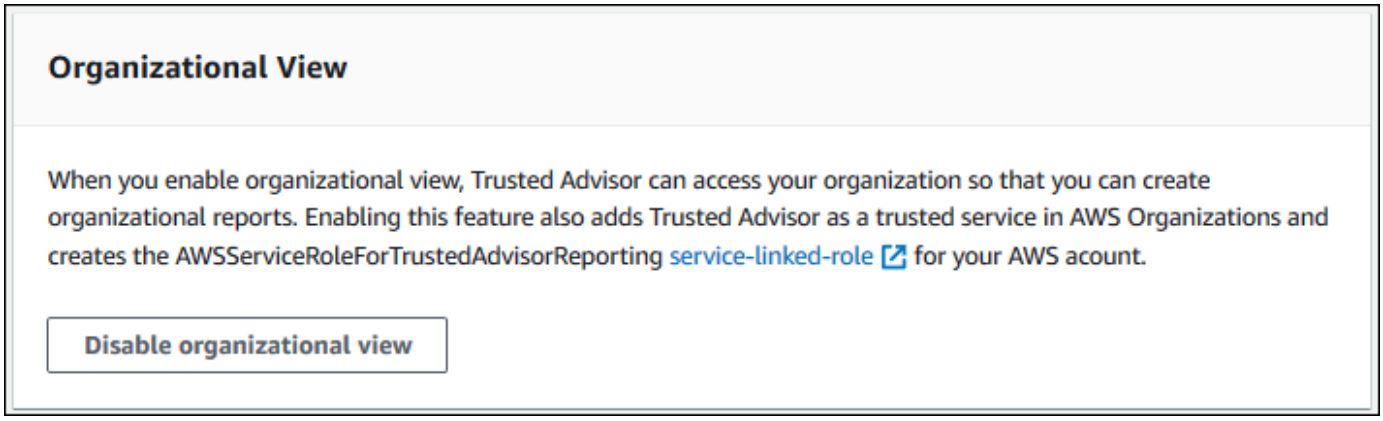
übernehmen, um diese Funktion zu deaktivieren. Sie können diese Funktion nicht von einem anderen Konto in der Organisation aus deaktivieren.

Nachdem Sie diese Funktion deaktiviert haben, geschieht Folgendes:

- Trusted Advisor wird als vertrauenswürdiger Dienst in Organizations entfernt.
- Die `AWSServiceRoleForTrustedAdvisorReporting` dienstgebundene Rolle wird im Verwaltungskonto der Organisation freigeschaltet. Das bedeutet, dass Sie sie bei Bedarf manuell löschen können.
- Sie können keine Berichte für Ihr Unternehmen erstellen, anzeigen oder herunterladen. Um auf zuvor erstellte Berichte zuzugreifen, müssen Sie die Organisationssicht in der Trusted Advisor Konsole erneut aktivieren. Siehe Aktivieren der Organisationsansicht.

So deaktivieren Sie die Organisationssicht für Trusted Advisor

1. Melden Sie sich beim Management-Konto der Organisation an und öffnen Sie die AWS Trusted Advisor Konsole unter https://console.aws.amazon.com/trustedadvisor.
2. Klicken Sie im Navigationsbereich auf Preferences (Präferenzen).
3. Wählen Sie unter Organisationssicht die Option Organisationssicht deaktivieren.



Nachdem Sie die Organisationssicht deaktiviert haben, aggregiert Trusted Advisor keine Prüfungen von anderen AWS Konten in Ihrer Organisation mehr. Die `AWSServiceRoleForTrustedAdvisorReporting` dienstverknüpfte Rolle bleibt jedoch im Verwaltungskonto der Organisation, bis Sie sie über die IAM-Konsole, die IAM-API oder AWS Command Line Interface (AWS CLI) löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

> **Note**
>
> Sie können AWS andere Dienste verwenden, um Ihre Daten für Berichte zur Organisationssicht abzufragen und zu visualisieren. Weitere Informationen finden Sie in den folgenden Ressourcen:
>
> - Sehen Sie sich die AWS Trusted Advisor Empfehlungen AWS Organizations im AWSManagement & Governance Blog an
> - Verwendung anderer AWS Dienste zur Anzeige von Trusted Advisor Berichten

Verwendung von IAM-Richtlinien, um den Zugriff auf die Organisationssicht zu ermöglichen

Sie können die folgenden AWS Identity and Access Management (IAM-)Richtlinien verwenden, um Benutzern oder Rollen in Ihrem Konto den Zugriff auf die Organisationssicht in AWS Trusted Advisor.

Example : Voller Zugriff auf die Organisationsansicht

Die folgende Richtlinie ermöglicht den vollen Zugriff auf die Funktion der Organisationssicht. Ein Benutzer mit diesen Rechten kann Folgendes tun:

- Aktivieren und Deaktivieren der Organisationsansicht
- Berichte erstellen, anzeigen und herunterladen

```
{
    "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 : Lesezugriff auf die Organisationsansicht

Die folgende Richtlinie erlaubt schreibgeschützten Zugriff auf die Organisationssicht für Trusted Advisor. Ein Benutzer mit diesen Berechtigungen kann nur vorhandene Berichte anzeigen und herunterladen.

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

Sie können auch Ihre eigene IAM-Richtlinie erstellen. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn Sie AWS CloudTrail in Ihrem Konto aktiviert haben, können die folgenden Rollen in Ihren Protokolleinträgen erscheinen:

- `AWSServiceRoleForTrustedAdvisorReporting` – Die mit dem Dienst verknüpfte Rolle, die Trusted Advisor für den Zugriff auf Konten in Ihrer Organisation verwendet.
- `AWSServiceRoleForTrustedAdvisor` – Die mit dem Dienst verknüpfte Rolle, die Trusted Advisor für den Zugriff auf Dienste in Ihrer Organisation verwendet.

Weitere Informationen zu Service-verknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Trusted Advisor.

Verwendung anderer AWS Dienste zur Anzeige von Trusted Advisor Berichten

Folgen Sie dieser Anleitung, um Ihre Daten mit Hilfe anderer AWS Dienste hochzuladen und anzuzeigen. In diesem Thema erstellen Sie einen Amazon Simple Storage Service (Amazon S3)-Bucket zum Speichern Ihres Berichts und eine AWS CloudFormation Vorlage zum Erstellen von Ressourcen in Ihrem Konto. Anschließend können Sie Amazon Athena verwenden, um Ihren Bericht zu analysieren oder Abfragen auszuführen, oder Amazon QuickSight, um diese Daten in einem Dashboard zu visualisieren.

Informationen und Beispiele für die Visualisierung Ihrer Berichtsdaten finden Sie im AWS Blog Management & Governance unter Empfehlungen AWS Trusted Advisor im Maßstab anzeigen mit AWS Organizations.

Voraussetzungen

Bevor Sie mit diesem Lernprogramm beginnen, müssen Sie die folgenden Voraussetzungen erfüllen:

- Melden Sie sich als AWS Identity and Access Management (IAM)-Benutzer mit Administratorberechtigung an.
- Verwenden Sie die AWS Region US East (N. Virginia), um Ihre AWS Dienste und Ressourcen schnell einzurichten.
- Erstellen Sie ein Amazon QuickSight-Konto. Weitere Informationen finden Sie unter Erste Schritte mit der Datenanalyse in Amazon QuickSight im Amazon QuickSight Benutzerhandbuch.

Hochladen des Berichts auf Amazon S3

Nachdem Sie Ihren `resources.json` Bericht heruntergeladen haben, laden Sie die Datei auf Amazon S3 hoch. Sie müssen einen Bucket in der Region US East (N. Virginia) verwenden.

So laden Sie den Bericht in einen Amazon S3-Bucket hoch

1. Melden Sie sich an der AWS Management Console unter https://console.aws.amazon.com/ an.
2. Verwenden Sie die Regionenauswahl und wählen Sie die Region US East (N. Virginia).
3. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.
4. Wählen Sie aus der Liste der Buckets einen S3-Bucket aus, und kopieren Sie den Namen. Sie verwenden den Namen im nächsten Verfahren.
5. Wählen Sie auf der Seite *Bucketname* die Option Ordner erstellen, geben Sie den Namen **folder1** ein, und wählen Sie dann Speichern.
6. Wählen Sie Ordner1.
7. Wählen Sie in Ordner1 die Option Hochladen und wählen Sie die `resources.json` Datei.
8. Wählen Sie Weiter, behalten Sie die Standardoptionen bei, und wählen Sie dann Hochladen.

> **Note**
>
> Wenn Sie einen neuen Bericht in diesen Bucket hochladen, benennen Sie die `.json` Dateien bei jedem Hochladen um, damit Sie die vorhandenen Berichte nicht überschreiben. Sie können zum Beispiel jeder Datei einen Zeitstempel hinzufügen, wie z. B. `resources-timestamp.json`, `resources-timestamp2.json`, usw.

Erstellen Sie Ihre von Ressourcen mit AWS CloudFormation

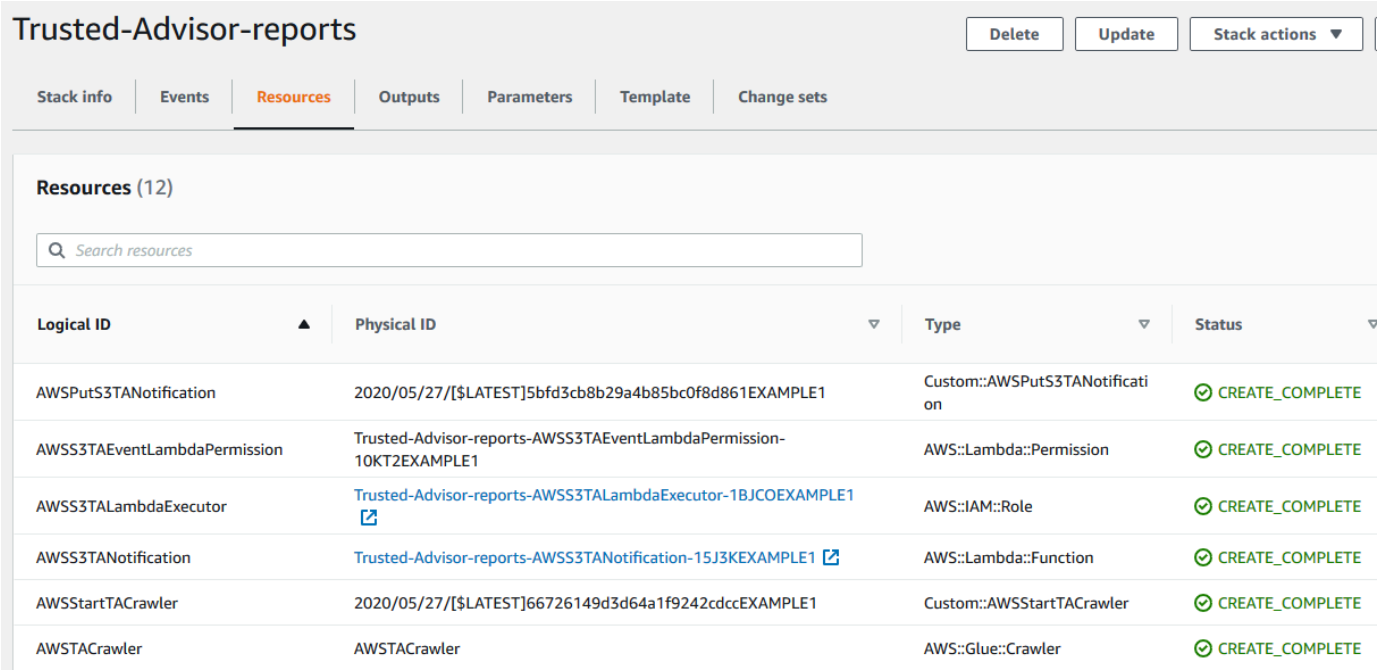
Nachdem Sie Ihren Bericht in Amazon S3 hochgeladen haben, laden Sie die folgende YAML-Vorlage in AWS CloudFormation. Diese Vorlage informiert AWS CloudFormation, welche Ressourcen für Ihr Konto erstellt werden sollen, damit andere Dienste die Berichtsdaten im S3-Bucket nutzen können. Die Vorlage erstellt Ressourcen für IAM, AWS Lambda, und AWS Glue.

So erstellen Sie Ihre Ressourcen mit AWS CloudFormation

1. Laden Sie die Datei trusted-advisor-reports-template.zip herunter.
2. Entpacken Sie die Datei.

3. Öffnen Sie die Vorlagendatei in einem Texteditor.
4. Ersetzen Sie bei den Parametern `BucketName` und `FolderName` die Werte für *`your-bucket-name-here`* und *`folder1`* durch den Bucketnamen und den Ordnernamen in Ihrem Konto.
5. Speichern Sie die Datei.
6. Öffnen Sie die AWS CloudFormation-Konsole unter https://console.aws.amazon.com/cloudformation.
7. Wenn Sie es noch nicht getan haben, wählen Sie in der Regionsauswahl die Region US East (N. Virginia).
8. Klicken Sie im Navigationsbereich auf Stacks.
9. Wählen Sie Create stack (Stack erstellen) und With new resources (standard) (Mit neuen Ressourcen (Standard)) aus.
10. Wählen Sie auf der Seite Create stack (Stapel erstellen) unter Vorlage angeben die Option Eine Vorlagendatei hochladen und dann Datei auswählen.
11. Wählen Sie die YAML-Datei aus und wählen Sie Weiter.
12. Geben Sie auf der Seite Stack-Details angeben einen Stack-Namen ein, z. B. **`Organizational-view-Trusted-Advisor-reports`**, und wählen Sie Weiter.
13. Behalten Sie auf der Seite Stack-Optionen konfigurieren die Standardoptionen bei, und wählen Sie dann Weiter.
14. Überprüfen Sie auf der Seite Überprüfung **`Organizational-view-Trusted-Advisor-reports`** Ihre Optionen. Aktivieren Sie unten auf der Seite das Kontrollkästchen für Ich bestätige, dass AWS CloudFormation möglicherweise IAM-Ressourcen erstellt.
15. Wählen Sie Stack erstellen aus.

    Die Erstellung des Stapels dauert etwa 5 Minuten.
16. Nachdem der Stapel erfolgreich erstellt wurde, erscheint die Registerkarte Ressourcen wie im folgenden Beispiel.



Abfrage der Daten in Amazon Athena

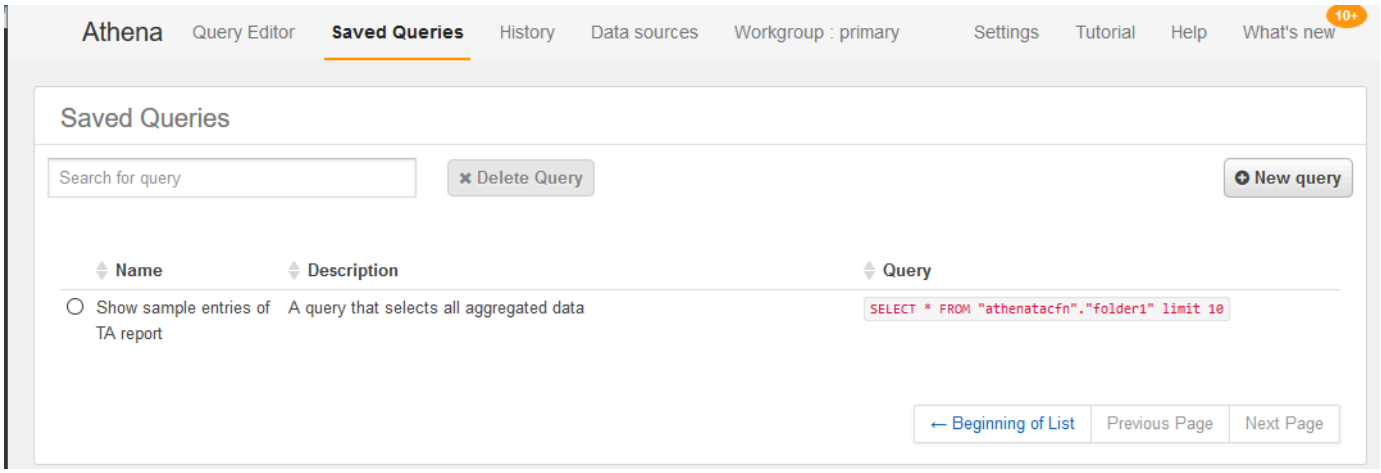
Wenn Sie Ihre Ressourcen haben, können Sie die Daten in Athena einsehen. Verwenden Sie Athena, um Abfragen zu erstellen und die Ergebnisse des Berichts zu analysieren, z. B. um bestimmte Prüfungsergebnisse für Konten in der Organisation zu suchen.

> **Hinweise**
>
> - Verwenden Sie die Region US East (N. Virginia).
> - Wenn Sie neu in Athena sind, müssen Sie einen Speicherort für Abfrageergebnisse angeben, bevor Sie eine Abfrage für Ihren Bericht ausführen können. Wir empfehlen Ihnen, einen anderen S3-Bucket für diesen Speicherort anzugeben. Weitere Informationen finden Sie unter Festlegen eines Abfrageergebnisspeichers im Amazon Athena User Guide.

So fragen Sie die Daten in Athena ab

1. Öffnen Sie die Athena-Konsole unter https://console.aws.amazon.com/athena/.
2. Wenn Sie es noch nicht getan haben, wählen Sie in der Regionsauswahl die Region US East (N. Virginia).
3. Wählen Sie Gespeicherte Abfragen und geben Sie **`Show sample`** in das Suchfeld ein.

4. Wählen Sie die angezeigte Abfrage, z. B. Beispieleinträge des TA-Berichts anzeigen.



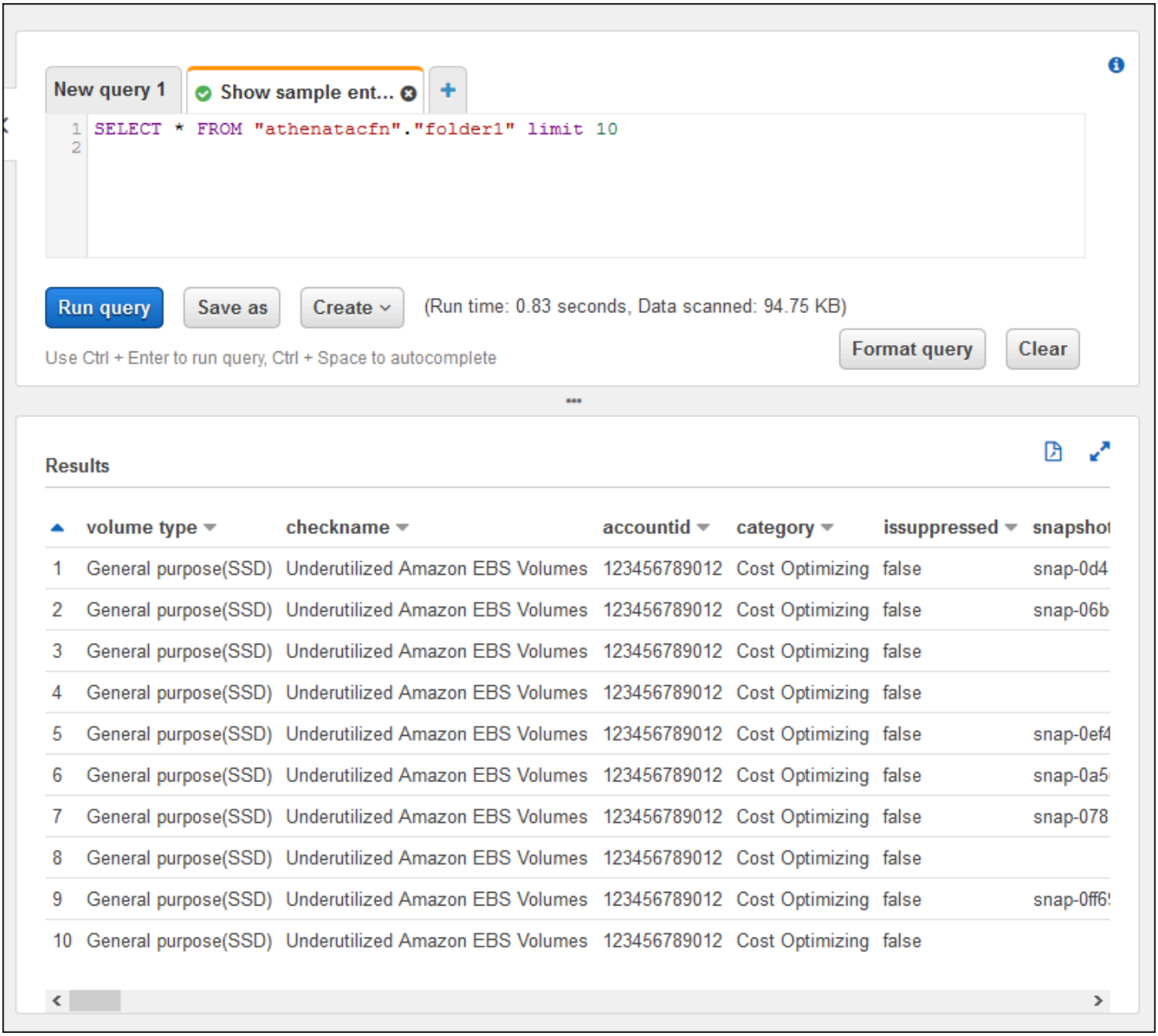
Die Abfrage sollte wie folgt aussehen.

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

5. Wählen Sie Abfrage ausführen. Ihre Abfrageergebnisse werden angezeigt.

Example : Athena-Abfrage

Das folgende Beispiel zeigt 10 Beispieleinträge aus dem Bericht.



	volume type	checkname	accountid	category	issuppressed	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

Weitere Informationen finden Sie unter Ausführen von SQL-Abfragen mit Amazon Athena im Amazon Athena User Guide.

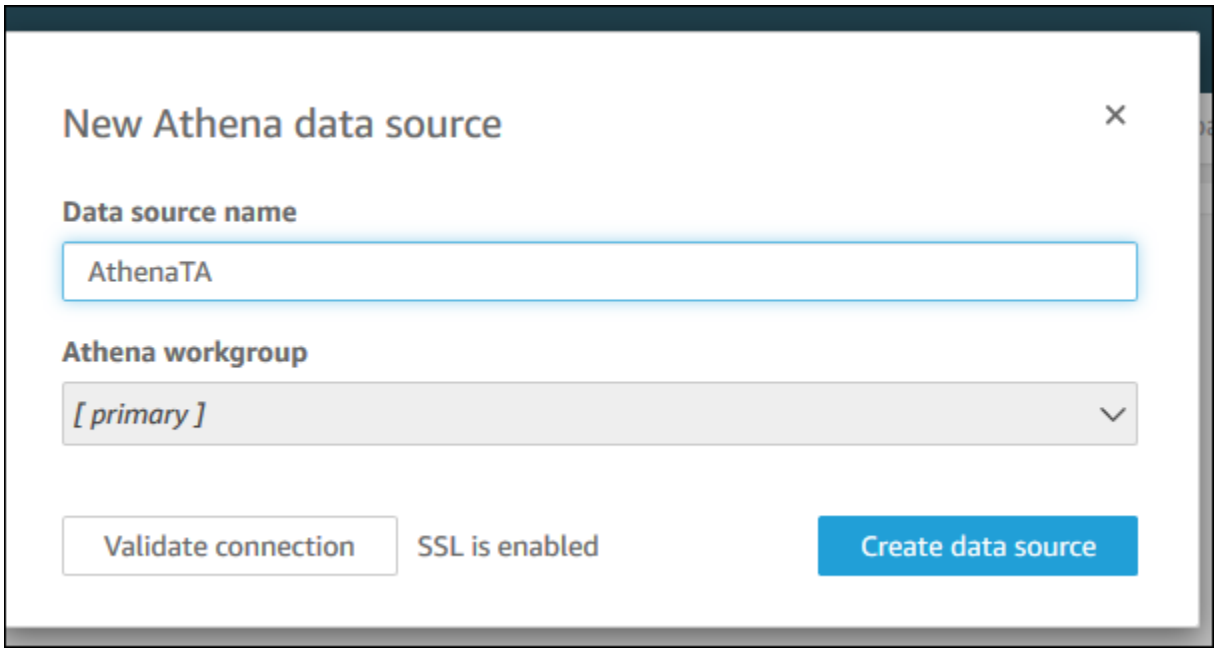
Erstellen Sie ein Dashboard in Amazon QuickSight

Sie können Amazon QuickSight auch so einrichten, dass Sie Ihre Daten in einem Dashboard anzeigen und Ihre Berichtsinformationen visualisieren können.

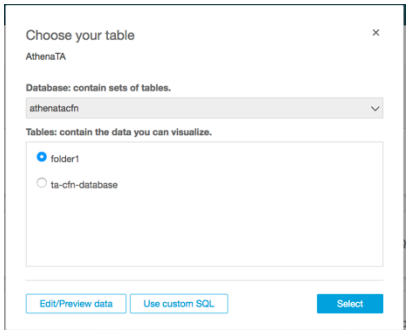
> **Note**
>
> Sie müssen die Region US East (N. Virginia) verwenden.

So erstellen Sie ein Dashboard in Amazon QuickSight

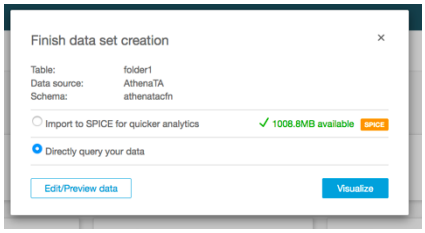
1. Navigieren Sie zur Amazon QuickSight-Konsole und melden Sie sich bei Ihrem Konto an.
2. Wählen Sie Neue Analyse, Neues Dataset und dann Athena.
3. Geben Sie im Dialogfeld Neue Athena-Datenquelle einen Datenquellennamen ein, z. B. AthenaTA, und wählen Sie dann Datenquelle erstellen.



4. Wählen Sie im Dialogfenster Wählen Sie Ihre Tabelle die Tabelle athenatacfn, wählen Sie Ordner1 und wählen Sie dann Auswählen.



5. Wählen Sie im Dialogfeld Datensatzerstellung beenden die Option Daten direkt abfragen und wählen Sie dann Visualisieren.

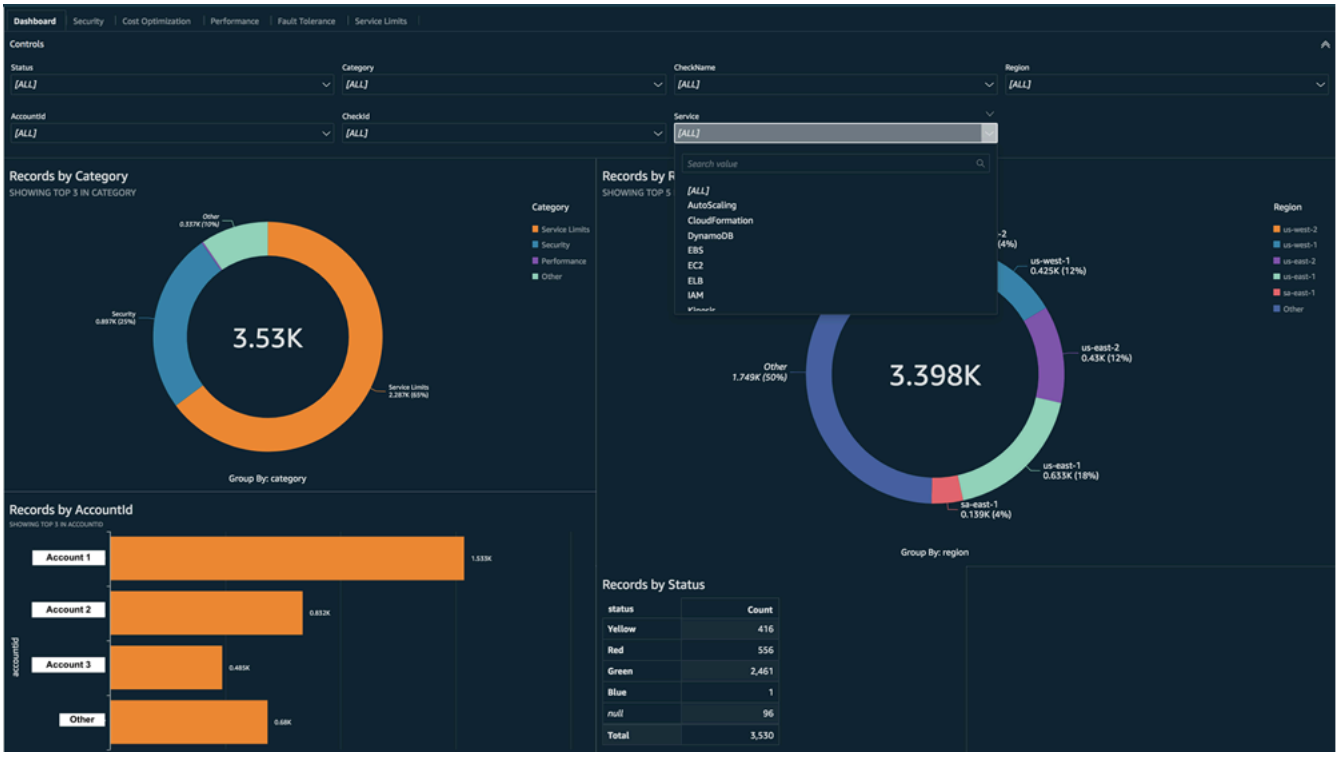


Sie können jetzt ein Dashboard in Amazon QuickSight erstellen. Weitere Informationen finden Sie unter Arbeiten mit Dashboards im Amazon QuickSight Benutzerhandbuch.

Example : Amazon QuickSight dashboard

Das folgende Beispiel-Dashboard zeigt Informationen über die Trusted Advisor Prüfungen, wie z. B. die folgenden:

- Betroffene Konto-IDs
- Zusammenfassung vonAWS-Regionen
- Kategorien prüfen
- Status prüfen
- Anzahl der Einträge im Bericht für jedes Konto



> **Note**
>
> Wenn Sie beim Erstellen Ihres Dashboards Berechtigungsfehler haben, stellen Sie sicher, dass Amazon QuickSight Athena verwenden kann. Weitere Informationen finden Sie unter Ich kann keine Verbindung zu Amazon Athena herstellen im Amazon QuickSight-Benutzerhandbuch.

Weitere Informationen und Beispiele für die Visualisierung Ihrer Berichtsdaten finden Sie im AWS Blog Management & Governance unter Empfehlungen AWS Trusted Advisor im Maßstab anzeigen mit AWS Organizations.

Fehlerbehebung

Wenn Sie Probleme mit dieser Anleitung haben, beachten Sie bitte die folgenden Tipps zur Fehlerbehebung.

Ich sehe die neuesten Daten nicht in meinem Bericht

Wenn Sie einen Bericht erstellen, aktualisiert die Organisationssichtfunktion nicht automatisch die Trusted Advisor Prüfungen in Ihrer Organisation. Um die neuesten Prüfungsergebnisse zu erhalten, aktualisieren Sie die Prüfungen für das Verwaltungskonto und jedes Mitgliedskonto in der Organisation. Weitere Informationen finden Sie unter Trusted Advisor- Prüfungen aktualisieren.

Ich habe doppelte Spalten im Bericht

Die Athena-Konsole zeigt möglicherweise den folgenden Fehler in Ihrer Tabelle an, wenn Ihr Bericht doppelte Spalten enthält.

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

Wenn Sie z. B. eine Spalte in Ihren Bericht eingefügt haben, die bereits vorhanden ist, kann dies zu Problemen führen, wenn Sie versuchen, die Berichtsdaten in der Athena-Konsole anzuzeigen. Sie können dieses Problem mit den folgenden Schritten beheben.

Doppelte Spalten finden

Sie können dieAWS Glue-Konsole verwenden, um das Schema anzuzeigen und schnell zu erkennen, ob Sie doppelte Spalten in Ihrem Bericht haben.

So finden Sie doppelte Spalten

1. Öffnen Sie die AWS Glue-Konsole unter https://console.aws.amazon.com/glue/.
2. Wenn Sie es noch nicht getan haben, wählen Sie in der Regionsauswahl die Region US East (N. Virginia).
3. Wählen Sie im Navigationsbereich Tables (Tabellen) aus.
4. Wählen Sie den Namen Ihres Ordners, z. B. ***`Older1`***, und zeigen Sie dann unter Schema die Werte für Kolumnenname an.

   Wenn Sie eine doppelte Spalte haben, müssen Sie einen neuen Bericht in Ihren Amazon S3-Bucket hochladen. Lesen Sie den folgenden Einen neuen Bericht hochladen Abschnitt.

Einen neuen Bericht hochladen

Nachdem Sie die doppelte Spalte identifiziert haben, empfehlen wir Ihnen, den bestehenden Bericht durch einen neuen zu ersetzen. Dadurch wird sichergestellt, dass die mit diesem Tutorial erstellten Ressourcen die neuesten Berichtsdaten Ihrer Organisation verwenden.

So laden Sie einen neuen Bericht hoch

1. Falls noch nicht geschehen, aktualisieren Sie Ihre Trusted Advisor Prüfungen für die Konten in Ihrer Organisation. Siehe Trusted Advisor- Prüfungen aktualisieren.
2. Erstellen und laden Sie einen weiteren JSON-Bericht in der Trusted Advisor-Konsole herunter. Siehe Berichte für die Organisationsansicht erstellen. Für dieses Lernprogramm müssen Sie eine JSON-Datei verwenden.
3. Melden Sie sich bei der AWS Management Console an und öffnen Sie die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/.
4. Wählen Sie Ihren Amazon S3-Bucket und den *`folder1`*-Ordner aus.
5. Markieren Sie die vorherigen *`resources`*`.json`-Berichte und wählen Sie Löschen.
6. Geben Sie **`permanently delete`** auf der Seite Objekte löschen unter Objekte permanent löschen? ein, und wählen Sie dann Objekte löschen.
7. Wählen Sie in Ihrem S3 Bucket die Option Hochladen und geben Sie dann den neuen Bericht an. Diese Aktion aktualisiert automatisch Ihre Athena-Tabelle und AWS Glue Crawler-Ressourcen mit den neuesten Berichtsdaten. Es kann ein paar Minuten dauern, bis Sie Ihre Ressourcen aktualisiert haben.

8. Geben Sie eine neue Abfrage in der Athena-Konsole ein. Siehe Abfrage der Daten in Amazon Athena.

> **Note**
>
> Wenn Sie immer noch Probleme mit diesem Tutorial haben, können Sie einen technischen Support-Fall im AWS Support Center erstellen.

AWS Trusted Advisor-Prüfungen anzeigen, die von AWS Config unterstützt werden

AWS Config ist ein Service, der Ihre Ressourcenkonfigurationen fortlaufend bewertet, prüft und auf die von Ihnen gewünschten Einstellungen hin untersucht. AWS Config stellt verwaltete Regeln zur Verfügung, bei denen es sich um vordefinierte, anpassbare Compliance-Überprüfungen handelt, mit denen AWS Config prüft, ob Ihre AWS-Ressourcen den gängigen bewährten Methoden entsprechen.

Die AWS Config-Konsole führt Sie durch die Konfiguration und Aktivierung der verwalteten Regeln. Außerdem können Sie mit der AWS Command Line Interface (AWS CLI)- oder AWS Config-API den JSON-Code übergeben, der Ihre Konfiguration einer verwalteten Regel definiert. Sie können das Verhalten einer verwalteten Regel Ihren Anforderungen entsprechend anpassen. Sie können die Regelparameter anpassen, um die Attribute zu definieren, über die Ihre Ressourcen verfügen müssen, damit sie regelkonform sind. Weitere Informationen zur Aktivierung von AWS Config finden Sie im AWS Config-Benutzerhandbuch.

AWS Config-verwaltete Regeln steuern eine Reihe von Trusted Advisor-Prüfungen in allen Kategorien. Wenn Sie bestimmte verwaltete Regeln aktivieren, werden die entsprechenden Trusted Advisor-Prüfungen automatisch aktiviert. Informationen darüber, welche Trusted Advisor-Prüfungen durch bestimmte von AWS Config verwaltete Regeln unterstützt werden, erhalten Sie unter AWS Trusted Advisor Referenz überprüfen.

Die von AWS Config unterstützten Prüfungen sind für Kunden mit AWS Business-Support-, AWS Enterprise-On-Ramp- und AWS Enterprise-Support-Plänen verfügbar. Wenn Sie AWS Config aktivieren und über einen dieser AWS-Supportpläne verfügen, werden Ihnen automatisch Empfehlungen angezeigt, die auf den entsprechenden, von AWS Config verwalteten Regeln basieren.

> **Note**
>
> Die Ergebnisse dieser Prüfungen werden automatisch auf der Grundlage der durch Änderungen ausgelösten Aktualisierungen der von AWS Config verwalteten Regeln aktualisiert. Aktualisierungsanfragen sind nicht zulässig. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Fehlerbehebung

Wenn Sie Probleme mit dieser Integration haben, lesen Sie die folgenden Informationen zur Fehlerbehebung.

Inhalt

Ich habe gerade die Aufnahme und die verwalteten Regeln für AWS Config aktiviert, aber es werden keine entsprechenden Trusted Advisor-Prüfungen angezeigt.

Nachdem die AWS Config-Regel Auswertungsergebnisse generiert hat, sehen Sie die Ergebnisse in Trusted Advisor nahezu in Echtzeit. Wenn Sie Probleme mit diesem Feature haben, erstellen Sie einen technischen Supportfall im AWS Support-Center.

Ich habe dieselbe verwaltete AWS Config-Regel zweimal bereitgestellt. Was wird in Trusted Advisor angezeigt?

In den Trusted Advisor-Prüfergebnissen werden für jede verwaltete Regel, die Sie installieren, separate Einträge angezeigt.

Ich habe die Aufnahme für AWS Config in einer AWS-Region deaktiviert. Was wird in Trusted Advisor angezeigt?

Wenn Sie die Ressourcenaufzeichnung für AWS Config in einer AWS-Region deaktiviert haben, erhält Trusted Advisor keine Daten mehr für entsprechende verwaltete Regeln und Prüfungen in dieser Region. Vorhandene verwaltete Regelergebnisse bleiben in AWS Config und in Trusted Advisor, bis AWS Config abläuft, basierend auf der Aufbewahrungsrichtlinie des Rekorders. Wenn Sie eine verwaltete Regel löschen, werden die Trusted Advisor-Prüfdaten in der Regel fast in Echtzeit gelöscht.

Anzeigen von AWS Security Hub Steuerelemente in AWS Trusted Advisor

Nachdem Sie aktiviert haben AWS Security Hub für Ihre AWS-Konto, können Sie Ihre Sicherheitskontrollen und deren Ergebnisse im Trusted Advisor console. Sie können Security Hub-Steuerelemente verwenden, um Sicherheitslücken in Ihrem Konto auf die gleiche Weise zu identifizieren, wie Sie Trusted Advisor Checks verwenden können. Sie können den Status der Überprüfung, die Liste der betroffenen Ressourcen anzeigen und dann den Empfehlungen des Security Hub folgen, um Ihre Sicherheitsprobleme zu beheben. Sie können diese Funktion verwenden, um Sicherheitsempfehlungen unter Trusted Advisor und Security Hub an einem günstigen Ort.

Hinweise

- Von Trusted Advisor aus können Sie alle Steuerelemente im Sicherheitsstandard AWS Foundational Security Best Practices anzeigen, mit Ausnahme der Steuerelemente der Kategorie Recover (Wiederherstellen) > Resilience (Resilienz). Eine Liste der unterstützten Steuerelemente finden Sie unter AWSFoundational Security Best Practices-Steuerelemente im AWS Security Hub-Benutzerhandbuch.

  Weitere Informationen zu den Security Hub-Kategorien finden Sie unter Kontrollkategorien.
- Derzeit, wenn Security Hub neue Steuerelemente zum Sicherheitsstandard AWSFoundational Security Best Practices hinzufügt, kann es zu einer Verzögerung von zwei bis vier Wochen kommen, bevor Sie sie in Trusted Advisor anzeigen können. Dieser Zeitrahmen ist das optimale Szenario und kann nicht garantiert werden.

Themen

Voraussetzungen

Folgende Anforderungen müssen erfüllt sein, damit Sie die Security Hub-Integration mit Trusted Advisor aktivieren können:

- Für diese Funktion benötigen Sie einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan. Sie können Ihren Supportplan im AWS Support-Center oder auf der Seite Supportpläne finden. Weitere Informationen finden Sie unter AWS Support-Pläne vergleichen.
- Sie müssen die Ressourcenaufzeichnung in AWS Config aktivieren, für die AWS-Regionen, die Sie für Ihre Security Hub-Steuerelemente wünschen. Weitere Informationen zur Konfiguration von SSH finden Sie unter Aktivieren und Konfigurieren von AWS Config.
- Sie müssen Security Hub aktivieren und AWSBest Practices für grundlegende Sicherheit v1.0.0 Sicherheitsstandard. Falls dies noch nicht geschehen ist, finden Sie weitere Informationen unter Einrichten von AWS Security Hub im AWS Security Hub-Benutzerhandbuch.

> **Note**
>
> Wenn Sie diese Voraussetzungen bereits erfüllt haben, können Sie mit Security Hub-Ergebnisse anzeigen fortfahren.

Informationen zu AWS Organizations-Konten

Wenn Sie die Voraussetzungen für ein Verwaltungskonto bereits erfüllt haben, wird diese Integration automatisch für alle Mitgliedskonten in Ihrer Organisation aktiviert. Einzelne Mitgliedskonten müssen sich nichtAWS Support kontaktieren, um diese Funktion zu aktivieren. Die Mitgliederkonten in Ihrer Organisation müssen jedoch Security Hub aktivieren, wenn sie ihre Ergebnisse in Trusted Advisor sehen wollen.

Wenn Sie diese Integration für ein bestimmtes Mitgliedskonto deaktivieren möchten, lesen Sie Deaktivieren Sie diese Funktion für AWS Organizations-Konten.

Security Hub-Ergebnisse anzeigen

Nachdem Sie Security Hub für Ihr Konto aktiviert haben, kann es bis zu 24 Stunden dauern, bis Ihre Security Hub-Ergebnisse in der Sicherheit-Seite der Trusted Advisor-Konsole.

Security Hub-Ergebnisse in Trusted Advisor anzeigen

1. Navigieren Sie zur Trusted AdvisorKonsole, und wählen Sie dann die Kategorie Sicherheit aus.
2. Im Feld Nach Schlüsselwort suchen den Namen oder die Beschreibung des Steuerelements in das Feld eingeben.

   > **Tip**
   >
   > Für Source können Sie AWS Security Hub wählen, um nach Security Hub-Steuerelementen zu filtern.

3. Wählen Sie den Security Hub-Steuerelement aus, um die folgenden Informationen anzuzeigen:

   - Beschreibung – Beschreibt, wie dieses Steuerelement Ihr Konto auf Sicherheitslücken überprüft.
   - Source – Ob die Prüfung von AWS Trusted Advisor oder AWS Security Hub kommt. Für Security Hub-Steuerelemente finden Sie die Steuerungs-ID.
   - Warnungskriterien – Der Status des Steuerelements. Wenn Security Hub beispielsweise ein wichtiges Problem erkennt, könnte der Status Rot: Kritisch oder Hoch sein.
   - Empfohlene Aktion – Verwenden Sie den Security Hub-Dokumentationslink, um die empfohlenen Schritte zur Behebung des Problems zu finden.
   - Security Hub-Ressourcen – Sie können die Ressourcen in Ihrem Konto finden, in dem Security Hub ein Problem festgestellt hat.

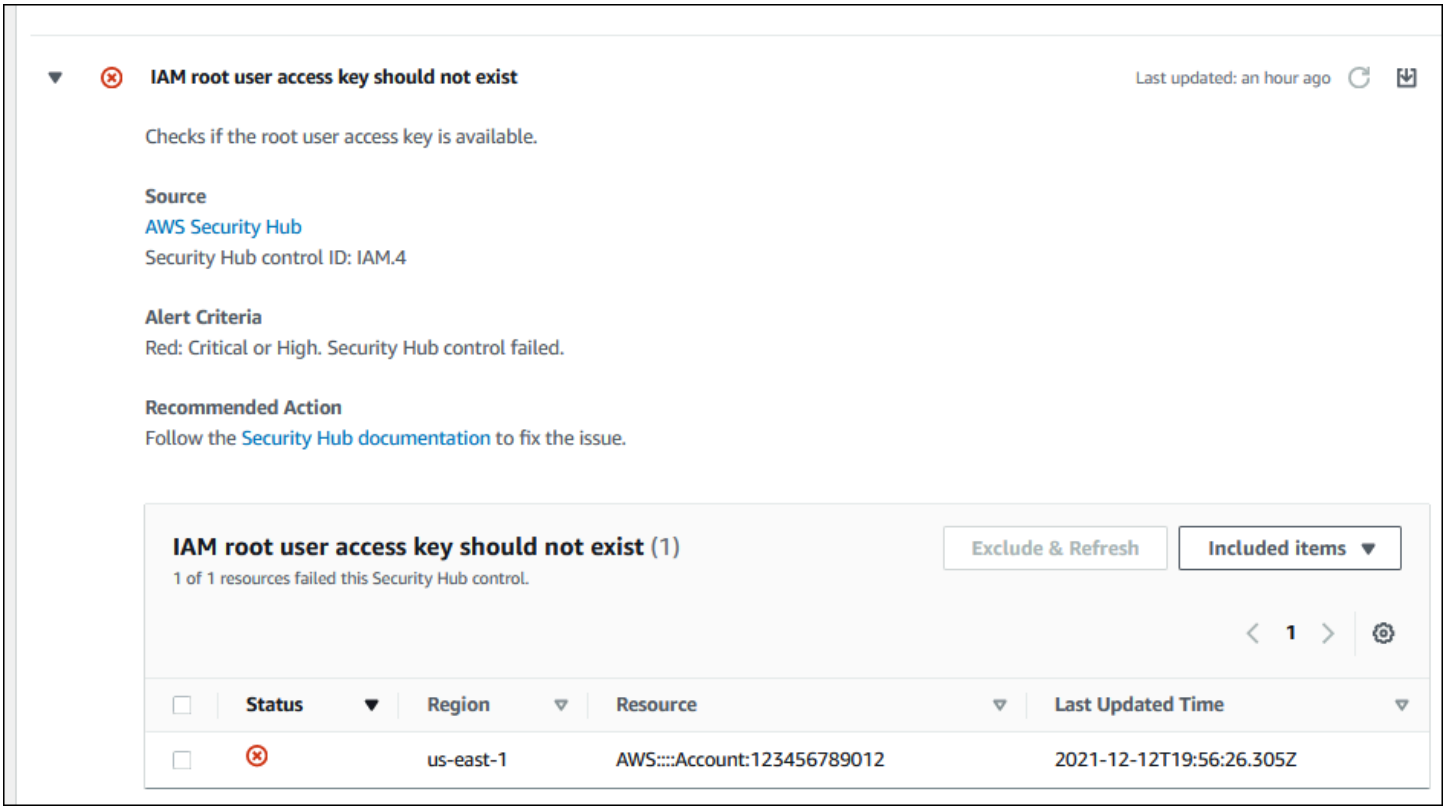
> **Hinweise**
>
> - Sie müssen Security Hub verwenden, um Ressourcen von Ihren Ergebnissen auszuschließen. Derzeit können Sie die Trusted Advisor-Konsole nicht zum Ausschließen

von Elementen aus Security Hub-Steuerelementen verwenden. Weitere Informationen finden Sie unter Festlegen des Workflow-Status für Ergebnisse.

- Die Funktion zur organisatorischen Ansicht unterstützt diese Integration mit Security Hub. Sie können Ihre Ergebnisse für Ihre Security Hub-Steuerelemente in Ihrem gesamten Unternehmen anzeigen und dann Berichte erstellen und herunterladen. Weitere Informationen finden Sie unter Organisationsansicht für AWS Trusted Advisor.

Example Beispiel: Security Hub Steuerelemente für IAM-Benutzerzugriffsschlüssel sollten nicht vorhanden sein

Im Folgenden finden Sie ein Beispiel für ein Security Hub-Steuerelement in der Trusted Advisor-Konsole.



Aktualisieren Sie Ihre Security Hub-Ergebnisse

Nachdem Sie einen Sicherheitsstandard aktiviert haben, kann es bis zu zwei Stunden dauern, bis Security Hub Ergebnisse für Ihre Ressourcen enthält. Es kann dann bis zu 24 Stunden dauern, bis diese Daten in der Trusted Advisor-Konsole erscheinen. Wenn Sie kürzlich den AWS-

Sicherheitsstandard Foundational Security Best Practices v1.0.0 aktiviert haben, überprüfen Sie die Trusted Advisor-Konsole später erneut.

> **Note**
>
> - Der Zeitplan zur Aktualisierung für jedes Security Hub-Steuerelement lautet regelmäßig oder von Änderungen ausgelöst. Derzeit können Sie weder die Trusted Advisor-Konsole noch die AWS Support-API verwenden, um Ihre Security Hub-Steuerungen zu aktualisieren. Weitere Informationen finden Sie unterZeitplan für die Ausführung von Sicherheitsprüfungen.
> - Sie müssen Security Hub verwenden, wenn Sie Ressourcen von Ihren Ergebnissen ausschließen möchten. Derzeit können Sie die Trusted Advisor-Konsole nicht zum Ausschließen von Elementen aus Security Hub-Steuerelementen verwenden. Weitere Informationen finden Sie unter Festlegen des Workflow-Status für Ergebnisse.

Deaktivieren Sie Security Hub von Trusted Advisor

Gehen Sie folgendermaßen vor, wenn Sie nicht möchten, dass Ihre Security Hub-Informationen in der Trusted Advisor-Konsole erscheint. Dieses Verfahren deaktiviert nur die Security Hub-Integration mit Trusted Advisor. Es wirkt sich nicht auf Ihre Konfigurationen mit Security Hub aus. Sie können weiterhin die Security Hub-Konsole verwenden, um Ihre Sicherheitskontrollen, Ressourcen und Empfehlungen anzuzeigen.

So deaktivieren Sie die Security Hub-Integration

1. Kontaktieren Sie AWS Support und beantragen Sie die Deaktivierung der Integration des Security Hub mit Trusted Advisor.

   Nachdem AWS Support diese Funktion deaktiviert hat, sendet Security Hub keine Daten mehr an Trusted Advisor. Ihre Security Hub-Daten werden von Trusted Advisor entfernt.
2. Wenn Sie diese Integration erneut aktivieren möchten, wenden Sie sich an AWS Support.

Deaktivieren Sie diese Funktion für AWS Organizations-Konten

Wenn Sie das vorherige Verfahren für ein Verwaltungskonto bereits abgeschlossen haben, wird die Security Hub-Integration automatisch aus allen Mitgliedskonten in Ihrer Organisation entfernt. Einzelne Mitgliedskonten in Ihrer Organisation müssen sich nicht separat an AWS Support wenden.

Wenn Sie ein Mitgliedskonto einer Organisation sind, können Sie sich an denAWS Support wenden, um diese Funktion nur von Ihrem Konto zu entfernen.

Fehlerbehebung

Wenn Sie Probleme mit dieser Integration haben, lesen Sie die folgenden Informationen zur Fehlerbehebung.

Inhalt

Ich sehe keine Ergebnisse von Security Hub in der Trusted Advisor-Konsole

Stellen Sie sicher, dass Sie die folgenden Schritte ausgeführt haben:

- Sie haben einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan.
- Sie haben die Ressourcenaufzeichnung in AWS Config in derselben Region wie Security Hub aktiviert.

- Sie haben Security Hub aktiviert und den Sicherheitsstandard AWS Foundational Security Best Practices v1.0.0 ausgewählt.
- Neue Steuerelemente von Security Hub werden als Überprüfungen in Trusted Advisor innerhalb von zwei bis vier Wochen hinzugefügt. Sehen Sie sich den Hinweis an.

Weitere Informationen hierzu finden Sie unter Voraussetzungen.

Ich habe Security Hub und AWS Config richtig konfiguriert und meine Ergebnisse fehlen immer noch

Es kann bis zu zwei Stunden dauern, bis Security Hub Ergebnisse für Ihre Ressourcen enthält. Es kann dann bis zu 24 Stunden dauern, bis diese Daten in der Trusted Advisor-Konsole erscheinen. Überprüfen Sie die Trusted Advisor-Konsolen Sie später erneut.

> **Hinweise**
>
> - Nur Ihre Ergebnisse für Kontrollen im AWS-Sicherheitsstandard Foundational Security Best Practices werden in Trusted Advisor angezeigt, außer für Kontrollen, die die Kategorie: Wiederherstellung > Widerstandsfähigkeit haben.
> - Wenn ein Dienstproblem mit Security Hub oder Security Hub nicht verfügbar ist, kann es bis zu 24 Stunden dauern, bis Ihre Ergebnisse in Trusted Advisor erscheinen. Überprüfen Sie die Trusted Advisor-Konsolen Sie später erneut.

Ich möchte bestimmte Security-Hub-Steuerelemente deaktivieren

Security Hub sendet Ihre Daten automatisch an Trusted Advisor. Wenn Sie ein Security Hub-Steuerelement deaktivieren oder keine Ressourcen mehr für dieses Steuerelement haben, werden Ihre Ergebnisse nicht in Trusted Advisor erscheinen.

Sie können sich bei der Security Hub-Konsole anmelden und überprüfen, ob Ihre Kontrolle aktiviert oder deaktiviert ist.

Wenn Sie ein Security-Hub-Steuerelement deaktivieren oder alle Steuerelemente für den Sicherheitsstandard AWS Foundational Security Best Practices deaktivieren möchten, werden Ihre Ergebnisse werden innerhalb der nächsten fünf Tage archiviert. Diese fünftägige Archivierungsfrist ist nur eine ungefähre Angabe, die nach besten Kräften bereitgestellt wird und nicht garantiert werden kann. Wenn Ihre Ergebnisse archiviert wurden, werden sie aus Trusted Advisor entfernt.

Weitere Informationen finden Sie unter den folgenden Themen:

- Deaktivieren und Aktivieren einzelner Steuerelemente
- Deaktivieren oder Aktivieren eines Sicherheitsstandards

Ich möchte meine ausgeschlossenen Security Hub-Ressourcen finden

Aus der Trusted Advisor-Konsole können Sie den Namen Ihres Security Hub-Steuerelements auswählen und dann die Option Ausgeschlossene Artikel. Diese Option zeigt alle Ressourcen an, die in Security Hub unterdrückt werden.

Wenn der Workflow-Status einer Ressource auf `SUPPRESSED` festgelegt ist, dann ist diese Ressource ein ausgeschlossenes Element in Trusted Advisor. Sie können die Ressourcen des Security Hubs nicht von der Trusted Advisor-Konsole aus unterdrücken. Verwenden Sie dazu die Security Hub-Konsole. Weitere Informationen finden Sie unter Festlegen des Workflow-Status für Ergebnisse.

Ich möchte diese Funktion für ein Mitgliedskonto aktivieren oder deaktivieren, das zu einer AWS-Organisation gehört

Standardmäßig erben Mitgliedskonten das Feature vom Verwaltungskonto für AWS Organizations. Wenn das Verwaltungskonto die Funktion aktiviert hat, verfügen alle Konten in der Organisation ebenfalls über diese Funktion. Wenn Sie über ein Mitgliedskonto verfügen und spezifische Änderungen für Ihr Konto vornehmen möchten, müssen Sie sich an den AWS Support wenden.

Ich sehe mehrere AWS-Regionen für dieselbe betroffene Ressource für eine Security-Hub-Prüfung

Einige AWS-Services sind global und nicht spezifisch für eine Region, wie z. B. IAM und Amazon CloudFront. Globale Ressourcen wie Amazon-S3-Buckets werden standardmäßig in der Region USA Ost (Nord-Virginia) angezeigt.

Bei Security-Hub-Prüfungen, die Ressourcen für globale Services auswerten, sehen Sie möglicherweise mehr als ein Element für betroffene Ressourcen. Wenn zum Beispiel die `Hardware MFA should be enabled for the root user`-Prüfung ergibt, dass Ihr Konto diese Funktion nicht aktiviert hat, sehen Sie mehrere Regionen für dieselbe Ressource in der Tabelle.

Sie können Security Hub und AWS Config konfigurieren, damit nicht mehrere Regionen für dieselbe Ressource angezeigt werden. Weitere Informationen finden Sie unter AWS Foundational

Best Practices controls that you might want to disable (AWS Foundational Best Practices für Steuerelemente, die Sie möglicherweise deaktivieren möchten).

Ich habe Security Hub AWS Config in einer Region deaktiviert

Wenn Sie die Ressourcenaufzeichnung mit AWS Config beenden oder Security Hub in einer AWS-Region deaktivieren, empfängt Trusted Advisor in dieser Region keine Daten für Steuerelemente mehr. Trusted Advisor entfernt Ihre Security-Hub-Ergebnisse innerhalb von 7–9 Tagen. Dieser Zeitrahmen ist das optimale Szenario und kann nicht garantiert werden. Weitere Informationen finden Sie unter Deaktivieren von Security Hub.

Wenn Sie diese Funktion für Ihr Konto deaktivieren möchten, finden Sie weitere Informationen unter Deaktivieren Sie Security Hub von Trusted Advisor.

Mein Steuerelement ist in Security Hub archiviert, aber ich sehe die Ergebnisse immer noch in Trusted Advisor

Wenn sich der `RecordState`-Status eines Ergebnisses zu `ARCHIVED` ändert, löscht Trusted Advisor das Ergebnis für dieses Security-Hub-Steuerelement aus Ihrem Konto. Möglicherweise sehen Sie den Befund noch bis zu 7-9 Tage in Trusted Advisor, bevor er gelöscht wird. Dieser Zeitrahmen ist das optimale Szenario und kann nicht garantiert werden.

Ich kann meine Security Hub-Ergebnisse immer noch nicht einsehen

Wenn Sie immer noch Probleme mit diesem Tutorial haben, können Sie einen technischen Support-Fall im AWS Support-Center erstellen.

Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an

Compute Optimizer ist ein Service, der die Konfigurations- und Auslastungsmetriken Ihrer AWS -Ressourcen analysiert. Dieser Service berichtet , ob Ihre Ressourcen für Effizienz und Zuverlässigkeit korrekt konfiguriert sind. Er schlägt auch Verbesserungen vor, die Sie implementieren können, um die Workload-Leistung zu verbessern. Mit Compute Optimizer sehen Sie dieselben Empfehlungen in Ihren Trusted Advisor Checks.

Sie können sich entweder für Ihr AWS-Konto einziges Konto oder für alle Mitgliedskonten entscheiden, die Teil einer Organisation sind. AWS Organizations Weitere Informationen finden Sie unter Erste Schritte im AWS Compute Optimizer -Benutzerhandbuch.

Sobald Sie sich für Compute Optimizer entschieden haben, erhalten die folgenden Prüfungen Daten von Ihren Lambda-Funktionen und Amazon-EBS-Volumes. Es kann bis zu 12 Stunden dauern, bis die Ergebnisse und Optimierungsempfehlungen erstellt werden. Es kann dann bis zu 48 Stunden dauern, bis Ihre Ergebnisse Trusted Advisor für die folgenden Prüfungen angezeigt werden:

Kostenoptimierung

- Amazon EBS mit nicht ausgelasteten Volumes
- AWS Lambda aufgrund der Speichergröße überdimensionierte Funktionen

Leistung

- Amazon EBS mit überlasteten Volumes
- AWS Lambda Funktionen, die im Hinblick auf die Speichergröße nicht ausreichend zur Verfügung stehen

Hinweise

- Die Ergebnisse für diese Prüfungen werden mehrmals täglich automatisch aktualisiert. Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.
- Trusted Advisor hat bereits die Prüfungen „Amazon EBS Volumes nicht ausgelastet“ und „Amazon EBS Magnetic Volumes überlastet“.

  Sobald Sie sich bei Compute Optimizer angemeldet haben, empfehlen wir Ihnen, stattdessen die neuen Überprüfungen für überlastete Amazon-EBS-Volumes und nicht ausgelastete Amazon-EBS-Volumes zu verwenden.

Ähnliche Informationen

Weitere Informationen finden Sie unter den folgenden Themen:

- Anzeigen von Amazon-EBS-Volume-Empfehlungen im AWS Compute Optimizer - Benutzerhandbuch
- Anzeigen von Lambda-Funktions-Empfehlungen im AWS Compute Optimizer -Benutzerhandbuch

- Konfigurieren des Lambda-Funktionsspeichers im AWS Lambda Entwicklerhandbuch
- Fordern Sie Änderungen an Ihren Amazon EBS-Volumes im Amazon EC2 EC2-Benutzerhandbuch an

Erste Schritte mit der AWS Trusted Advisor-Priorität

Die Trusted Advisor-Priorität hilft Ihnen, Ihr AWS-Konto zu sichern und zu optimieren, damit Sie die bewährten Methoden von AWS befolgen können. Mit der Trusted Advisor-Priorität kann Ihr AWS-Konto-Team Ihr Konto proaktiv überwachen und priorisierte Empfehlungen erstellen, wenn es Möglichkeiten für Sie identifiziert.

So kann Ihr Kontoteam beispielsweise feststellen, wenn Ihr Root-Benutzer des AWS-Kontos nicht über eine Multi-Faktor-Authentifizierung (MFA) verfügt. Ihr Kontoteam kann eine Empfehlung erstellen, damit Sie bei einer Prüfung, wie z. B. `MFA on Root Account`, sofort handeln können. Die Empfehlung wird als aktive priorisierte Empfehlung auf der Seite der Trusted Advisor-Priorität der Trusted Advisor-Konsole angezeigt. Sie befolgen dann die Empfehlungen zu ihrer Auflösung.

Trusted Advisor Priority-Empfehlungen stammen aus diesen beiden Quellen:

- AWS-Services – Services wie Trusted Advisor, AWS Security Hub, und AWS Well-Architected erstellen automatisch Empfehlungen. Ihr Kontoteam gibt diese Empfehlungen für Sie frei, damit diese Empfehlungen in der Trusted Advisor Priority sichtbar sind.
- Ihrem Kontoteam – Ihr Kontoteam kann manuelle Empfehlungen erstellen.

Die Trusted Advisor-Priorität hilft Ihnen, sich auf die wichtigsten Empfehlungen zu konzentrieren. Sie und Ihr Kontoteam können den Lebenszyklus der Empfehlung überwachen, von dem Zeitpunkt an, an dem Ihr Kontoteam die Empfehlung freigegeben hat, bis zu dem Zeitpunkt, an dem Sie die Empfehlung bestätigen, auflösen oder ablehnen. Sie können die Trusted Advisor-Priorität verwenden, um Empfehlungen für alle Mitgliedskonten in Ihrer Organisation zu finden.

Themen

- Eine Empfehlung lösen
- Eine Empfehlung wieder aufnehmen
- Empfehlungsdetails herunterladen
- Registrieren von delegierten Administratoren
- Abmelden eines delegierten Administrators
- Verwalten von Benachrichtigungen der Trusted Advisor-Priorität
- Deaktivieren der Trusted Advisor-Priorität

Voraussetzungen

Um die Trusted Advisor Priority verwenden zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über einen Enterprise-Supportplan verfügen.
- Ihr Konto muss Teil einer Organisation sein, die alle Funktionen in AWS Organizations aktiviert hat. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.
- Ihre Organisation muss vertrauenswürdigen Zugriff auf Trusted Advisor aktiviert haben. Um den vertrauenswürdigen Zugriff zu aktivieren, melden Sie sich als Verwaltungskonto an. Öffnen Sie in der Trusted Advisor-Konsole die Seite Ihre Organisation.
- Sie müssen bei Ihrem AWS-Konto angemeldet sein, um Trusted Advisor-Prioritätsempfehlungen für Ihr Konto anzeigen zu können.
- Sie müssen beim Verwaltungskonto der Organisation oder bei einem delegierten Administratorkonto angemeldet sein, um aggregierte Empfehlungen in Ihrer Organisation anzeigen zu können. Anweisungen zur Registrierung delegierter Administratorkonten finden Sie unter Registrieren von delegierten Administratoren.
- Sie müssen über AWS Identity and Access Management (IAM)-Berechtigungen verfügen, um auf die Trusted Advisor-Priorität zugreifen zu können. Weitere Informationen zum Steuern des Zugriffs auf die Trusted Advisor Priority finden Sie unter Zugriff verwalten auf AWS Trusted Advisor und AWS verwaltete Richtlinien für AWS Trusted Advisor.

Aktivieren der Trusted Advisor-Priorität

Bitten Sie Ihr Kontoteam, dieses Feature für Sie zu aktivieren. Sie müssen über einen Enterprise Support-Plan verfügen und der Eigentümer des Verwaltungskontos für Ihre Organisation sein. Wenn auf der Seite „Trusted Advisor Priority“ in der Konsole angegeben ist, dass Sie vertrauenswürdigen Zugriff mit AWS Organizations benötigen, wählen Sie die Option Vertrauenswürdigen Zugriff mit AWS Organizations ermöglichen aus. Weitere Informationen finden Sie im Abschnitt Voraussetzungen.

Anzeigen von priorisierten Empfehlungen

Sobald Ihr Kontoteam die Trusted Advisor Priority für Sie aktiviert hat, können Sie die neuesten Empfehlungen für Ihr AWS-Konto anzeigen.

So zeigen Sie Ihre priorisierten Empfehlungen an

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Seite Trusted Advisor Priority können Sie Folgendes anzeigen:

   Wenn Sie ein AWS Organizations-Management- oder delegiertes Administratorkonto verwenden, wechseln Sie zur Registerkarte Mein Konto.

   - Actions needed (Erforderliche Aktionen) – die Anzahl der Empfehlungen, für die noch keine Antwort vorliegt oder die noch in Bearbeitung sind.
   - Overview (Übersicht) – die folgenden Informationen:
     - Verworfene Empfehlungen in den letzten 90 Tagen
     - Gelöste Empfehlungen in den letzten 90 Tagen
     - Empfehlungen ohne Aktualisierung in über 30 Tagen
     - Durchschnittliche Zeit zur Lösung von Empfehlungen
3. Auf der Registerkarte Aktiv werden unter Aktive priorisierte Empfehlungen die Empfehlungen angezeigt, die Ihr Kontoteam für Sie priorisiert hat. Auf der Registerkarte Closed (Geschlossen) werden aufgelöste oder verworfene Empfehlungen angezeigt.

   - Verwenden Sie die folgenden Optionen, um Ihre Ergebnisse zu filtern:

     - Recommendation (Empfehlung) – Geben Sie Schlüsselwörter ein, um nach Namen zu suchen. Dies kann ein Prüfungsname oder ein benutzerdefinierter Name sein, den Ihr Kontoteam erstellt hat.

- Status – ob für die Empfehlung noch eine Antwort aussteht, diese in Bearbeitung ist, verworfen oder aufgelöst wurde.
- Source (Quelle) – Der Ursprung einer priorisierten Empfehlung. Die Empfehlung kann von AWS-Services, Ihrem AWS-Konto-Team oder einem geplanten Service-Ereignis stammen.
- Category (Kategorie) – Die Empfehlungskategorie wie Sicherheit oder Kostenoptimierung.
- Age (Alter) – Zeitpunkt, an dem Ihr Kontoteam die Empfehlung für Sie freigegeben hat.

4. Wählen Sie eine Empfehlung aus, um mehr über deren Details, die betroffenen Ressourcen und die empfohlenen Maßnahmen zu erfahren. Sie können die Empfehlung dann bestätigen oder verwerfen.

So zeigen Sie priorisierte Empfehlungen für alle Konten in Ihrer AWS-Organisation an

Sowohl das Verwaltungskonto als auch die delegierten Administratoren für Trusted Advisor Priority können die in Ihrem Unternehmen aggregierten Empfehlungen einsehen.

> **Note**
>
> Mitgliedskonten haben keinen Zugriff auf aggregierte Empfehlungen.

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Seite Trusted Advisor-Priorität müssen Sie sich auf der Registerkarte Meine Organisation befinden.
3. Wählen Sie ein Konto aus der Dropdown-Liste Konto Ihrer Organisation auswählen aus, um Empfehlungen für ein Konto anzuzeigen. Alternativ können Sie Empfehlungen für alle Ihre Konten anzeigen.

   Auf der Registerkarte Meine Organisation können Sie die folgenden Elemente anzeigen:

   - Erforderliche Aktionen: Die Anzahl der Empfehlungen für ihre Organisation, für die noch keine Antwort vorliegt oder die noch in Bearbeitung sind.
   - Übersicht: Zeigt die folgenden Elemente an:

     – Verworfene Empfehlungen in den letzten 90 Tagen

– Gelöste Empfehlungen in den letzten 90 Tagen

– Empfehlungen ohne Aktualisierung in über 30 Tagen

– Durchschnittliche Zeit zur Lösung von Empfehlungen

4. Auf der Registerkarte Aktiv werden im Abschnitt Aktive priorisierte Empfehlungen die Empfehlungen angezeigt, die Ihr Kontoteam für Sie priorisiert hat. Auf der Registerkarte Closed (Geschlossen) werden aufgelöste oder verworfene Empfehlungen angezeigt.

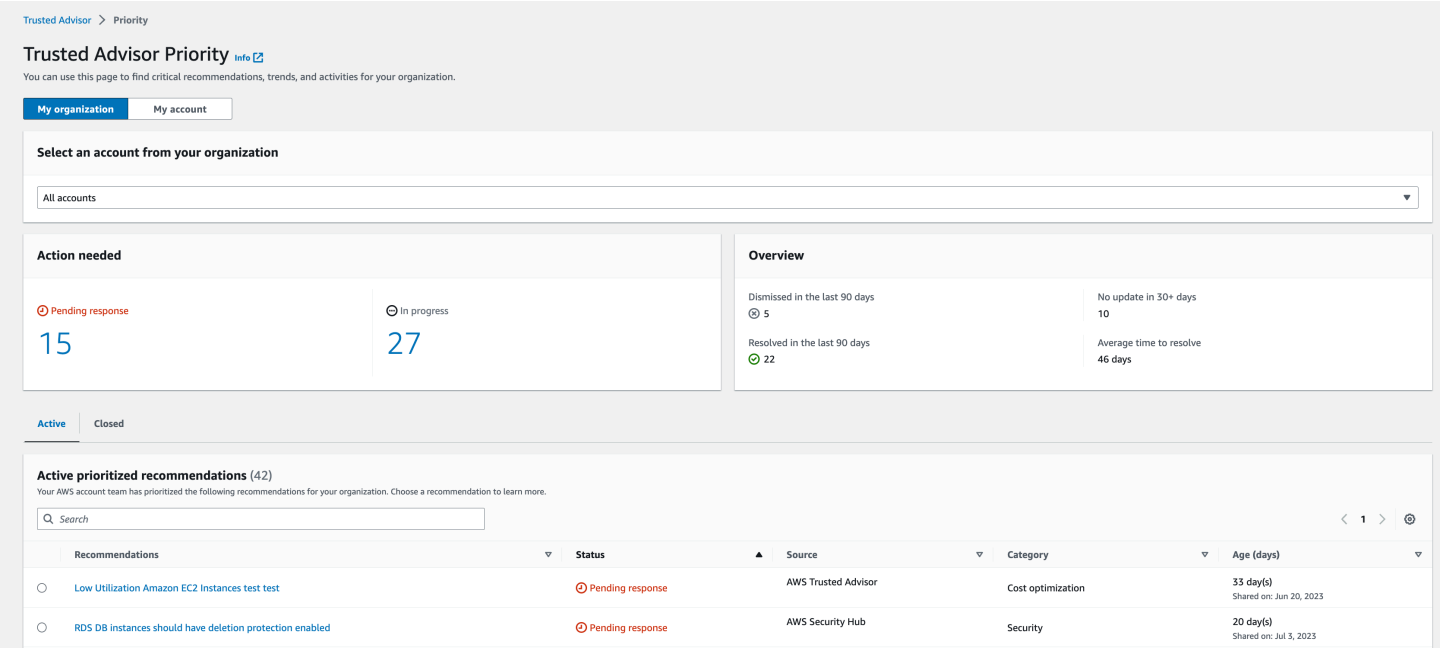
   Verwenden Sie die folgenden Optionen, um Ihre Ergebnisse zu filtern:

   - Recommendation (Empfehlung) – Geben Sie Schlüsselwörter ein, um nach Namen zu suchen. Dies kann entweder ein Prüfungsname oder ein benutzerdefinierter Name sein, den Ihr Kontoteam erstellt hat.
   - Status – ob für die Empfehlung noch eine Antwort aussteht, diese in Bearbeitung ist, verworfen oder aufgelöst wurde.
   - Source (Quelle) – Der Ursprung einer priorisierten Empfehlung. Die Empfehlung kann von AWS-Services, Ihrem AWS-Konto-Team oder einem geplanten Service-Ereignis stammen.
   - Category (Kategorie) – Die Empfehlungskategorie wie Sicherheit oder Kostenoptimierung.
   - Age (Alter) – Zeitpunkt, an dem Ihr Kontoteam die Empfehlung für Sie freigegeben hat.

5. Wählen Sie eine Empfehlung aus, um zusätzliche Details, betroffene Konten und Ressourcen sowie die empfohlenen Maßnahmen anzuzeigen. Sie können die Empfehlung dann bestätigen oder verwerfen.

Example : Trusted Advisor-Prioritätsempfehlungen

Das folgende Beispiel zeigt 15 Empfehlungen, deren Antwort noch aussteht, und 27 Empfehlungen, die im Abschnitt Aktion erforderlich in Bearbeitung sind. Die folgende Abbildung zeigt zwei der Empfehlungen, deren Antwort noch aussteht, auf der Registerkarte Aktive priorisierte Empfehlungen.



Bestätigen einer Empfehlung

Auf der Registerkarte Active (Aktiv) können Sie mehr über die Empfehlung erfahren und dann entscheiden, ob Sie sie bestätigen möchten.

Bestätigen Sie eine Empfehlung wie folgt:

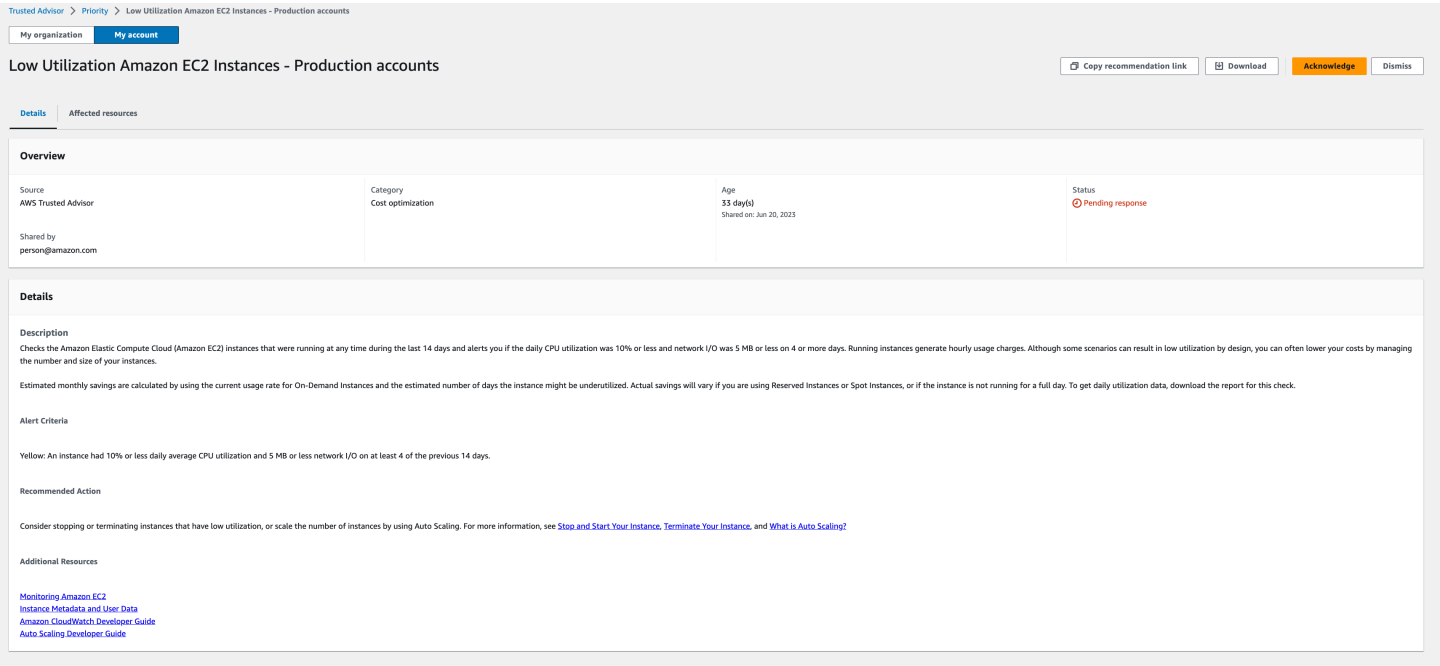
1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wenn Sie ein AWS Organizations-Management- oder delegiertes Administratorkonto verwenden, wechseln Sie zur Registerkarte Mein Konto.
3. Wählen Sie auf der Seite Trusted Advisor Priority (-Priorität) unter der Registerkarte Active (Aktiv) einen Empfehlungsnamen aus.
4. Im Abschnitt Details können Sie die empfohlenen Aktionen zum Lösen der Empfehlung überprüfen.
5. Im Abschnitt Betroffene Ressourcen können Sie die betroffenen Ressourcen überprüfen und nach Status filtern.
6. Wählen Sie Acknowledge (Bestätigen).
7. Wählen Sie im Dialogfeld Acknowledge recommendation (Empfehlung bestätigen) die Option Acknowledge (Bestätigen) aus.

Der Empfehlungsstatus ändert sich in In progress (In Bearbeitung). Empfehlungen, die in Bearbeitung sind oder auf eine Antwort warten, werden auf der Registerkarte Active (Aktiv) auf der Seite Trusted Advisor-Priorität angezeigt.

8. Führen Sie die empfohlenen Aktionen aus, um die Empfehlung aufzulösen. Weitere Informationen finden Sie unter Eine Empfehlung lösen.

Example : Manuelle Empfehlung der Trusted Advisor-Priorität

Das folgende Image zeigt die Empfehlung für EC2-Instances mit niedriger Auslastung, für die eine Antwort aussteht.



So bestätigen Sie eine Empfehlung für alle Konten in Ihrer AWS-Organisation

Das Verwaltungskonto oder die vom Trusted Advisor delegierten Administratoren können eine Empfehlung für alle betroffenen Konten bestätigen.

> **Note**
>
> Mitgliedskonten haben keinen Zugriff auf aggregierte Empfehlungen.

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.

2. Auf der Seite Trusted Advisor-Priorität müssen Sie sich auf der Registerkarte Meine Organisation befinden.
3. Wählen Sie auf der Registerkarte Aktiv einen Empfehlungsnamen aus.
4. Wählen Sie Acknowledge (Bestätigen).
5. Wählen Sie im Dialogfeld Acknowledge recommendation (Empfehlung bestätigen) die Option Acknowledge (Bestätigen) aus.

   Der Empfehlungsstatus ändert sich in In progress (In Bearbeitung).
6. Führen Sie die empfohlenen Aktionen aus, um die Empfehlung aufzulösen. Weitere Informationen finden Sie unter Eine Empfehlung lösen.
7. Wählen Sie den Empfehlungsnamen aus, um die Empfehlungsdetails anzuzeigen.

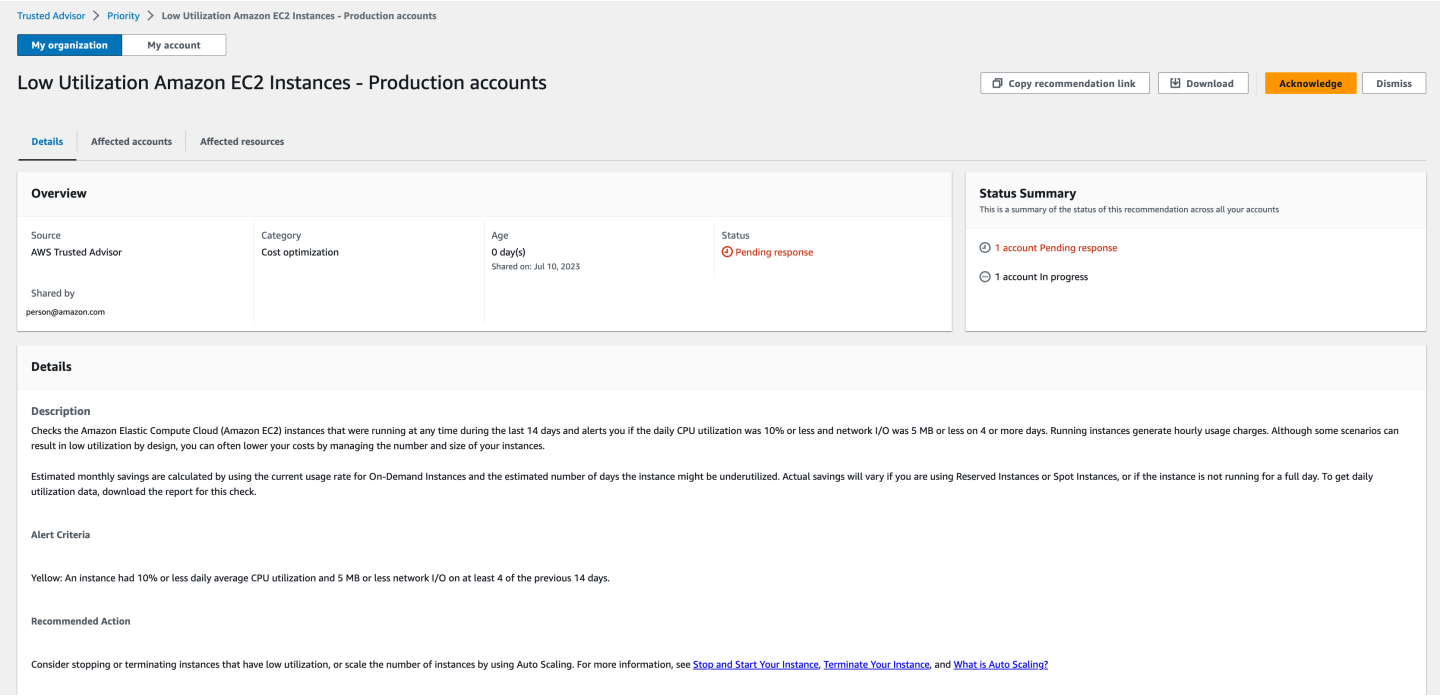
   Im Abschnitt Details können Sie die folgenden Informationen zur Empfehlung überprüfen:

   - Eine Übersicht über die Empfehlung und ein Abschnitt mit Details zu den Maßnahmen, die im Rahmen der Empfehlung durchzuführen sind.

     Eine Status-Übersicht mit Empfehlungen für alle betroffenen Konten.
   - Im Abschnitt Betroffene Konten können Sie die betroffenen Ressourcen für all Ihre Konten überprüfen. Sie können nach Kontonummer und Status filtern.
   - Im Abschnitt Betroffene Ressourcen können Sie die betroffenen Ressourcen für all Ihre Konten überprüfen. Sie können nach Kontonummer und Status filtern.

Example : Manuelle Empfehlung der Trusted Advisor-Priorität

Das folgende Image zeigt die Empfehlung für Amazon-EC2-Instances mit niedriger Auslastung, für die eine Antwort aussteht. Ein betroffenes Konto hat die Empfehlung bestätigt. Bei einem anderen Konto steht eine Antwort aus, sodass der Empfehlungsstatus Antwort ausstehend lautet.



Verwerfen einer Empfehlung

Sie können eine Empfehlung auch verwerfen. Das bedeutet, dass Sie die Empfehlung bestätigen, sie aber nicht umsetzen werden. Sie können eine Empfehlung verwerfen, wenn sie für Ihr Konto nicht relevant ist. Wenn Sie beispielsweise ein Test-AWS-Konto haben, das Sie löschen möchten, müssen Sie die empfohlenen Aktionen nicht ausführen.

Verwerfen Sie eine Empfehlung wie folgt:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wenn Sie ein AWS Organizations-Management- oder delegiertes Administratorkonto verwenden, wechseln Sie zur Registerkarte Mein Konto.
3. Wählen Sie auf der Seite Trusted Advisor Priority (-Priorität) unter der Registerkarte Active (Aktiv) einen Empfehlungsnamen aus.
4. Überprüfen Sie auf der Detailseite der Empfehlung die Informationen zu den betroffenen Ressourcen.
5. Wenn diese Empfehlung nicht auf Ihr Konto zutrifft, wählen Sie Dismiss (Verwerfen).
6. Wählen Sie im Dialogfeld Dismiss recommendation (Empfehlung verwerfen) einen Grund aus, warum Sie die Empfehlung nicht umsetzen werden.

7. (Optional) Geben Sie einen Hinweis ein, warum Sie die Empfehlung verwerfen. Wenn Sie Other (Andere) wählen, müssen Sie im Abschnitt Note (Hinweis) eine Beschreibung eingeben.
8. Wählen Sie Dismiss (Verwerfen). Der Status der Empfehlung ändert sich in Dismissed (Verworfen) und wird auf der Registerkarte Closed (Geschlossen) auf der Seite „Trusted Advisor Priority“ angezeigt.

So verwerfen Sie eine Empfehlung für alle Konten in Ihrer AWS-Organisation

Das Verwaltungskonto oder delegierte Administratoren von Trusted Advisor Priority können eine Empfehlung für alle Konten verwerfen.

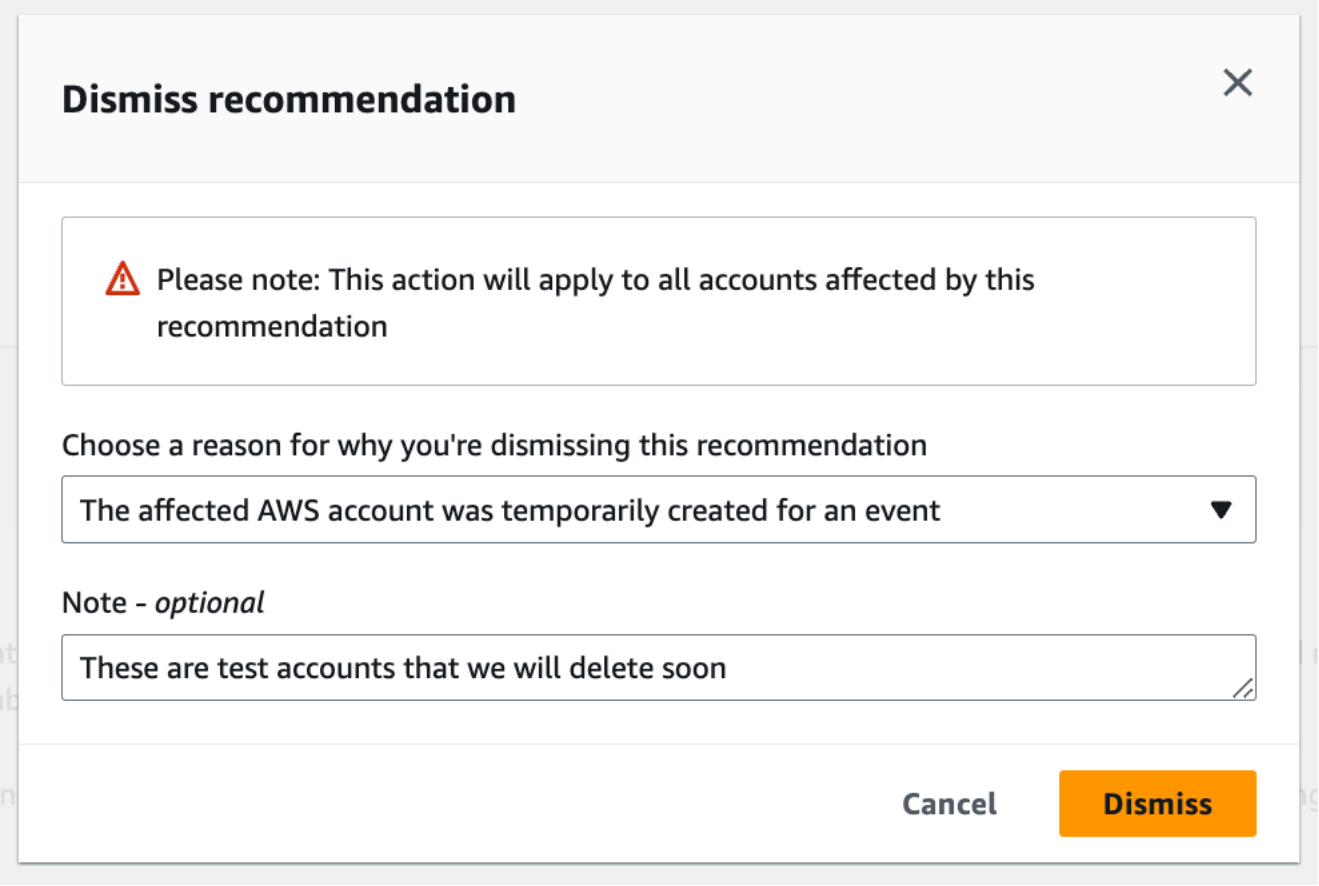
1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Seite Trusted Advisor-Priorität müssen Sie sich auf der Registerkarte Meine Organisation befinden.
3. Wählen Sie auf der Registerkarte Aktiv einen Empfehlungsnamen aus.
4. Wenn diese Empfehlung nicht auf Ihr Konto zutrifft, wählen Sie Verwerfen.
5. Wählen Sie im Dialogfeld Dismiss recommendation (Empfehlung verwerfen) einen Grund aus, warum Sie die Empfehlung nicht umsetzen werden.
6. (Optional) Geben Sie einen Hinweis ein, warum Sie die Empfehlung verwerfen. Wenn Sie Andere wählen, müssen Sie im Abschnitt Hinweis eine Beschreibung eingeben.
7. Wählen Sie Dismiss (Verwerfen). Der Empfehlungsstatus ändert sich in Verworfen. Die Empfehlung wird auf der Registerkarte Abgeschlossen auf der Seite „Trusted Advisor Priority“ angezeigt.

> **Note**
>
> Sie können den Namen einer Empfehlung und View note (Notiz anzeigen) wählen, um den Grund für das Verwerfen zu finden. Wenn Ihr Kontoteam die Empfehlung für Sie verworfen hat, wird die entsprechende E-Mail-Adresse neben der Notiz angezeigt.

Trusted Advisor Priority benachrichtigt auch Ihr Kontoteam, dass Sie die Empfehlung verworfen haben.

Example : Verwerfen einer Empfehlung von Trusted Advisor Priority

Das folgende Beispiel zeigt, wie Sie eine Empfehlung verwerfen können.



Eine Empfehlung lösen

Nachdem Sie die Empfehlung bestätigt und die empfohlenen Aktionen abgeschlossen haben, können Sie die Empfehlung auflösen.

> **Tip**
>
> Nachdem Sie eine Empfehlung aufgelöst haben, können Sie sie nicht wieder öffnen. Wenn Sie die Empfehlung später wieder aufgreifen möchten, finden Sie weitere Informationen unter Verwerfen einer Empfehlung.

So lösen Sie eine Empfehlung

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.

2. Auf der Seite Trusted Advisor-Priorität müssen Sie sich auf der Registerkarte Meine Organisation befinden.
3. Auf der Seite Trusted Advisor-Priorität wählen Sie die Empfehlung und dann Resolve (Lösen).
4. Wählen Sie im Dialogfeld Resolve recommendation (Empfehlung auflösen) die Option Resolve (Auflösen). Gelöste Empfehlungen werden unter der Registerkarte Closed (Abgeschlossen) auf der Seite der Trusted Advisor-Priorität angezeigt. Trusted Advisor Die Priorität benachrichtigt Ihr Kontoteam, dass Sie die Empfehlung gelöst haben.

So lösen Sie eine Empfehlung für alle Konten in Ihrer AWS-Organisation

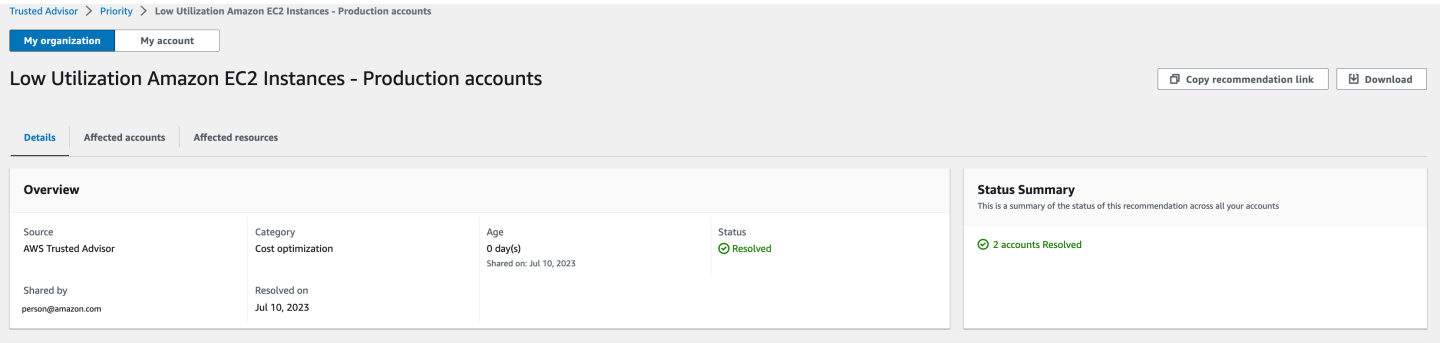
Das Verwaltungskonto oder delegierte Administratoren von Trusted Advisor Priority können eine Empfehlung für alle Konten lösen.

> **Note**
>
> Mitgliedskonten haben keinen Zugriff auf aggregierte Empfehlungen.

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wenn Sie ein AWS Organizations-Management- oder delegiertes Administratorkonto verwenden, wechseln Sie zur Registerkarte Mein Konto.
3. Wählen Sie auf der Registerkarte Aktiv einen Empfehlungsnamen aus.
4. Wenn die Empfehlung nicht auf Ihr Konto zutrifft, wählen Sie Lösen.
5. Wählen Sie im Dialogfeld Resolve recommendation (Empfehlung auflösen) die Option Resolve (Auflösen). Gelöste Empfehlungen werden unter der Registerkarte Closed (Abgeschlossen) auf der Seite der Trusted Advisor-Priorität angezeigt. Trusted Advisor Die Priorität benachrichtigt Ihr Kontoteam, dass Sie die Empfehlung gelöst haben.

Example : Manuelle Empfehlung der Trusted Advisor-Priorität

Das folgende Beispiel zeigt eine aufgelöste Empfehlung für Amazon-EC2-Instances mit niedriger Auslastung.



Eine Empfehlung wieder aufnehmen

Nachdem Sie eine Empfehlung verworfen haben, können Sie oder Ihr Kontoteam die Empfehlung wieder öffnen.

Nehmen Sie eine Empfehlung wieder auf wie folgt

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wenn Sie ein AWS Organizations-Management- oder delegiertes Administratorkonto verwenden, wechseln Sie zur Registerkarte Mein Konto.
3. Wählen Sie auf der Seite Trusted Advisor Priority (-Priorität) die Registerkarte Closed (Abgeschlossen).
4. Wählen Sie unter Closed recommendations (Geschlossene Empfehlungen) die verworfene Empfehlung und dann Reopen (Erneut öffnen) aus.
5. Beschreiben Sie im Dialogfeld Reopen recommendation (Empfehlung erneut öffnen), warum Sie die Empfehlung erneut öffnen.
6. Wählen Sie Reopen (Wieder aufnehmen) aus. Der Status der Empfehlung ändert sich in In progress (In Bearbeitung) und wird auf der Registerkarte Active (Aktiv) angezeigt.

> **Tip**
>
> Sie können den Namen einer Empfehlung und dann Notiz anzeigen wählen, um den Grund für das erneute Öffnen zu finden. Wenn Ihr Kontoteam die Empfehlung für Sie erneut geöffnet hat, wird der entsprechende Name neben der Notiz angezeigt.

7. Befolgen Sie die Schritte in den Empfehlungsdetails.

So öffnen Sie eine Empfehlung für alle Konten in Ihrer AWS-Organisation erneut

Das Verwaltungskonto oder die delegierten Administratoren von Trusted Advisor Priority können eine Empfehlung für alle Konten erneut öffnen.

> **Note**
>
> Mitgliedskonten haben keinen Zugriff auf aggregierte Empfehlungen.

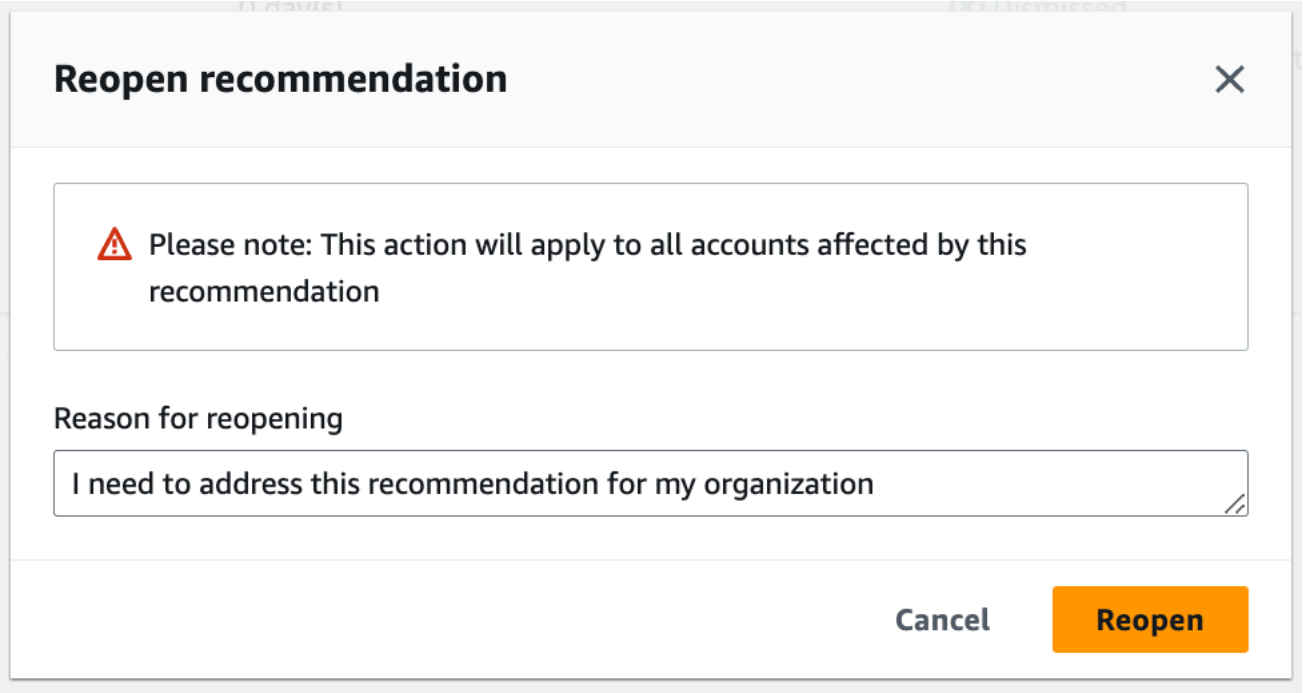
1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Seite Trusted Advisor-Priorität müssen Sie sich auf der Registerkarte Meine Organisation befinden.
3. Wählen Sie unter Closed recommendations (Geschlossene Empfehlungen) die verworfene Empfehlung und dann Reopen (Erneut öffnen) aus.
4. Beschreiben Sie im Dialogfeld Reopen recommendation (Empfehlung erneut öffnen), warum Sie die Empfehlung erneut öffnen.
5. Wählen Sie Reopen (Wieder aufnehmen) aus. Der Status der Empfehlung ändert sich in In progress (In Bearbeitung) und wird auf der Registerkarte Active (Aktiv) angezeigt.

   > **Tip**
   >
   > Sie können den Namen einer Empfehlung und View note (Notiz anzeigen) wählen, um den Grund für das erneute Öffnen zu finden. Wenn Ihr Kontoteam die Empfehlung für Sie erneut geöffnet hat, wird der entsprechende Name neben der Notiz angezeigt.

6. Befolgen Sie die Schritte in den Empfehlungsdetails.

Example : Wiederaufnahme einer Empfehlung über die Trusted Advisor-Priorität

Das folgende Beispiel zeigt eine Empfehlung, die Sie wieder aufnehmen möchten.



Empfehlungsdetails herunterladen

Sie können die Ergebnisse einer priorisierten Empfehlung der Trusted Advisor-Priorität auch herunterladen.

> **Note**
>
> Derzeit können Sie immer nur eine Empfehlung auf einmal herunterladen.

So laden Sie eine Empfehlung herunter

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Seite Trusted Advisor-Priorität wählen Sie die Empfehlung und dann Download (Herunterladen).
3. Öffnen Sie die Datei, um die Empfehlungsdetails anzuzeigen.

Registrieren von delegierten Administratoren

Sie können Mitgliedskonten hinzufügen, die Teil Ihrer Organisation als delegierte Administratoren sind. Delegierte Administratorkonten können Empfehlungen in Trusted Advisor Priority anzeigen, bestätigen, auflösen, verwerfen und erneut öffnen.

Nachdem Sie ein Konto registriert haben, müssen Sie dem:der delegierten Administrator:in die erforderlichen AWS Identity and Access Management-Berechtigungen für den Zugriff auf die Trusted Advisor Priority gewähren. Weitere Informationen finden Sie unter Zugriff verwalten auf AWS Trusted Advisor und AWS verwaltete Richtlinien für AWS Trusted Advisor.

Sie können bis zu fünf Mitgliedskonten registrieren. Nur das Verwaltungskonto kann delegierte Administratoren für die Organisation hinzufügen. Sie müssen beim Verwaltungskonto der Organisation angemeldet sein, um delegierte Administratoren anzumelden oder abzumelden.

Registrieren Sie einen delegierten Administrator wie folgt

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home als Verwaltungskonto an.
2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Your organization (Meine Organisation) aus.
3. Wählen Sie unter Delegated administrator (Delegierter Administrator) die Option Register new account (Neues Konto registrieren).
4. Geben Sie im Dialogfeld die Mitgliedskonto-ID ein und wählen Sie dann Register (Registrieren) aus.
5. (Optional) Um ein Konto abzumelden, wählen Sie ein Konto aus und wählen Sie Deregister (Abmelden). Wählen Sie im Dialogfeld erneut Deregister (Abmelden) aus.

Abmelden eines delegierten Administrators

Wenn Sie ein Mitgliedskonto abmelden, hat dieses Konto nicht mehr denselben Zugriff auf die Trusted Advisor-Priorität wie das Verwaltungskonto. Konten, die keine delegierten Administratoren mehr sind, erhalten keine E-Mail-Benachrichtigungen von der Trusted Advisor-Priorität.

Heben Sie die Registrierung eines delegierten Administrators auf wie folgt

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home als Verwaltungskonto an.

2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Your organization (Meine Organisation) aus.
3. Wählen Sie unter Delegierter Administrator ein Konto aus und wählen Sie dann Abmelden aus.
4. Wählen Sie im Dialogfeld Deregister (Abmelden) aus.

Verwalten von Benachrichtigungen der Trusted Advisor-Priorität

Die Trusted Advisor-Priorität übermittelt Benachrichtigungen per E-Mail. Diese E-Mail-Benachrichtigung enthält eine Zusammenfassung der Empfehlungen, die Ihr Kontoteam für Sie priorisiert hat. Sie können die Häufigkeit angeben, mit der Sie Aktualisierungen von der Trusted Advisor-Priorität erhalten.

Wenn Sie Mitgliedskonten als delegierte Administratoren registriert haben, können diese ihre Konten auch so einrichten, dass sie E-Mail-Benachrichtigungen mit der Trusted Advisor-Priorität erhalten.

E-Mail-Benachrichtigungen der Trusted Advisor-Priorität enthalten keine Prüfergebnisse für einzelne Konten und sind von der wöchentlichen Benachrichtigung für Trusted Advisor-Benachrichtigungen getrennt. Weitere Informationen finden Sie unter Einrichten von Benachrichtigungseinstellungen.

> **Note**
>
> Nur das Verwaltungskonto oder delegierte Administratoren können E-Mail-Benachrichtigungen für Trusted Advisor Priority einrichten.

Verwalten Sie Ihre Benachrichtigungen von der Trusted Advisor-Priorität wie folgt

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home als Verwaltungs- oder delegiertes Administratorkonto an.
2. Wählen Sie im Navigationsbereich unter Preferences (Präferenzen) die Option Notifications (Benachrichtigungen).
3. Unter -Priorität können Sie die folgenden Optionen auswählen.
    a. Daily (Täglich) – Erhalten Sie täglich eine E-Mail-Benachrichtigung.
    b. Weekly (Wöchentlich) – Erhalten Sie einmal pro Woche eine E-Mail-Benachrichtigung.
    c. Wählen Sie die Benachrichtigungen, die Sie erhalten möchten:
        - Zusammenfassung von priorisierten Empfehlungen

- Daten der Lösung

4. Wählen Sie unter Empfänger andere Kontakte aus, die die E-Mail-Benachrichtigungen erhalten sollen. Sie können Kontakte auf der Seite Account Setting (Kontoeinstellungen) in der AWS Billing and Cost Management-Konsole hinzufügen und entfernen.
5. Wählen Sie unter Language (Sprache) die Sprache für die E-Mail-Benachrichtigung.
6. Wählen Sie Save your preferences (Ihre Präferenzen speichern) aus.

> **Note**
>
> Die Trusted Advisor-Priorität sendet E-Mail-Benachrichtigungen von der noreply@notifications.trustedadvisor.us-west-2.amazonaws.com-Adresse. Möglicherweise müssen Sie überprüfen, ob Ihr E-Mail-Client diese E-Mails nicht als Spam identifiziert.

Deaktivieren der Trusted Advisor-Priorität

Wenden Sie sich an Ihr Kontoteam und bitten Sie es, diese Funktion für Sie zu deaktivieren. Nach der Deaktivierung dieses Features werden die priorisierten Empfehlungen nicht mehr in Ihrer Trusted Advisor-Konsole angezeigt.

Wenn Sie die Trusted Advisor-Priorität deaktivieren und später wieder aktivieren, können Sie weiterhin die Empfehlungen anzeigen, die Ihr Kontoteam gesendet hat, bevor Sie die Trusted Advisor-Priorität deaktiviert haben.

Erste Schritte mit AWS Trusted Advisor Engage (Vorschau)

> **Note**
>
> Bei AWS Trusted Advisor Engage handelt es sich um eine Vorversion, die Änderungen unterliegt. Eine Vorschau der Servicebedingungen finden Sie unter https://aws.amazon.com/service-terms/.

Mit AWS Trusted Advisor Engage können Sie das Beste aus Ihren AWS Support-Plänen herausholen, indem Sie alle Ihre proaktiven Engagements sehen, anfordern und nachverfolgen und mit Ihrem AWS-Konto-Team über laufende Engagements kommunizieren können.

Sie können zum Beispiel eine „Überprüfung des Management-Geschäfts“ für Ihr AWS-Konto-Team anfordern, indem Sie die Einbinden-Seite in der AWS Trusted Advisor-Konsole aufrufen. Anschließend wird Ihrer Anfrage ein:e AWS-Expert:in zugewiesen, der:die Sie während des gesamten Projekts begleitet.

Themen

Voraussetzungen

Zum Erfüllen der folgenden Anforderungen müssen Sie die erforderlichen Maßnahmen ergreifen, um Trusted Advisor Engage nutzen zu können:

- Sie müssen über einen Enterprise-On-Ramp-Supportplan verfügen.
- Ihr Konto muss Teil einer Organisation sein, die alle Funktionen in AWS Organizations aktiviert hat. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.
- Ihre Organisation muss vertrauenswürdigen Zugriff auf Trusted Advisor aktiviert haben. Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie sich als Verwaltungskonto anmelden und in der Trusted Advisor-Konsole die Seite Ihre Organisation aufrufen.
- Sie müssen über AWS Identity and Access Management (IAM)-Berechtigungen verfügen, um auf Trusted Advisor Engage zugreifen zu können. Weitere Informationen zum Steuern des Zugriffs auf Trusted Advisor Engage finden Sie unter Zugriff verwalten auf AWS Trusted Advisor.

> **Note**
>
> Jedes Konto innerhalb einer AWS-Organisation kann eine Engagement-Anfrage erstellen. Wenn ein Konto, das ein Engagement besitzt, zu einer anderen AWS-Organisation wechselt, ist das Engagement nur noch für dieses Konto zugänglich. Informationen zur Einschränkung der Kontrollen finden Sie unter Beispiel für Service-Kontrollrichtlinien für AWS Trusted Advisor.

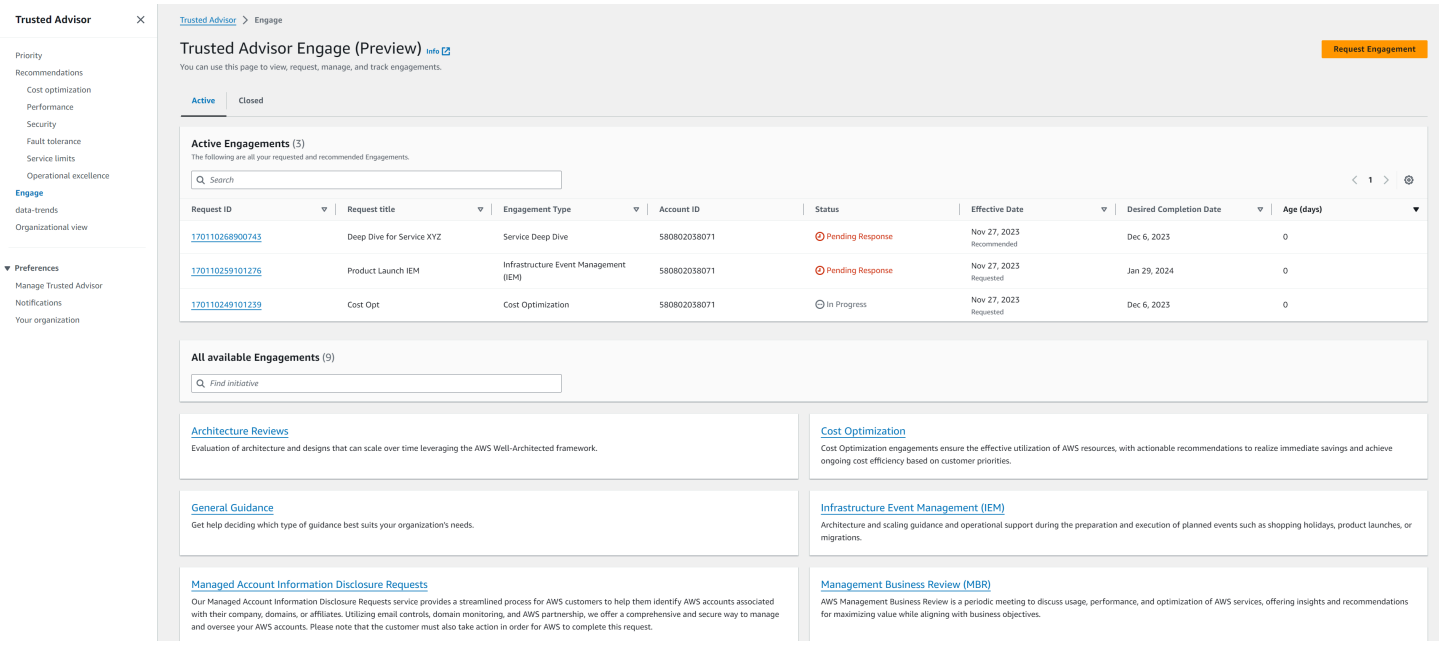
Anzeigen des Engagement-Dashboards

Nachdem Sie Zugriffsrechte erhalten haben, können Sie auf die Seite „Trusted Advisor Engage“ innerhalb der Trusted Advisor-Konsole zugreifen, um ein Dashboard anzuzeigen, auf dem Sie Engagements mit Ihrem AWS-Konto-Team verwalten können.

So verwalten Sie Ihre Engagements:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Trusted Advisor Engage-Seite können Sie Folgendes anzeigen:
   - Schaltfläche Engagement anfragen
   - Tabelle Aktive Engagements
   - Tabelle Geschlossene Engagements
   - Katalog Alle verfügbaren Engagements

Example : Engagement-Dashboard



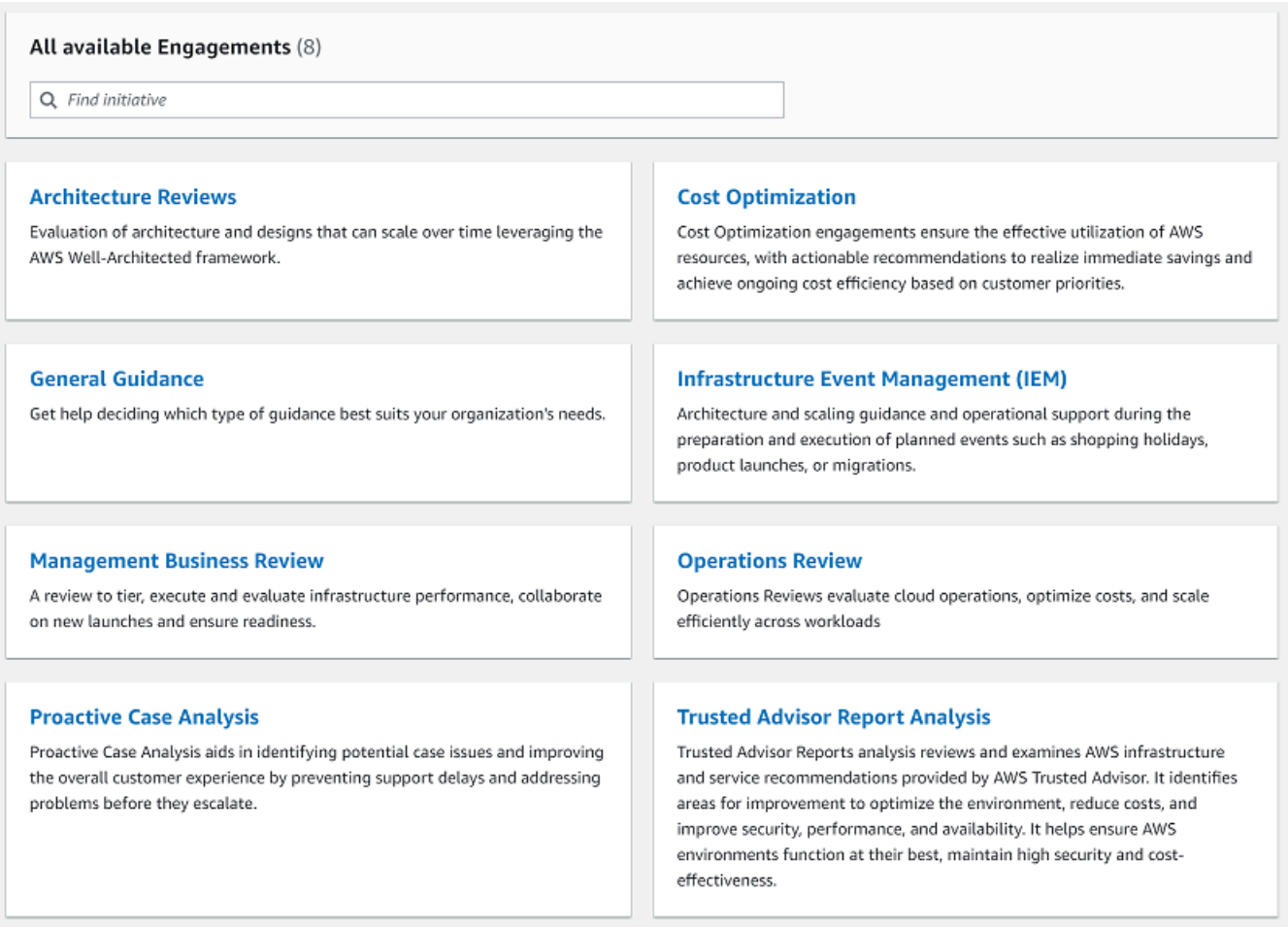
Anzeigen des Katalog der Engagementtypen

Sie können den Katalog der Engagementtypen anzeigen, um die neuesten Engagementtypen zu finden, die Sie für Ihr AWS-Konto-Team anfordern können.

So zeigen Sie den Katalog der Engagementtypen an:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Trusted Advisor Engage-Seite finden Sie den Katalog der Engagementtypen.

Example : Katalog der Engagementtypen



Anfordern eines Engagements

Sie können Ihrem AWS-Konto-Team Aufträge entsprechend den in Ihrem AWS-Supportplan enthaltenen Engagementtypen erteilen.

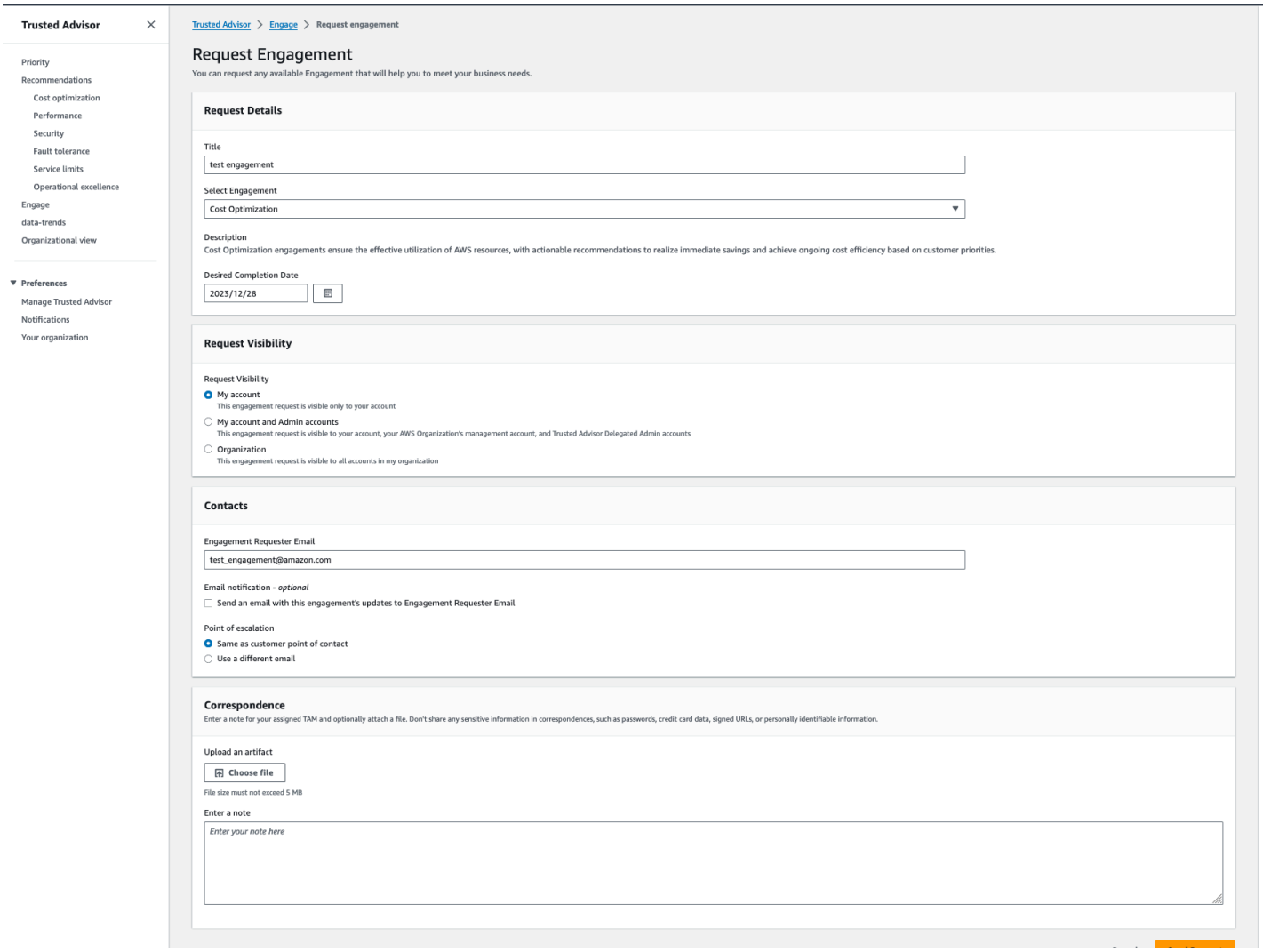
So fordern Sie ein Engagement an:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wählen Sie auf der Seite Trusted Advisor Engage die Option Engagement anfragen aus.
3. Füllen Sie Folgendes aus:
   - Titel
   - Engagement auswählen: Die Art des Engagements, das Sie anfordern möchten.

- Gewünschtes Abschlussdatum: Das gewünschte Abschlussdatum des Engagements. Jeder Engagement-Typ hat eine andere Vorlaufzeit, die in den gewünschten Mindestabschlusstermin eingerechnet wird.
- Sichtbarkeit anfragen:
  - Mein Konto: Diese Engagement-Anfrage ist nur für Ihr Konto sichtbar.
  - Mein Konto und Administratorkonten: Diese Engagement-Anfrage ist für Ihr Konto, das Verwaltungskonto und alle delegierten Administratorkonten Ihrer AWS-Organisation sichtbar.
  - Organisation: Diese Engagement-Anfrage ist für alle Konten in Ihrer AWS-Organisation sichtbar.
- E-Mail des Interaktionsanforderers: Die E-Mail-Adresse, die als Hauptansprechpartner für dieses Engagement verwendet AWS wird.
- Einstellungen für E-Mail-Benachrichtigungen: Wählen Sie aus, ob die E-Mail des Interaktionsanforderers E-Mail-Benachrichtigungen über das Engagement erhalten soll.
- Eskalationspunkt: Die E-Mail-Adresse, die AWS verwenden wird, wenn für dieses Engagement eine Eskalation erforderlich ist.
- Korrespondenz: Eine Notiz und ein optionaler Dateianhang, in dem Sie Einzelheiten zu diesem Engagement angeben können.

4. Wählen Sie Anfrage senden aus.

Example : Anfordern eines Engagements



Bearbeiten eines Engagements

Sie können die Details Ihrer Engagementanfrage bearbeiten.

So bearbeiten Sie ein Engagement:

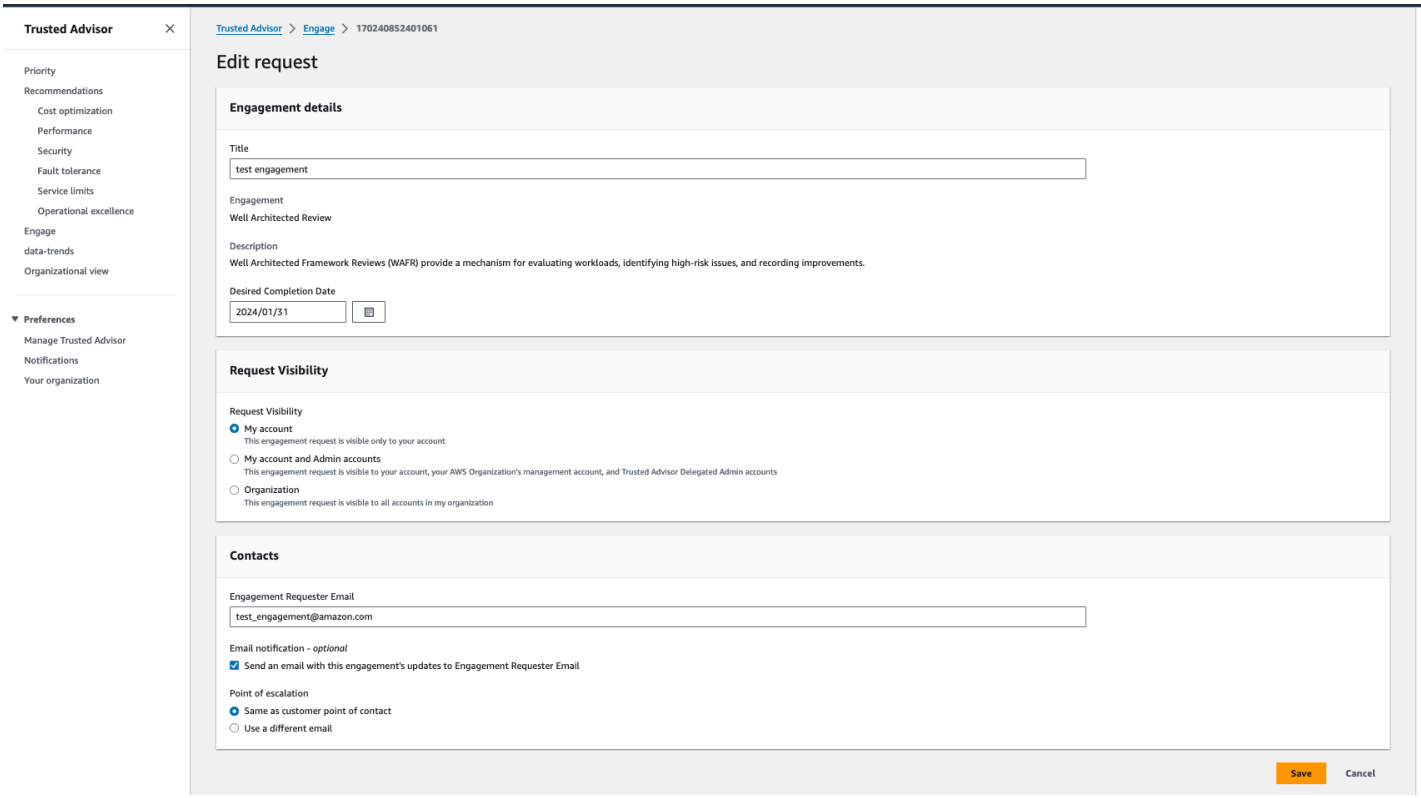
1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wählen Sie auf der Seite Trusted Advisor Engage ein vorhandenes Engagement aus.
3. Wählen Sie Bearbeiten aus.
4. Folgendes kann bearbeitet werden:

   - Titel

- Gewünschtes Abschlussdatum: Das gewünschte Abschlussdatum des Engagements. Jeder Engagement-Typ hat eine andere Vorlaufzeit, die in den gewünschten Mindestabschlusstermin eingerechnet wird.
- Sichtbarkeit anfragen:
  - Mein Konto: Diese Engagement-Anfrage ist nur für Ihr Konto sichtbar.
  - Mein Konto und Administratorkonten: Diese Engagement-Anfrage ist für Ihr Konto, das Verwaltungskonto und alle delegierten Administratorkonten Ihrer AWS-Organisation sichtbar.
  - Organisation: Diese Engagement-Anfrage ist für alle Konten in Ihrer AWS-Organisation sichtbar.
- E-Mail-Adresse des Interaktionsanforderers: Die E-Mail-Adresse, die als Hauptansprechpartner für dieses Engagement verwendet AWS wird.
- Einstellungen für E-Mail-Benachrichtigungen: Wählen Sie aus, ob die E-Mail des Interaktionsanforderers E-Mail-Benachrichtigungen über das Engagement erhalten soll.
- Eskalationspunkt: Die E-Mail-Adresse, die AWS verwenden wird, wenn für dieses Engagement eine Eskalation erforderlich ist.

5. Wählen Sie Speichern.

Example : Bearbeiten eines Engagements



Senden von Anhängen und Notizen

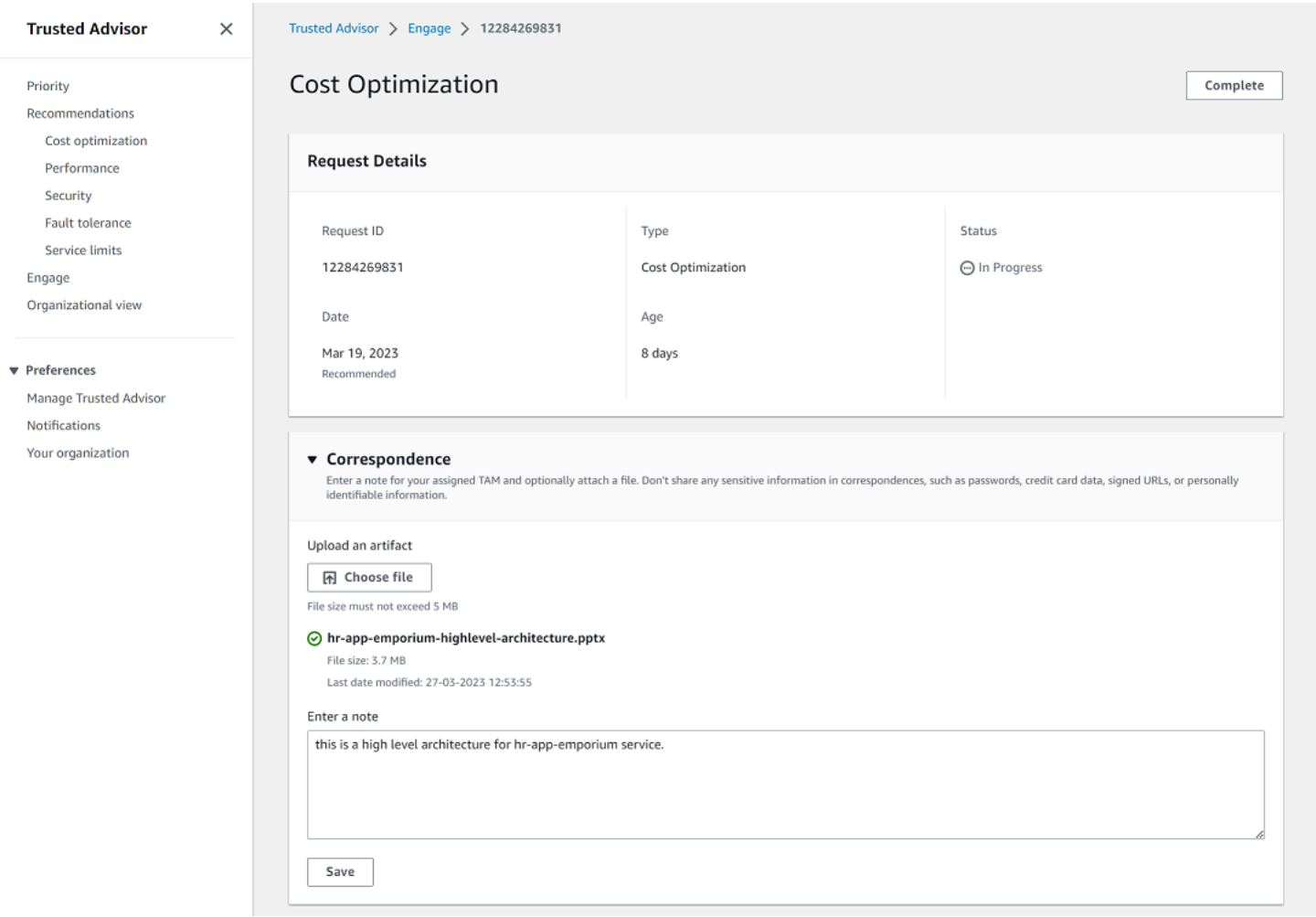
Sie können bei einzelnen Engagements mit Ihrem AWS-Konto-Team kommunizieren, indem Sie Notizen und Dateianhänge zur Unterstützung Ihrer Anfrage senden. Sie können nur einen einzigen Anhang und eine einzige Notiz pro Mitteilung einfügen, Sie können Dateien nur an ein Engagement mit demselben AWS-Konto anhängen, das das Engagement angefordert hat, und Sie können keine Anhänge oder Notizen löschen, nachdem eine Mitteilung gesendet wurde.

So hängen Sie Dateien an oder fügen Notizen zu einer Anfrage für aktives Engagement hinzu:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wählen Sie auf der Seite Trusted Advisor Engage die ID des aktiven Engagements aus, an das Sie Dateien anhängen oder Notizen hinzufügen möchten.
3. Wählen Sie Korrespondenz, um das Formular zu erweitern.
4. Geben Sie eine Notiz für Ihren zugewiesenes TAM ein und hängen Sie optional eine Datei an. Geben Sie in der Korrespondenz keine sensiblen Informationen weiter, wie z. B. Passwörter, Kreditkartendaten, signierte URLs oder persönlich identifizierbare Informationen.

5. Wählen Sie Speichern.

Example : Notiz hinzufügen und Datei an ein Engagement anhängen



Ändern des Engagement-Status

Sie können den Status von Engagements ändern, um Engagements zu stornieren, die auf eine Antwort warten, um laufende Engagements abzuschließen und um Engagements wieder zu öffnen, die als abgebrochen oder geschlossen markiert wurden.

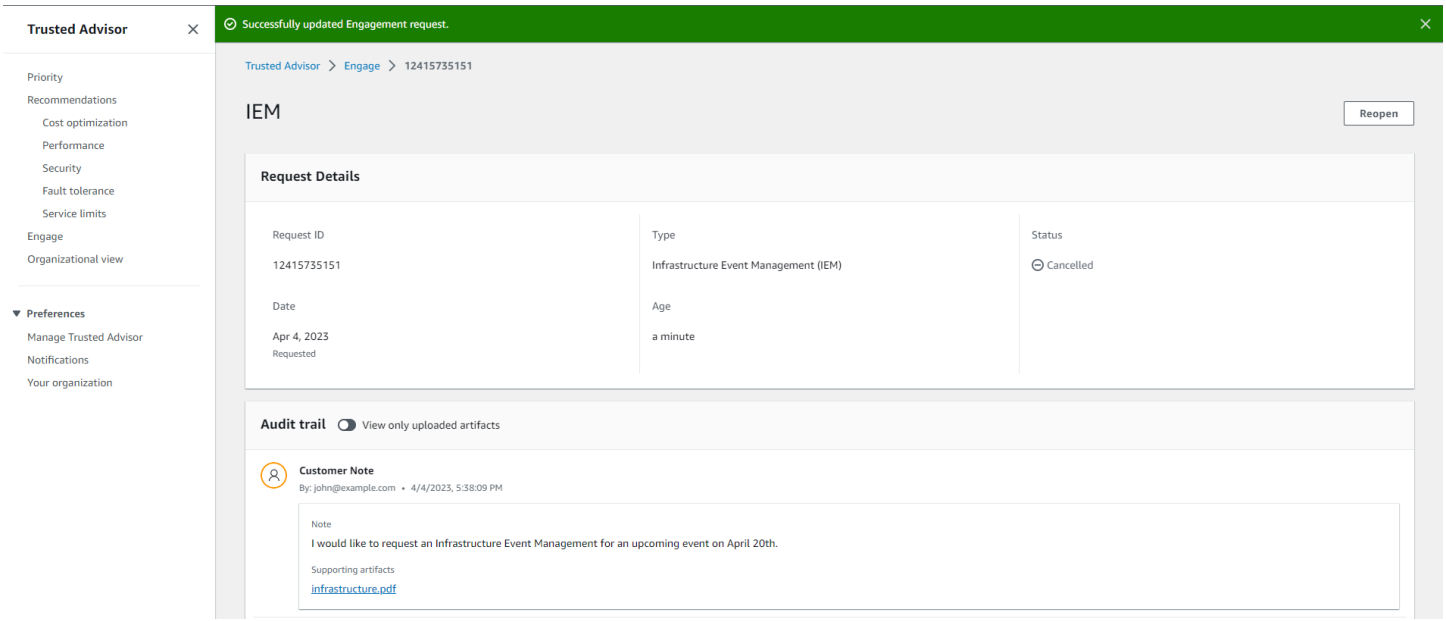
So ändern Sie den Status eines Engagements:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Wählen Sie auf der Seite Trusted Advisor Engage die ID des aktiven Engagements aus, dessen Status Sie ändern möchten.

3. Auf der Seite mit den Engagement-Details können Sie den Status in Abgebrochen oder Abgeschlossen ändern.

   - Sie können Abbrechen auswählen, wenn der Engagement-Status Antwort ausstehend lautet.
   - Sie können Abgeschlossen auswählen, wenn der Engagement-Status In Bearbeitung lautet.
   - Sie können für abgeschlossene Engagements die Option Erneut öffnen auswählen. Abgebrochene Engagements werden in den Status Antwort ausstehend verschoben, während abgeschlossene Engagements in den Status In Bearbeitung verschoben werden.

Example : Ändern des Engagement-Status



Unterscheiden zwischen empfohlenen und angeforderten Engagements

Sie können die Quelle von Engagements identifizieren, um zu erfahren, ob ein Engagement von Ihnen angefordert oder von Ihrem AWS-Konto-Team empfohlen wurde.

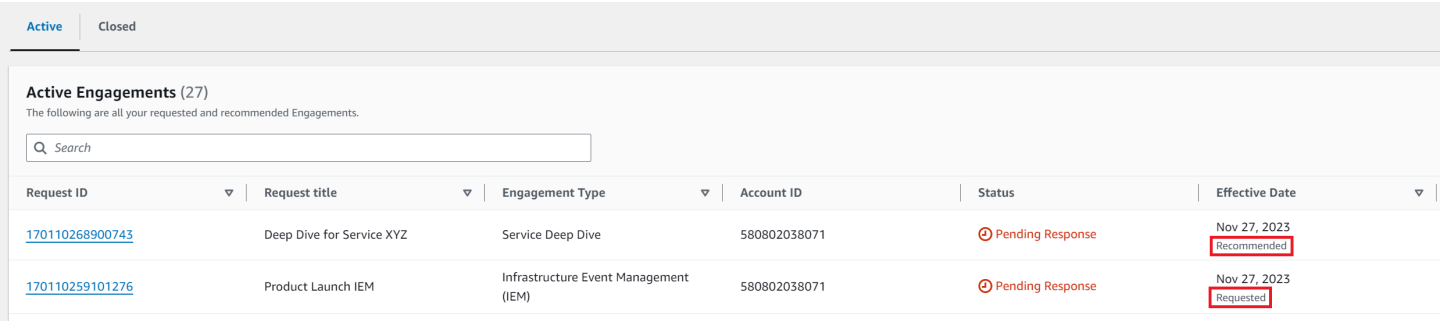
So können Sie verschiedene Quellen für aktive Engagements anzeigen:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Sehen Sie sich auf der Trusted AdvisorEngage-Seite die Spalte Gültigkeitsdatum an, um zwischen empfohlenen und angeforderten Interaktionen zu unterscheiden:

   - Empfohlen: Von Ihren AWS-Konto-Teams erstellte Engagement-Anfrage.

- Angefragt: Vom Benutzer erstellte Engagement-Anfrage.

Example : Unterscheiden zwischen empfohlenen und angeforderten Engagements



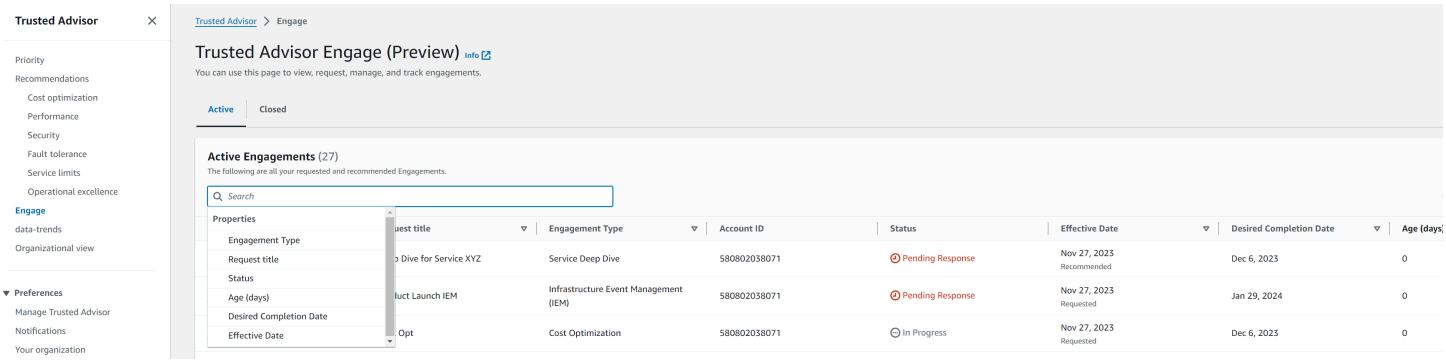
Engagements durchsuchen

Sie können Ihre bestehenden aktiven und geschlossenen Engagements mithilfe von Filtern durchsuchen.

So durchsuchen Sie Engagements:

1. Melden Sie sich bei der Trusted Advisor-Konsole unter https://console.aws.amazon.com/trustedadvisor/home an.
2. Auf der Trusted Advisor Engage-Seite können Sie aus den folgenden Filtern wählen:
   - Alter (Tage)
   - Interaktionstyp
   - Titel der Anfrage
   - Status
   - Gewünschtes Abschlussdatum
   - Datum des Inkrafttretens

Example : Engagements suchen



AWS Trusted Advisor Referenz überprüfen

In der folgenden Referenz können Sie Trusted Advisor sich alle Namen, Beschreibungen und IDs von Schecks ansehen. Sie können sich auch bei der Trusted Advisor Konsole anmelden, um weitere Informationen über die Prüfungen, die empfohlenen Maßnahmen und deren Status anzuzeigen.

Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie auch die AWS Trusted Advisor API und die AWS Command Line Interface (AWS CLI) verwenden, um auf Ihre Prüfungen zuzugreifen. Weitere Informationen finden Sie unter den folgenden Themen:

- Erste Schritte mit der Trusted Advisor API
- AWS Trusted Advisor API Reference

> **Note**
>
> Wenn Sie über einen Basic Support- und Developer Support-Plan verfügen, können Sie über die Trusted Advisor Konsole auf alle Prüfungen in der Kategorie Service Limits und auf die folgenden Prüfungen in der Kategorie Sicherheit zugreifen:
>
> - Amazon EBS-Snapshots
> - Öffentliche Amazon RDS-Snapshots
> - Amazon S3 Bucket-Berechtigungen
> - MFA auf Root-Konto
> - Sicherheitsgruppen – Bestimmte Ports uneingeschränkt

Kategorien prüfen

- Kostenoptimierung
- Leistung
- Sicherheit
- Fehlertoleranz
- Service Limits
- Operative Exzellenz

Kostenoptimierung

Sie können die folgenden Prüfungen für die Kategorie Kostenoptimierung verwenden.

Namen prüfen

- AWS-Konto ist nicht Teil von AWS Organizations
- Amazon Comprehend nicht-ausgelastete Endpunkte
- Amazon EBS mit nicht ausgelasteten Volumes
- Konsolidierung von Amazon-EC2-Instances für Microsoft SQL Server
- Amazon-EC2-Instances für Microsoft SQL Server mit übermäßiger Bereitstellung
- Amazon-EC2-Instances gestoppt
- Ende der Laufzeit von Amazon EC2-Reserved-Instances
- Amazon EC2 Reserved Instance Optimierung
- Amazon-ECR-Repository ohne konfigurierte Lebenszyklus-Richtlinie
- Amazon ElastiCache Reserved Node Optimization
- Amazon OpenSearch Service Reserved Instance-Optimierung
- Amazon RDS-DB-Instances im Leerlauf
- Amazon Redshift Reserved Node Optimierung
- Amazon Relational Database Service (RDS) Reserved Instance Optimierung
- Amazon Route 53 Latenz-Ressourceneintragsätze
- Amazon-S3-Bucket-Lebenszyklus-Richtlinie konfiguriert
- Konfiguration für unvollständigen mehrteiligen Upload-Abbruch in Amazon S3

- Amazon-S3-versionsfähige Buckets ohne konfigurierte Lebenszyklus-Richtlinien
- AWS Lambda Funktionen mit übermäßigen Timeouts
- AWS Lambda Funktionen mit hohen Fehlerraten
- AWS Lambda stellt zu viele Funktionen für die Speichergröße bereit
- AWS Well-Architected-Probleme mit hohem Risiko für die Kostenoptimierung
- Load Balancer im Leerlauf
- Low Utilization Amazon EC2 Instances
- Savings Plan
- Nicht zugeordnete elastische IP-Adressen
- Nicht ausgelastete Amazon EBS-Volumes
- Nicht ausgelastete Amazon Redshift-Cluster

AWS-Konto ist nicht Teil von AWS Organizations

Beschreibung

Überprüft, ob ein AWS-Konto Teil von AWS Organizations unter dem entsprechenden Verwaltungskonto ist.

AWS Organizations ist ein Kontoverwaltungsservice zur Konsolidierung mehrerer AWS-Konten in einer zentral verwalteten Organisation. Damit können Sie Konten für die Abrechnungskonsolidierung zentral strukturieren und Eigentümerschafts- und Sicherheitsrichtlinien implementieren, wenn Ihre Workloads in AWS größer werden.

Sie können die Verwaltungskonto-ID mit dem MasterAccountId Parameter der AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Was ist AWS Organizations?

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz127`

Quelle

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

Warnungskriterien

Gelb: Dieses AWS-Konto ist nicht Teil von AWS Organizations.

Empfohlene Aktion

Fügen Sie dieses AWS-Konto als Teil von AWS Organizations hinzu.

Weitere Informationen finden Sie unter Praktische Anleitung: Erstellen und Konfigurieren einer Organisation.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config-Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon Comprehend nicht-ausgelastete Endpunkte

Beschreibung

Überprüft die Durchsatzkonfiguration Ihrer Endpunkte. Diese Prüfung warnt Sie, wenn Endpunkte nicht aktiv für Echtzeit-Inferenzanforderungen genutzt werden. Ein Endpunkt, der nicht mehr als 15 aufeinanderfolgende Tage genutzt wird, gilt als nicht ausgelastet. Es fallen für alle Endpunkte Gebühren an – basierend auf dem eingestellten Durchsatz, und wie lange der Endpunkt aktiv ist.

> **Note**
>
> Diese Überprüfung wird einmal täglich automatisch aktualisiert. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Cm24dfsM12`

Warnungskriterien

Gelb: Der Endpunkt ist aktiv, wurde aber in den letzten 15 Tagen nicht für Echtzeit-Inferenzanforderungen verwendet.

Empfohlene Aktion

Wenn der Endpunkt in den letzten 15 Tagen nicht verwendet wurde, empfehlen wir Ihnen, mit Application Autoscaling eine Skalierungsrichtlinie für die Ressource zu definieren.

Wenn für den Endpunkt eine Skalierungsrichtlinie definiert wurde, die in den letzten 30 Tagen nicht verwendet wurde, sollten Sie den Endpunkt löschen und die asynchrone Inferenz verwenden. Weitere Informationen finden Sie unter Deleting an endpoint with Amazon Comprehend (Löschen eines Endpunkts mit Amazon Comprehend).

Berichtsspalten

- Status
- Region
- Endpunkt-ARN
- Bereitgestellte Inferenzeinheit
- AutoScaling Status
- Grund
- Zeitpunkt der letzten Aktualisierung

Amazon EBS mit nicht ausgelasteten Volumes

Beschreibung

Prüft die Amazon Elastic Block Store (Amazon EBS)-Volumes, die zu einem beliebigen Zeitpunkt während des Lookback-Zeitraums ausgeführt wurden. Diese Überprüfung warnt Sie, wenn eine zu hohe Kapazität für EBS-Volumes für Ihre Workloads bereitgestellt wurden. Wenn Volumes übermäßig bereitgestellt werden, zahlen Sie für nicht genutzte Ressourcen. Obwohl einige Szenarien von vornherein zu einer geringen Optimierung führen können, lassen sich die Kosten oft senken, indem Sie die Konfiguration Ihrer EBS-Volumes ändern. Die geschätzten monatlichen

Einsparungen werden anhand der aktuellen Nutzungsrate für EBS-Volumes berechnet. Die tatsächlichen Einsparungen variieren, wenn das Volumen einen ganzen Monat lang nicht vorhanden ist.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`C0r6dfpM03`

Warnungskriterien

Gelb: Ein EBS-Volume, das während des Lookback-Zeitraums nicht ausgelastet war. Um festzustellen, ob ein Volume überlastet ist, berücksichtigen wir alle CloudWatch Standardmetriken (einschließlich IOPS und Durchsatz). Der Algorithmus, der zur Identifizierung nicht ausgelasteter EBS-Volumes verwendet wird, folgt bewährten Methoden für AWS. Der Algorithmus wird aktualisiert, wenn ein neues Muster identifiziert wurde.

Empfohlene Aktion

Sie sollten Volumes mit geringer Auslastung verkleinern.

Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Berichtsspalten

- Status
- Region
- Volume-ID
- Volume-Typ
- Volumegröße (GB)
- Volume-IOPS-Basisleistung
- Volume-IOPS-Spitzenleistung

- Volume-Spitzendurchsatz
- Empfohlener Volume-Typ
- Empfohlene Volume-Größe (GB)
- Empfohlene Volumen-IOPS-Basisleistung
- Empfohlene Volume-IOPS-Spitzenleistung
- Empfohlener Volume-Basisdurchsatz
- Empfohlener Volume-Spitzendurchsatz
- Lookback-Zeitraum (in Tagen)
- Einsparmöglichkeiten (in %)
- Geschätzte monatliche Einsparungen
- Währung der geschätzten monatlichen Einsparungen
- Zeitpunkt der letzten Aktualisierung

Konsolidierung von Amazon-EC2-Instances für Microsoft SQL Server

Beschreibung

Überprüft Ihre Amazon-Elastic-Compute-Cloud(Amazon EC2)-Instances, auf denen in den letzten 24 Stunden SQL Server ausgeführt wurde. Diese Prüfung warnt Sie, wenn Ihre Instance weniger als die Mindestanzahl an SQL Server-Lizenzen hat. Gemäß dem Microsoft SQL Server Licensing Guide zahlen Sie 4 vCPU-Lizenzen, auch wenn eine Instance nur 1 oder 2 vCPU-Lizenzen hat. Sie können kleinere SQL Server-Instances konsolidieren, um die Kosten zu senken.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Qsdfp3A4L2`

Warnungskriterien

Gelb: Eine Instance mit SQL-Server hat weniger als 4 vCPUs.

Empfohlene Aktion

Konsolidieren Sie kleinere SQL-Server-Workloads in Instances mit mindestens 4 vCPUs.

Weitere Ressourcen

- Microsoft SQL Server auf AWS
- Microsoft-Lizenzierung auf AWS
- Microsoft SQL Server Licensing Guide (Leitfaden zur Lizenzierung von Microsoft SQL Server)

Berichtsspalten

- Status
- Region
- Instance-ID
- Instance-Typ
- vCPU
- Minimale vCPU
- SQL Server Edition
- Zeitpunkt der letzten Aktualisierung

Amazon-EC2-Instances für Microsoft SQL Server mit übermäßiger Bereitstellung

Beschreibung

Überprüft Ihre Amazon-Elastic-Compute-Cloud(Amazon EC2)-Instances, auf denen in den letzten 24 Stunden SQL Server ausgeführt wurde. Eine SQL Server-Datenbank hat für jede Instance ein Rechenkapazitätslimit. Eine Instance mit SQL Server Standard Edition kann bis zu 48 vCPUs nutzen. Eine Instance mit SQL Server Web kann bis zu 32 vCPUs nutzen. Diese Prüfung warnt Sie, wenn eine Instance dieses vCPU-Limit überschreitet.

Wenn Ihre Instance übermäßig bereitgestellt wurde, zahlen Sie den vollen Preis, ohne eine Verbesserung der Leistung zu erzielen. Sie können die Anzahl und Größe Ihrer Instances verwalten, um die Kosten zu senken.

Die geschätzten monatlichen Einsparungen werden unter Verwendung derselben Instance-Familie mit der maximalen Anzahl von vCPUs berechnet, die eine SQL Server-Instance verwenden kann, und dem On-Demand-Preis. Die tatsächlichen Einsparungen variieren, wenn Sie Reserved Instances (RI) verwenden oder wenn die Instance nicht einen ganzen Tag lang läuft.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Qsdfp3A4L1`

Warnungskriterien

- Eine Instance mit SQL Server Standard Edition verfügt über mehr als 48 vCPUs.
- Eine Instance mit SQL Server Web Edition verfügt über mehr als 32 vCPUs.

Empfohlene Aktion

Für die SQL Server Standard Edition sollten Sie zu einer Instance derselben Instance-Familie mit 48 vCPUs wechseln. Für die SQL Server Web Edition sollten Sie zu einer Instance derselben Instance-Familie mit 32 vCPUs wechseln. Wenn die Anwendung speicherintensiv ist, sollten Sie auf speicheroptimierte R5-Instances umzusteigen. Weitere Informationen finden Sie unter Best Practices for Deploying Microsoft SQL Server on Amazon EC2 (Bewährte Methoden für die Bereitstellung von Microsoft SQL Server auf Amazon EC2).

Weitere Ressourcen

- Microsoft SQL Server auf AWS
- Mit dem Startassistenten vereinfachen Sie die SQL-Server-Bereitstellung auf EC2.

Berichtsspalten

- Status
- Region
- Instance-ID
- Instance-Typ

- vCPU
- SQL Server Edition
- Maximale vCPU
- Empfohlener Instance-Typ
- Geschätzte monatliche Einsparungen
- Zeitpunkt der letzten Aktualisierung

Amazon-EC2-Instances gestoppt

Beschreibung

Überprüft, ob Amazon-EC2-Instances vorhanden sind, die länger als 30 Tage gestoppt wurden.

Sie können den Wert für die zulässige Anzahl von Tagen in der AllowedDays der der AWS Config Parameter angeben.

Weitere Informationen finden Sie unter Warum wird mir Amazon EC2 in Rechnung gestellt, obwohl alle meine Instances beendet wurden?

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz150
```

Quelle

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

Warnungskriterien

- Gelb: Es gibt Amazon-EC2-Instances, die länger als die zulässige Anzahl von Tagen angehalten wurden.

Empfohlene Aktion

Überprüfen Sie die Amazon-EC2-Instances, die seit 30 Tagen oder länger gestoppt wurden. Um unnötige Kosten zu vermeiden, beenden Sie alle Instances, die nicht mehr benötigt werden.

Weitere Informationen finden Sie unter Beenden Ihrer Instance.

Weitere Ressourcen

- On-Demand-Preise von Amazon EC2

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config-Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Ende der Laufzeit von Amazon EC2-Reserved-Instances

Beschreibung

Prüft nach Amazon EC2-Reserved-Instances, die innerhalb der nächsten 30 Tage ablaufen sollen oder in den letzten 30 Tagen abgelaufen sind.

Reservierte Instances werden nicht automatisch erneuert. Sie können eine durch die Reservierung abgedeckte Amazon-EC2-Instance ohne Unterbrechung weiter nutzen, aber es werden Ihnen On-Demand-Tarife berechnet. Neue Reserved Instances können die gleichen Parameter haben wie die abgelaufenen, oder Sie können Reserved Instances mit anderen Parametern erwerben.

Die geschätzten monatlichen Einsparungen ergeben sich aus der Differenz zwischen den Tarifen für On-Demand und Reserved Instances für denselben Instance-Typ.

Prüf-ID

`1e93e4c0b5`

Warnungskriterien

- Gelb: Die Reserved-Instance-Lease läuft in weniger als 30 Tagen ab.

- Gelb: Die Reserved-Instance-Lease ist in den letzten 30 Tagen abgelaufen.

Empfohlene Aktion

Erwägen Sie den Kauf einer neuen Reserved Instance, um diejenige zu ersetzen, die sich dem Ende der Laufzeit nähert. Weitere Informationen finden Sie unter Erwerb von Reserved Instances und Kaufen von Reserved Instances.

Weitere Ressourcen

- Reserved Instances
- Instance-Typen

Berichtsspalten

- Status
- Bereich
- Instance-Typ
- Plattform
- Instance-Anzahl
- Aktuelle monatliche Kosten
- Geschätzte monatliche Einsparungen
- Ablaufdatum
- Reserved Instance ID
- Grund

Amazon EC2 Reserved Instance Optimierung

Beschreibung

Ein wichtiger Teil der Nutzung von AWS ist der Abgleich zwischen dem Kauf einer Reserved Instance (RI) und der Nutzung einer On-Demand-Instance. Diese Prüfung gibt Empfehlungen, welche RIs dazu beitragen, die durch die Nutzung von On-Demand-Instances entstehenden Kosten zu reduzieren.

Wir erstellen diese Empfehlungen durch die Analyse Ihrer On-Demand-Nutzung in den letzten 30 Tagen. Anschließend wird die Nutzung in Kategorien eingeteilt, die für Reservierungen in Frage kommen. Wir simulieren jede Kombination von Reservierungen in der generierten Nutzungskategorie, um die empfohlene Anzahl der einzelnen RI-Typen für den Kauf zu ermitteln.

Dieser Simulations- und Optimierungsprozess ermöglicht es uns, Ihre Kosteneinsparungen zu maximieren. Diese Prüfung bezieht sich auf Empfehlungen, die auf Standard Reserved Instances mit der Option der teilweisen Vorauszahlung basieren.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

`cX3c2R1chu`

Warnungskriterien

Gelb: Die Optimierung der Verwendung von Partial Upfront RIs kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere und individuelle Empfehlungen. Darüber hinaus erfahren Sie im Kaufleitfaden, wie der Kauf von RIs funktioniert und welche Optionen verfügbar sind.

Weitere Ressourcen

- Informationen zu RIs und den damit verbundenen Einsparungen finden Sie hier.
- Weitere Informationen zu dieser Empfehlung finden Sie unter Prüfung von Reserved-Instance-Optimierungen in den häufig gestellten Fragen zu Trusted Advisor.

Berichtsspalten

- Region
- Instance-Typ
- Plattform
- Empfohlene Anzahl der zu kaufenden RIs
- Erwartete durchschnittliche RI-Auslastung
- Geschätzte Einsparungen mit Empfehlungen (monatlich)
- Vorabkosten von RIs
- Geschätzte Kosten von RIs (monatlich)
- Geschätzte On-Demand-Kosten nach dem empfohlenen RI-Kauf (monatlich)
- Geschätzter Break Even (in Monaten)

- Lookback-Zeitraum (in Tagen)
- Laufzeit (in Jahren)

Amazon-ECR-Repository ohne konfigurierte Lebenszyklus-Richtlinie

Beschreibung

Prüft, ob für ein privates Amazon-ECR-Repository mindestens eine Lebenszyklus-Richtlinie konfiguriert wurde. Mithilfe von Lebenszyklus-Richtlinien können Sie eine Reihe von Regeln definieren, um alte oder ungenutzte Container-Images automatisch zu bereinigen. Dies gibt Ihnen die Kontrolle über die Lebenszyklus-Verwaltung der Images, ermöglicht eine bessere Organisation der Amazon-ECR-Repositorys und trägt zur Senkung der Gesamtspeicherkosten bei.

Weitere Informationen finden Sie unter Lebenszyklus-Richtlinien.

Prüf-ID

```
c18d2gz128
```

Quelle

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

Warnungskriterien

Gelb: Für ein privates Amazon-ECR-Repository sind keine Lebenszyklus-Richtlinien konfiguriert.

Empfohlene Aktion

Erwägen Sie, mindestens eine Lebenszyklus-Richtlinie für Ihr privates Amazon-ECR-Repository zu erstellen.

Weitere Informationen finden Sie unter Erstellen einer Lebenszyklus-Richtlinie.

Weitere Ressourcen

- Lebenszyklus-Richtlinien.
- Erstellen einer Lebenszyklus-Richtlinie.
- Beispiele für Lebenszyklus-Richtlinien.

Berichtsspalten

- Status
- Region

- Ressource
- AWS Config-Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon ElastiCache Reserved Node Optimization

Beschreibung

Prüft Ihre Nutzung von ElastiCache und gibt Empfehlungen zum Kauf von reservierten Knoten. Diese Empfehlungen sollen die Kosten senken, die durch die Nutzung von ElastiCache On-Demand entstehen. Wir erstellen diese Empfehlungen durch die Analyse Ihrer On-Demand-Nutzung in den letzten 30 Tagen.

Mit dieser Analyse simulieren wir jede Kombination von Reservierungen in der generierten Nutzungskategorie. Auf diese Weise können wir Ihnen die Anzahl der einzelnen Reserved Nodes empfehlen, die Sie kaufen sollten, um Ihre Einsparungen zu maximieren. Diese Prüfung bezieht sich auf Empfehlungen, die auf der Option der teilweisen Vorauszahlung mit einer 1- oder 3-jährigen Verpflichtung basieren.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

`h3L1otH3re`

Warnungskriterien

Gelb: Die Optimierung des Kaufs von ElastiCache reservierten Knoten kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere Empfehlungen, Anpassungsoptionen (z. B. Lookback-Zeitraum, Zahlungsoption usw.) und Informationen zum Kauf von ElastiCache reservierten Knoten.

Weitere Ressourcen

- Informationen zu ElastiCache Reserved Nodes und den damit verbundenen Einsparungen finden Sie hier.

- Weitere Informationen zu dieser Empfehlung finden Sie unter Prüfung von Reserved-Instance-Optimierungen in den häufig gestellten Fragen zu Trusted Advisor.
- Eine detailliertere Beschreibung der Felder finden Sie in der Cost-Explorer-Dokumentation.

Berichtsspalten

- Region
- Familie
- Node Type
- Produktbeschreibung
- Empfohlene Anzahl reservierter Knoten zum Kauf
- Erwartete durchschnittliche Auslastung reservierter Knoten
- Geschätzte Einsparungen mit Empfehlungen (monatlich)
- Vorabkosten für reservierte Knoten
- Geschätzte Kosten für reservierte Knoten (monatlich)
- Geschätzte On-Demand-Kosten nach dem empfohlenen Kauf reservierter Knoten (monatlich)
- Geschätzter Break Even (in Monaten)
- Lookback-Zeitraum (in Tagen)
- Laufzeit (in Jahren)

Amazon OpenSearch Service Reserved Instance-Optimierung

Beschreibung

Prüft Ihre Nutzung von Amazon OpenSearch Service und gibt Empfehlungen zum Kauf von Reserved Instances. Diese Empfehlungen sollen die Kosten senken, die durch die Nutzung von OpenSearch On-Demand entstehen. Wir erstellen diese Empfehlungen durch die Analyse Ihrer On-Demand-Nutzung in den letzten 30 Tagen.

Mit dieser Analyse simulieren wir jede Kombination von Reservierungen in der generierten Nutzungskategorie. So können wir Ihnen die Anzahl der Reserved Instances empfehlen, die Sie kaufen sollten, um Ihre Einsparungen zu maximieren. Diese Prüfung deckt Empfehlungen ab, die auf der Option einer teilweisen Vorauszahlung mit einer 1- oder 3-jährigen Verpflichtung basieren.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

`7ujm6yhn5t`

Warnungskriterien

Gelb: Die Optimierung des Kaufs von Amazon OpenSearch Service Reserved Instances kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere Empfehlungen, Anpassungsoptionen (z. B. Lookback-Zeitraum, Zahlungsoption usw.) und Informationen zum Kauf von Amazon OpenSearch Service Reserved Instances.

Weitere Ressourcen

- Informationen zu Amazon OpenSearch Service Reserved Instances und den damit verbundenen Einsparungen finden Sie hier.
- Weitere Informationen zu dieser Empfehlung finden Sie unter Prüfung von Reserved-Instance-Optimierungen in den häufig gestellten Fragen zu Trusted Advisor.
- Eine detailliertere Beschreibung der Felder finden Sie in der Cost-Explorer-Dokumentation.

Berichtsspalten

- Region
- Instance-Klasse
- Instance-Größe
- Empfohlene Anzahl von Reserved Instances zum Kauf
- Erwartete durchschnittliche Auslastung von Reserved Instances
- Geschätzte Einsparungen mit Empfehlungen (monatlich)
- Vorabkosten für Reserved Instances
- Geschätzte Kosten für Reserved Instances (monatlich)
- Geschätzte On-Demand-Kosten nach dem empfohlenen Kauf von Reserved Instances (monatlich)
- Geschätzter Break Even (in Monaten)
- Lookback-Zeitraum (in Tagen)
- Laufzeit (in Jahren)

Amazon RDS-DB-Instances im Leerlauf

Beschreibung

Prüft die Konfiguration Ihres Amazon Relational Database Service (Amazon RDS) auf alle Datenbank-Instances (DB), die im Leerlauf zu sein scheinen.

Wenn eine DB-Instance über einen längeren Zeitraum keine Verbindung hatte, können Sie die Instance löschen, um Kosten zu sparen. Eine DB-Instance gilt als inaktiv, wenn in den letzten 7 Tagen keine Verbindung mit der Instance bestand. Wenn für die Daten auf der Instance eine dauerhafte Speicherung erforderlich ist, können Sie kostengünstigere Optionen verwenden, wie z. B. die Erstellung und Aufbewahrung eines DB-Snapshots. Manuell erstellte DB-Snapshots bleiben erhalten, bis Sie sie löschen.

Prüf-ID

`Ti39halfu8`

Warnungskriterien

Gelb: Eine aktive DB-Instance hat in den letzten 7 Tagen keine Verbindung hergestellt.

Empfohlene Aktion

Sie können einen Snapshot der inaktiven DB-Instance erstellen und ihn dann entweder anhalten oder löschen. Das Anhalten der DB-Instance senkt einen Teil der Kosten dafür, jedoch keine Speicherkosten. Eine angehaltene Instance speichert alle automatisierten Backups basierend auf dem konfigurierten Aufbewahrungszeitraum. Das Anhalten einer DB-Instance verursacht in der Regel zusätzliche Kosten im Vergleich zum Löschen der Instance und der anschließenden Beibehaltung des endgültigen Snapshots. Weitere Informationen finden Sie unter Eine Amazon RDS-DB-Instance temporär stoppen und Löschen einer DB-Instance.

Weitere Ressourcen

Sichern und Wiederherstellen

Berichtsspalten

- Region
- Name der DB-Instance
- Multi-AZ
- Instance-Typ

- Bereitgestellter Speicher (GB)
- Tage seit der letzten Verbindung
- Geschätzte monatliche Einsparungen (auf Abruf)

Amazon Redshift Reserved Node Optimierung

Beschreibung

Prüft Ihre Nutzung von Amazon Redshift und gibt Empfehlungen zum Kauf von Reserved Nodes, um die Kosten für die Nutzung von Amazon Redshift On-Demand zu reduzieren.

Wir erstellen diese Empfehlungen, indem wir Ihre On-Demand-Nutzung der letzten 30 Tage analysieren. Mit dieser Analyse simulieren wir jede Kombination von Reservierungen in der generierten Nutzungskategorie. Auf diese Weise können wir für jede Art von Reserved Nodes die beste Anzahl für den Kauf ermitteln, um Ihre Einsparungen zu maximieren. Diese Prüfung deckt Empfehlungen ab, die auf der Option einer teilweisen Vorauszahlung mit einer 1- oder 3-jährigen Verpflichtung basieren.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

```
1qw23er45t
```

Warnungskriterien

Gelb: Die Optimierung des Kaufs von reservierten Knoten für Amazon Redshift kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere Empfehlungen, Anpassungsoptionen (z. B. Lookback-Zeitraum, Zahlungsoption usw.) und Informationen zum Kauf von reservierten Knoten für Amazon Redshift.

Weitere Ressourcen

- Informationen zu reservierten Knoten für Amazon Redshift und den damit verbundenen Einsparungen finden Sie hier.
- Weitere Informationen zu dieser Empfehlung finden Sie unter Prüfung von Reserved-Instance-Optimierungen in den häufig gestellten Fragen zu Trusted Advisor.

- Eine detailliertere Beschreibung der Felder finden Sie in der Cost-Explorer-Dokumentation.

Berichtsspalten

- Region
- Familie
- Node Type
- Empfohlene Anzahl reservierter Knoten zum Kauf
- Erwartete durchschnittliche Auslastung reservierter Knoten
- Geschätzte Einsparungen mit Empfehlungen (monatlich)
- UpFront Kosten für reservierte Knoten
- Geschätzte Kosten für reservierte Knoten (monatlich)
- Geschätzte On-Demand-Kosten nach dem empfohlenen Kauf reservierter Knoten (monatlich)
- Geschätzter Break Even (in Monaten)
- Lookback-Zeitraum (in Tagen)
- Laufzeit (in Jahren)

Amazon Relational Database Service (RDS) Reserved Instance Optimierung

Beschreibung

Prüft Ihre RDS-Nutzung und gibt Empfehlungen zum Kauf von Reserved Instances, um die durch die Nutzung von RDS On-Demand entstehenden Kosten zu reduzieren.

Wir erstellen diese Empfehlungen, indem wir Ihre On-Demand-Nutzung der letzten 30 Tage analysieren. Mit dieser Analyse simulieren wir jede Kombination von Reservierungen in der generierten Nutzungskategorie. Auf diese Weise können wir die beste Anzahl jeder Art von Reserved Instance ermitteln, die Sie kaufen sollten, um Ihre Einsparungen zu maximieren. Diese Prüfung deckt Empfehlungen ab, die auf der Option einer teilweisen Vorauszahlung mit 1- oder 3-jähriger Verpflichtung basieren.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

```
1qazXsw23e
```

Warnungskriterien

Gelb: Die Optimierung des Kaufs von Reserved Instances für Amazon RDS kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere Empfehlungen, Anpassungsoptionen (z. B. Lookback-Zeitraum, Zahlungsoption usw.) und Informationen zum Kauf von Reserved Instances für Amazon RDS.

Weitere Ressourcen

- Informationen zu Reserved Instances für Amazon RDS und den damit verbundenen Einsparungen finden Sie hier.
- Weitere Informationen zu dieser Empfehlung finden Sie unter Prüfung von Reserved-Instance-Optimierungen in den häufig gestellten Fragen zu Trusted Advisor.
- Eine detailliertere Beschreibung der Felder finden Sie in der Cost-Explorer-Dokumentation.

Berichtsspalten

- Region
- Familie
- Instance-Typ
- Lizenzmodell
- Datenbank-Edition
- Datenbank-Engine
- Bereitstellungsoption
- Empfohlene Anzahl von Reserved Instances zum Kauf
- Erwartete durchschnittliche Auslastung von Reserved Instances
- Geschätzte Einsparungen mit Empfehlungen (monatlich)
- Vorabkosten für Reserved Instances
- Geschätzte Kosten für Reserved Instances (monatlich)
- Geschätzte On-Demand-Kosten nach dem empfohlenen Kauf von Reserved Instances (monatlich)
- Geschätzter Break Even (in Monaten)
- Lookback-Zeitraum (in Tagen)
- Laufzeit (in Jahren)

Amazon Route 53 Latenz-Ressourceneintragsätze

Beschreibung

Prüft auf Amazon Route 53 Latenz-Datensätze, die ineffizient konfiguriert sind.

Damit Amazon Route 53 Abfragen an den AWS-Region mit der geringsten Netzwerklatenz weiterleiten kann, sollten Sie Latenz-Ressourceneintragsätze für einen bestimmten Domainnamen (z. B. example.com) in verschiedenen Regionen erstellen. Wenn Sie nur einen Latenz-Ressourceneintragsatz für einen Domainnamen erstellen, werden alle Abfragen an eine Region weitergeleitet, und Sie zahlen zusätzlich für latenzbasiertes Routing, ohne die Vorteile zu erhalten.

Gehostete Zonen, die von AWS-Services erstellt wurden, erscheinen nicht in Ihren Prüfergebnissen.

Prüf-ID

`51fC20e7I2`

Warnungskriterien

Gelb: Nur ein Latenz-Ressourcendatenssatz ist für einen bestimmten Domainnamen konfiguriert.

Empfohlene Aktion

Wenn Sie Ressourcen in mehreren Regionen haben, stellen Sie sicher, dass Sie für jede Region einen Latenz-Ressourcendatensatz definiert haben. Weitere Informationen finden Sie unter Latenzbasiertes Routing.

Wenn Sie nur in einer AWS-Region über Ressourcen verfügen, können Sie Ressourcen in mehr als einer AWS-Region konfigurieren und für jede Region einen Latenz-Ressourcendatensatz definieren. Weitere Informationen hierzu finden Sie unter Latenzbasiertes Routing.

Wenn Sie nicht mehrere AWS-Regionen verwenden möchten, sollten Sie einen einfachen Ressourcendatensatz verwenden. Weitere Informationen finden Sie unter Arbeiten mit Ressourcendatensätzen.

Weitere Ressourcen

- Entwicklerhandbuch zu Amazon Route 53
- Preise für Amazon Route 53

Berichtsspalten

- Name der gehosteten Zone
- ID der gehosteten Zone

- Name des Ressourcendatensatzes
- Typ des Ressourcendatensatzes

Amazon-S3-Bucket-Lebenszyklus-Richtlinie konfiguriert

Beschreibung

Überprüft, ob für einen Amazon-S3-Bucket eine Lebenszyklus-Richtlinie konfiguriert wurde. Eine Amazon-S3-Lebenszyklus-Richtlinie stellt sicher, dass Amazon-S3-Objekte innerhalb des Buckets während des gesamten Lebenszyklus kostengünstig gespeichert werden. Dies ist wichtig, um die gesetzlichen Anforderungen an die Aufbewahrung und Speicherung von Daten zu erfüllen. Die Richtlinienkonfiguration besteht aus einer Reihe von Regeln, mit denen Aktionen definiert werden, die der Amazon-S3-Service auf eine Gruppe von Objekten anwendet. Eine Lebenszyklus-Richtlinie ermöglicht es Ihnen, die Übertragung von Objekten auf kostengünstigere Speicherklassen oder das Löschen von Objekten zu automatisieren, wenn sie veralten. Sie können ein Objekt beispielsweise 30 Tage nach der Erstellung in den Amazon-S3-Standard-IA-Speicher oder nach einem Jahr auf Amazon S3 Glacier übertragen.

Sie können auch den Ablauf von Objekten so definieren, dass Amazon S3 das Objekt nach einem bestimmten Zeitraum in Ihrem Namen löscht.

Sie können die Prüfkonfiguration mithilfe der Parameter in Ihren AWS Config-Regeln anpassen.

Weitere Informationen finden Sie unter Verwalten Ihres Speicher-Lebenszyklus.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz100
```

Quelle

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

Warnungskriterien

Gelb: Für den Amazon-S3-Bucket ist keine Lebenszyklus-Richtlinie konfiguriert.

Empfohlene Aktion

Stellen Sie sicher, dass in Ihrem Amazon-S3-Bucket eine Lebenszyklus-Richtlinie konfiguriert ist.

Wenn Ihr Unternehmen keine Aufbewahrungsrichtlinie eingerichtet hat, sollten Sie die Nutzung von Amazon S3 Intelligent-Tiering in Betracht ziehen, um die Kosten zu optimieren.

Informationen zur Definition Ihrer Amazon-S3-Lebenszyklus-Richtlinie finden Sie unter Festlegen der Lebenszykluskonfiguration für einen Bucket.

Informationen zu Amazon S3 Intelligent-Tiering finden Sie unter Amazon-S3-Intelligent-Tiering-Speicherklasse.

Weitere Ressourcen

Festlegen der Lebenszyklus-Konfiguration für einen Bucket

Beispiele der S3-Lebenszyklus-Konfiguration

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config-Regel
- Eingabeparameter

Konfiguration für unvollständigen mehrteiligen Upload-Abbruch in Amazon S3

Beschreibung

Prüft, ob jeder Amazon S3-Bucket mit einer Lebenszyklusregel konfiguriert ist, um mehrteilige Uploads abzubrechen, die nach 7 Tagen unvollständig bleiben. Es wird empfohlen, eine Lebenszyklusregel zu verwenden, um diese unvollständigen Uploads abzubrechen und den zugehörigen Speicher zu löschen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden einmal oder mehrmals täglich automatisch aktualisiert, und Aktualisierungsanforderungen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1cj39rr6v`

Warnungskriterien

Gelb: Der Lebenszykluskonfigurations-Bucket enthält keine Lebenszyklusregel, um alle mehrteiligen Uploads abzubrechen, die nach 7 Tagen unvollständig bleiben.

Empfohlene Aktion

Überprüfen Sie die Lebenszykluskonfiguration für Buckets ohne Lebenszyklusregel, die alle unvollständigen mehrteiligen Uploads bereinigt. Es ist unwahrscheinlich, dass Uploads, die nach 24 Stunden nicht abgeschlossen werden, abgeschlossen werden. Klicken Sie hier, um den Anweisungen zum Erstellen einer Lebenszyklusregel zu folgen. Es wird empfohlen, dies auf alle Objekte in Ihrem Bucket anzuwenden. Wenn Sie andere Lebenszyklusaktionen auf ausgewählte Objekte in Ihrem Bucket anwenden müssen, können Sie mehrere Regeln mit unterschiedlichen Filtern haben. Weitere Informationen finden Sie im Speicher-Lensen-Dashboard oder in der ListMultipartUpload API.

Weitere Ressourcen

- Erstellen einer Lebenszykluskonfiguration
- Erkennen und Löschen unvollständiger mehrteiliger Uploads zur Senkung der Amazon S3-Kosten
- Hochladen und Kopieren von Objekten mit mehrteiligem Upload
- Elemente der Lebenszykluskonfiguration
- Elemente zur Beschreibung von Lebenszyklusaktionen
- Lebenszykluskonfiguration zum Abbrechen mehrteiliger Uploads

Berichtsspalten

- Status
- Region
- Bucket-Name
- Bucket-ARN
- Lebenszyklusregel zum Löschen unvollständiger MPU
- Tage nach Initiierung
- Zeitpunkt der letzten Aktualisierung

Amazon-S3-versionsfähige Buckets ohne konfigurierte Lebenszyklus-Richtlinien

Beschreibung

Prüft, ob für Amazon-S3-versionsfähige Buckets eine Lebenszyklus-Richtlinie konfiguriert ist.

Weitere Informationen finden Sie unter Verwalten Ihres Speicher-Lebenszyklus.

Sie können die Bucket-Namen, die Sie überprüfen möchten, mithilfe der BucketNames-Parameter in Ihren AWS Config-Regeln angeben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz171`

Quelle

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

Warnungskriterien

Gelb: Ein Amazon-S3-versionsfähiger Bucket, für den keine Lebenszyklus-Richtlinie konfiguriert ist.

Empfohlene Aktion

Konfigurieren Sie Lebenszyklus-Richtlinien für Ihre Amazon-S3-Buckets, um Ihre Objekte so zu verwalten, dass diese während ihres gesamten Lebenszyklus kosteneffizient gespeichert werden.

Weitere Informationen finden Sie unter Festlegen der Lebenszyklus-Konfiguration für einen Bucket.

Weitere Ressourcen

Verwalten Ihres Speicher-Lebenszyklus

Festlegen der Lebenszyklus-Konfiguration für einen Bucket

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config-Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Lambda Funktionen mit übermäßigen Timeouts

Beschreibung

Prüft auf Lambda-Funktionen mit hohen Timeout-Quoten, die zu hohen Kosten führen können.

Lambda wird nach Laufzeit und Anzahl der Anfragen für Ihre Funktion berechnet. Funktions-Timeouts führen zu Fehlern, die Wiederholungsversuche verursachen können. Bei der Wiederholung von Funktionen fallen zusätzliche Gebühren für die Anfrage und die Laufzeit an.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

L4dfs2Q3C3

Warnungskriterien

Gelb: Funktionen, bei denen > 10 % der Aufrufe an einem bestimmten Tag innerhalb der letzten 7 Tage aufgrund eines Timeouts zu einem Fehler geführt haben.

Empfohlene Aktion

Untersuchen Sie die Funktionsprotokollierung und X-Ray-Ablaufverfolgungen, um festzustellen, was zu der hohen Funktionsdauer beigetragen hat. Implementieren Sie die Protokollierung Ihres Codes an relevanten Stellen, z. B. vor oder nach API-Aufrufen oder Datenbankverbindungen. Standardmäßig können die Timeouts von AWS-SDK-Clients länger als die konfigurierte Funktionsdauer sein. Passen Sie die API- und SDK-Verbindungsclients so an, dass der Verbindungsvorgang innerhalb des Funktionstimeouts erneut versucht wird oder fehlschlägt. Wenn die erwartete Dauer länger als der konfigurierte Timeout ist, können Sie die Timeout-Einstellung für die Funktion erhöhen. Weitere Informationen finden Sie unter Überwachung von und Fehlerbehebung bei Lambda-Anwendungen.

Weitere Ressourcen

- Überwachung von und Fehlerbehebung bei Lambda-Anwendungen
- Lambda-Funktion: Timeout-SDK erneut versuchen
- Verwenden von AWS Lambda mit AWS X-Ray
- Zugriff auf Amazon- CloudWatch Protokolle für AWS Lambda
- Fehlerverarbeitungs-Beispielanwendung für AWS Lambda

Berichtsspalten

- Status
- Region
- Funktion-ARN
- Max. tägliche Timeout-Rate
- Datum der max. täglichen Timeout-Rate
- Durchschnittliche tägliche Timeout-Rate
- Einstellungen für Funktionstimeout (Millisekunden)
- Entgangene tägliche Rechenkosten

- Durchschnittliche tägliche Aufrufe
- Aufrufe für den aktuellen Tag
- Timeout-Rate für den aktuellen Tag
- Zeitpunkt der letzten Aktualisierung

AWS Lambda Funktionen mit hohen Fehlerraten

Beschreibung

Prüft auf Lambda-Funktionen mit hohen Fehlerquoten, die zu höheren Kosten führen könnten.

Die Lambda-Gebühren basieren auf der Anzahl der Anfragen und der Gesamtlaufzeit für Ihre Funktion. Bei Funktionsfehlern kann es zu Wiederholungsversuchen kommen, die zusätzliche Kosten verursachen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`L4dfs2Q3C2`

Warnungskriterien

Gelb: Funktionen, bei denen > 10 % der Aufrufe an einem bestimmten Tag innerhalb der letzten 7 Tage zu einem Fehler geführt haben.

Empfohlene Aktion

Halten Sie sich an die folgenden Richtlinien, um Fehler zu reduzieren. Zu Funktionsfehlern gehören Fehler, die vom Code der Funktion zurückgegeben werden, sowie Fehler, die von der Laufzeit der Funktion zurückgegeben werden.

Um Sie bei der Behebung von Lambda-Fehlern zu unterstützen, lässt sich Lambda in -Services wie Amazon CloudWatch und integrierenAWS X-Ray. Sie können mithilfe einer Kombination

aus Protokollen, Metriken, Alarmen und der X-Ray-Nachverfolgung Probleme in Funktionscode, API und anderen Ressourcen, die für Ihre Anwendung erforderlich sind, schnell erkennen und aufdecken. Weitere Informationen finden Sie unter Überwachung von und Fehlerbehebung bei Lambda-Anwendungen.

Weitere Informationen zur Behandlung von Fehlern mit bestimmten Laufzeiten finden Sie unter Fehlerbehandlung und automatische Wiederholungen in AWS Lambda.

Weitere Informationen zur Fehlerbehebung finden Sie unter Beheben von Problemen in Lambda.

Sie haben außerdem die Wahl aus einem Ökosystem von Überwachungs- und Beobachtbarkeitstools, die von AWS Lambda-Partnern bereitgestellt werden. Weitere Informationen finden Sie unter AWS Lambda-Partner.

Weitere Ressourcen

- Fehlerbehandlung und automatische Wiederholungen in AWS Lambda
- Überwachung von und Fehlerbehebung bei Lambda-Anwendungen
- Lambda-Funktion: Timeout-SDK erneut versuchen
- Beheben von Problemen in Lambda
- API-Aufruffehler
- Fehlerverarbeitungs-Beispielanwendung für AWS Lambda

Berichtsspalten

- Status
- Region
- Funktion-ARN
- Max. tägliche Fehlerrate
- Datum für max. Fehlerrate
- Durchschnittliche tägliche Fehlerrate
- Entgangene tägliche Rechenkosten
- Durchschnittliche tägliche Aufrufe
- Aufrufe für den aktuellen Tag

  Fehlerrate für den aktuellen Tag
- Zeitpunkt der letzten Aktualisierung

AWS Lambda stellt zu viele Funktionen für die Speichergröße bereit

Beschreibung

Überprüft die Funktionen von AWS Lambda, die während des Lookback-Zeitraums mindestens einmal aufgerufen wurden. Diese Überprüfung warnt Sie, wenn eine Ihrer Lambda-Funktionen für die Speichergröße übermäßig bereitgestellt wurde. Wenn Sie über Lambda-Funktionen verfügen, die für Speichergrößen übermäßig bereitgestellt werden, zahlen Sie für ungenutzte Ressourcen. Obwohl einige Szenarien von vornherein zu einer geringen Auslastung führen können, lassen sich die Kosten oft senken, indem Sie die Speicherkonfiguration Ihrer Lambda-Funktionen ändern. Die geschätzten monatlichen Einsparungen werden anhand der aktuellen Nutzungsrate für Lambda-Funktionen berechnet.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`COr6dfpM05`

Warnungskriterien

Gelb: Eine Lambda-Funktion, die während des Lookback-Zeitraums für die Speichergröße nicht ausgelastet war. Um festzustellen, ob eine Lambda-Funktion übermäßig bereitgestellt wird, berücksichtigen wir alle CloudWatch Standardmetriken für diese Funktion. Der Algorithmus, der zur Identifizierung nicht ausgelasteter Lambda-Funktionen verwendet wird, folgt bewährten Methoden für AWS. Der Algorithmus wird aktualisiert, wenn ein neues Muster identifiziert wurde.

Empfohlene Aktion

Ziehen Sie in Erwägung, die Arbeitsspeichergröße Ihrer Lambda-Funktionen zu reduzieren.

Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Berichtsspalten

- Status

- Region
- Funktionsname
- Funktionsversion
- Speichergröße (MB)
- Empfohlene Speichergröße (MB)
- Lookback-Zeitraum (in Tagen)
- Einsparmöglichkeiten (in %)
- Geschätzte monatliche Einsparungen
- Währung der geschätzten monatlichen Einsparungen
- Zeitpunkt der letzten Aktualisierung

AWS Well-Architected-Probleme mit hohem Risiko für die Kostenoptimierung

Beschreibung

Prüft auf Probleme mit hohem Risiko (HRI) für Ihre Workloads hinsichtlich der Kostenoptimierung. Diese Prüfung basiert auf Ihren AWS-Well Architected-Beurteilungen. Ihre Prüfergebnisse hängen davon ab, ob Sie die Workload-Bewertung mit AWS Well-Architected durchgeführt haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Wxdfp4B1L1`

Warnungskriterien

- Rot: Mindestens ein aktives Problem mit hohem Risiko wurde hinsichtlich der Kostenoptimierung für AWS Well-Architected erkannt.
- Grün: Hinsichtlich der Kostenoptimierung wurden keine aktiven Probleme mit hohem Risiko für AWS Well-Architected erkannt.

Empfohlene Aktion

AWS Well-Architected hat während Ihrer Workload-Bewertung Probleme mit hohem Risiko erkannt. Diese Probleme bieten Möglichkeiten, Risiken zu reduzieren und Geld zu sparen. Melden Sie sich bei AWS Well-Architected an, um Ihre Antworten zu überprüfen und Maßnahmen zur Lösung der aktiven Probleme zu ergreifen.

Berichtsspalten

- Status
- Region
- Workload-ARN
- Name der Workload
- Name des Reviewers
- Workload-Typ
- Startdatum der Workload
- Datum der letzten Änderung der Workload
- Anzahl der identifizierten HRI für die Kostenoptimierung
- Anzahl der behobenen HRI für die Kostenoptimierung
- Anzahl der für die Kostenoptimierung beantworteten Fragen
- Gesamtzahl der Fragen hinsichtlich der Kostenoptimierung
- Zeitpunkt der letzten Aktualisierung

Load Balancer im Leerlauf

Beschreibung

Prüft Ihre Elastic Load Balancing-Konfiguration auf Lastverteilungen, die im Leerlauf sind.

Für jeden konfigurierten Load Balancer fallen Gebühren an. Wenn ein Load Balancer keine zugehörigen Back-End-Instances hat oder der Netzwerkverkehr stark eingeschränkt ist, wird der Load Balancer nicht effektiv genutzt. Dieser Prüfung prüft derzeit nur auf den Typ Classic Load Balancer innerhalb des ELB-Dienstes. Andere ELB-Typen (Application Load Balancer, Network Load Balancer) sind hier nicht enthalten.

Prüf-ID

`hjLMh88uM8`

Warnungskriterien

- Gelb: Ein Load Balancer hat keine aktiven Backend-Instances.
- Gelb: Ein Load Balancer hat keine funktionsfähigen Backend-Instances.
- Gelb: Ein Load Balancer hat in den letzten 7 Tagen weniger als 100 Anfragen pro Tag erhalten.

Empfohlene Aktion

Wenn Ihr Load Balancer keine aktiven Backend-Instances hat, sollten Sie Instances registrieren oder Ihren Load Balancer löschen Weitere Informationen finden Sie unter Registering Your Amazon EC2 Instances with Your Load Balancer (Registrieren Ihrer Amazon-EC2-Instances mit Ihrem Load Balancer) oder Löschen des Load Balancers.

Wenn Ihr Load Balancer keine funktionsfähigen Backend-Instances hat, finden Sie weitere Informationen unter Troubleshooting Elastic Load Balancing: Health Check Configuration (Fehlerbehebung bei Elastic Load Balancing: Zustandsprüfungskonfiguration).

Wenn Ihr Load Balancer eine geringe Anzahl von Anfragen erhalten hat, sollten Sie erwägen, Ihren Load Balancer zu löschen. Weitere Informationen finden Sie unter Löschen des Load Balancers.

Weitere Ressourcen

- Managing Load Balancers (Verwalten von Load Balancern)
- Troubleshoot Elastic Load Balancing (Fehlerbehebung bei Elastic Load Balancing)

Berichtsspalten

- Region
- Load-Balancer-Name
- Grund
- Geschätzte monatliche Einsparungen

Low Utilization Amazon EC2 Instances

Beschreibung

Prüft die Amazon Elastic Compute Cloud (Amazon EC2) Instances, die zu einem beliebigen Zeitpunkt in den letzten 14 Tagen ausgeführt wurden. Diese Prüfung warnt Sie, wenn die tägliche CPU-Auslastung 10 % oder weniger und die Netzwerk-I/O 5 MB oder weniger an mindestens 4 Tagen betrug.

Laufende Instances erzeugen stündliche Nutzungsgebühren. Obwohl einige Szenarien von vornherein zu einer geringen Auslastung führen können, lassen sich die Kosten oft senken, indem Sie die Anzahl und Größe Ihrer Instances verwalten.

Die geschätzten monatlichen Einsparungen werden anhand der aktuellen Nutzungsrate für On-Demand-Instances und der geschätzten Anzahl der Tage, an denen die Instance nicht ausgelastet ist, berechnet. Die tatsächlichen Einsparungen variieren, wenn Sie Reserved Instances oder Spot Instances verwenden oder wenn die Instance nicht einen ganzen Tag lang läuft. Um tägliche Nutzungsdaten zu erhalten, laden Sie den Bericht für diese Prüfung herunter.

Prüf-ID

`Qch7DwouX1`

Warnungskriterien

Gelb: Eine Instance hatte an mindestens 4 der letzten 14 Tage eine durchschnittliche CPU-Auslastung von 10 % oder weniger und eine Netzwerk-E/A von 5 MB oder weniger.

Empfohlene Aktion

Erwägen Sie, Instances mit geringer Auslastung anzuhalten oder zu beenden, oder skalieren Sie die Anzahl der Instances mithilfe von Auto Scaling. Weitere Informationen finden Sie unter Anhalten und Starten der Instance, Beenden Ihrer Instance und Was ist Auto Scaling?

Weitere Ressourcen

- Überwachen von Amazon EC2
- Instance-Metadaten und Benutzerdaten
- Amazon CloudWatch -Benutzerhandbuch
- Auto-Scaling-Entwicklerhandbuch

Berichtsspalten

- Region/AZ
- Instance-ID
- Instance-Name
- Instance-Typ
- Geschätzte monatliche Einsparungen
- CPU-Auslastung im 14-Tage-Durchschnitt
- Netzwerk-E/A im 14-Tage-Durchschnitt

- Anzahl der Tage mit niedriger Auslastung

Savings Plan

Beschreibung

Überprüft Ihre Nutzung von Amazon EC2, Fargate und Lambda in den letzten 30 Tagen und gibt Empfehlungen zum Kauf von Savings Plans. Mit diesen Empfehlungen können Sie sich für einen Zeitraum von einem oder drei Jahren auf eine gleichbleibende Nutzungsmenge in Dollar pro Stunde festlegen und erhalten dafür vergünstigte Tarife.

Diese stammen aus dem AWS Cost Explorer, der detailliertere Informationen zu den Empfehlungen liefern kann. Sie können auch einen Savings Plan über Cost Explorer erwerben. Diese Empfehlungen sollten als Alternative zu Ihren RI-Empfehlungen betrachtet werden. Wir schlagen vor, dass Sie nur eine Reihe von Empfehlungen befolgen. Wenn man sich auf beide Gruppen einlässt, kann man sich zu sehr verpflichten.

Diese Prüfung ist nicht für Konten verfügbar, die mit einer konsolidierten Abrechnung verbunden sind. Die Empfehlungen für diese Prüfung sind nur für das Zahlungskonto verfügbar.

Prüf-ID

`vZ2c2W1srf`

Warnungskriterien

Gelb: Die Optimierung des Kaufs von Savings Plans kann zur Kostensenkung beitragen.

Empfohlene Aktion

Auf der Seite Cost Explorer finden Sie detailliertere und individuelle Empfehlungen und Informationen zum Kauf von Savings Plans.

Weitere Ressourcen

- Savings-Plans-Benutzerhandbuch
- Häufig gestellte Fragen zu Savings Plans

Berichtsspalten

- Savings-Plan-Typ
- Zahlungsoption
- Vorauszahlungskosten

- Stündliche Verpflichtung zum Kauf
- Geschätzte durchschnittliche Auslastung
- Geschätzte monatliche Einsparungen
- Geschätzter Einsparungen in Prozent
- Laufzeit (in Jahren)
- Lookback-Zeitraum (in Tagen)

Nicht zugeordnete elastische IP-Adressen

Beschreibung

Prüft auf elastische IP-Adressen (EIPs), die nicht mit einer laufenden Amazon Elastic Compute Cloud (Amazon EC2)-Instance verbunden sind.

EIPs sind statische IP-Adressen, die für dynamisches Cloud-Computing entwickelt wurden. Im Gegensatz zu herkömmlichen statischen IP-Adressen maskieren EIPs den Ausfall einer Instance oder Availability Zone, indem sie eine öffentliche IP-Adresse einer anderen Instance in Ihrem Konto zuordnen. Für eine EIP, die nicht mit einer ausgeführten Instance verbunden ist, wird eine geringe Gebühr erhoben.

Prüf-ID

`Z4AUBRNSmz`

Warnungskriterien

Gelb: Eine zugewiesene Elastic-IP-Adresse (EIP) ist keiner ausgeführten Amazon-EC2-Instance zugeordnet.

Empfohlene Aktion

Ordnen Sie die EIP einer ausgeführten aktiven Instance zu oder geben Sie die nicht zugeordnete EIP frei. Weitere Informationen finden Sie unter Zuordnen einer Elastic-IP-Adresse zu einer Instance oder Netzwerkschnittstelle und Freigeben einer Elastic-IP-Adresse.

Weitere Ressourcen

Elastic IP-Adressen

Berichtsspalten

- Region

- IP-Adresse

Nicht ausgelastete Amazon EBS-Volumes

Beschreibung

Prüft Amazon Elastic Block Store (Amazon EBS) Volume-Konfigurationen und warnt, wenn Volumes nicht ausgelastet zu sein scheinen.

Die Gebühren beginnen, wenn ein Volume erstellt wird. Wenn ein Volume über einen bestimmten Zeitraum nicht angeschlossen ist oder nur eine sehr geringe Schreibaktivität aufweist (ausgenommen Boot-Volumes), ist das Volume nicht ausgelastet. Wir empfehlen Ihnen, nicht ausgelastete Volumes zu entfernen, um die Kosten zu senken.

Prüf-ID

`DAvU99Dc4C`

Warnungskriterien

Gelb: Ein Volume ist nicht verbunden oder hatte in den letzten 7 Tagen weniger als 1 IOPS pro Tag.

Empfohlene Aktion

Ziehen Sie in Erwägung, einen Snapshot zu erstellen und das Volume zu löschen, um Kosten zu senken. Weitere Informationen finden Sie unter Erstellen von Amazon-EBS-Snapshots und Löschen eines Amazon-EBS-Volumes.

Weitere Ressourcen

- Amazon Elastic Block Store (Amazon EBS)
- Überwachen des Status Ihrer Volumes

Berichtsspalten

- Region
- Volume-ID
- Volume-Name
- Volume-Typ
- Volume-Größe
- Monatliche Speicherkosten
- Snapshot-ID

- Snapshot-Name
- Snapshot-Alter

> **Note**
>
> Wenn Sie sich für Ihr Konto für AWS Compute Optimizer entschieden haben, empfehlen wir Ihnen, stattdessen die Überprüfung für nicht ausgelastete Amazon-EBS-Volumes durchzuführen. Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Nicht ausgelastete Amazon Redshift-Cluster

Beschreibung

Prüft Ihre Amazon Redshift-Konfiguration auf Cluster, die nicht ausgelastet zu sein scheinen.

Wenn ein Amazon Redshift-Cluster über einen längeren Zeitraum keine Verbindung hatte oder nur eine geringe CPU-Auslastung aufweist, können Sie kostengünstigere Optionen nutzen, wie z. B. die Verkleinerung des Clusters oder das Herunterfahren des Clusters und Erstellen eines letzten Snapshots. Die endgültigen Snapshots bleiben auch nach dem Löschen des Clusters erhalten.

Prüf-ID

`G31sQ1E9U`

Warnungskriterien

- Gelb: Ein ausgeführter Cluster hat in den letzten 7 Tagen keine Verbindung hergestellt.
- Gelb: Ein laufender Cluster hatte in 99 % der letzten 7 Tage eine clusterweite durchschnittliche CPU-Auslastung von weniger als 5 %.

Empfohlene Aktion

Erwägen Sie, den Cluster herunterzufahren und einen abschließenden Snapshot zu erstellen oder den Cluster zu verkleinern. Weitere Informationen finden Sie unter Schließen und Löschen von Clustern und Größenanpassung eines Clusters.

Weitere Ressourcen

Amazon CloudWatch -Benutzerhandbuch

Berichtsspalten

- Status
- Region
- Cluster
- Instance-Typ
- Grund
- Geschätzte monatliche Einsparungen

Leistung

Verbessern Sie die Leistung Ihres Dienstes, indem Sie Ihre Service Quotas (früher als Limits bezeichnet) überprüfen, so dass Sie die Vorteile des bereitgestellten Durchsatzes nutzen, überlastete Instances überwachen und ungenutzte Ressourcen erkennen können.

Sie können die folgenden Prüfungen für die Leistungskategorie verwenden.

Namen prüfen

- Amazon Aurora Aurora-DB-Cluster mit unzureichender Bereitstellung für Lese-Workloads
- Amazon DynamoDB Auto Scaling nicht aktiviert
- Amazon EBS-Optimierung nicht aktiviert
- Amazon EBS bereitgestellte IOPS (SSD) Volume Attachment Konfiguration
- Amazon EBS mit überlasteten Volumes
- Amazon EC2 Auto Scaling-Gruppe ist keiner Startvorlage zugeordnet
- Amazon EC2 to EBS-Durchsatzoptimierung
- Der EC2-Virtualisierungstyp ist paravirtual
- Hard-Limit des Amazon ECS-Speichers
- Amazon EFS – Optimierung des Durchsatzmodus
- Der Amazon RDS-Autovakuum-Parameter ist ausgeschaltet
- Amazon RDS-DB-Cluster unterstützen nur ein Volumen von bis zu 64 TiB
- Amazon RDS-DB-Instances in den Clustern mit heterogenen Instance-Klassen
- Amazon RDS-DB-Instances in den Clustern mit heterogenen Instance-Größen
- Die Speicherparameter von Amazon RDS DB weichen vom Standard ab

- Der Amazon RDS-Parameter enable_indexonlyscan ist ausgeschaltet
- Der Amazon RDS-Parameter enable_indexscan ist ausgeschaltet
- Der Amazon RDS-Parameter general_logging ist aktiviert
- Der Amazon RDS-Parameter InnoDB_Change_Buffering verwendet weniger als den optimalen Wert
- Der Amazon RDS-Parameter innodb_open_files ist niedrig
- Der Amazon RDS-Parameter innodb_stats_persistent ist ausgeschaltet
- Amazon RDS-Instance mit unzureichender Systemkapazität
- Amazon RDS Magnetic Volume wird verwendet
- Amazon RDS-Parametergruppen verwenden keine riesigen Seiten
- Der Amazon RDS-Abfrage-Cache-Parameter ist aktiviert
- Eine Aktualisierung der Amazon RDS-Ressourcen-Instance-Klasse ist erforderlich
- Aktualisierung der Hauptversionen von Amazon RDS-Ressourcen ist erforderlich
- Amazon RDS-Ressourcen, die die End-of-Support-Engine-Edition im Rahmen der inbegriffenen Lizenz verwenden
- Amazon Route 53 Alias Ressourceneintragsätze
- AWS Lambda stellt zu wenig Funktionen für die Speichergröße bereit
- AWS Lambda Funktionen ohne Parallelitätslimit konfiguriert
- AWS Well-Architected-Probleme mit hohem Risiko für die Leistung
- CloudFront Alternative Domainnamen
- CloudFront Optimierung der Inhaltsbereitstellung
- CloudFront Header-Weiterleitung und Cache-Trefferquote
- Hohe Nutzung Amazon-EC2-Instances

Amazon Aurora Aurora-DB-Cluster mit unzureichender Bereitstellung für Lese-Workloads

Beschreibung

Prüft, ob der Amazon Aurora Aurora-DB-Cluster über die Ressourcen verfügt, um einen Lese-Workload zu unterstützen.

Prüf-ID

`c1qf5bt038`

Warnungskriterien

Gelb:

Zunehmende Datenbanklesevorgänge: Die Datenbanklast war hoch und die Datenbank hat mehr Zeilen gelesen als Zeilen geschrieben oder aktualisiert.

Empfohlene Aktion

Wir empfehlen Ihnen, Ihre Abfragen zu optimieren, um die Datenbanklast zu verringern, oder Ihrem DB-Cluster eine Reader-DB-Instance mit derselben Instance-Klasse und Größe wie die Writer-DB-Instance im Cluster hinzuzufügen. Die aktuelle Konfiguration umfasst mindestens eine DB-Instance mit einer kontinuierlich hohen Datenbanklast, die hauptsächlich durch Lesevorgänge verursacht wird. Verteilen Sie diese Operationen, indem Sie dem Cluster eine weitere DB-Instance hinzufügen und die Lese-Arbeitslast an den schreibgeschützten Endpunkt des DB-Clusters weiterleiten.

Weitere Ressourcen

Ein Aurora-DB-Cluster hat einen Leser-Endpunkt für schreibgeschützte Verbindungen. Dieser Endpunkt verwendet Lastenausgleich, um die Abfragen zu verwalten, die am meisten zur Datenbanklast in Ihrem DB-Cluster beitragen. Der Reader-Endpunkt leitet diese Anweisungen an die Aurora Read Replicas weiter und reduziert die Belastung der primären Instance. Der Reader-Endpunkt skaliert auch die Kapazität zur Verarbeitung gleichzeitiger SELECT-Abfragen mit der Anzahl der Aurora Read Replicas im Cluster.

Weitere Informationen finden Sie unter Hinzufügen von Aurora Replicas zu einem DB-Cluster und Verwaltung der Leistung und Skalierung für Aurora-DB-Cluster.

Berichtsspalten

- Status
- Region
- Ressource
- Erhöhung der Anzahl der Datenbanklesevorgänge
- Letzter Erkennungszeitraum

- Zeitpunkt der letzten Aktualisierung

Amazon DynamoDB Auto Scaling nicht aktiviert

Beschreibung

Überprüft, ob für Ihre Amazon-DynamoDB-Tabellen und globalen sekundären Indizes Auto Scaling oder On-Demand aktiviert ist.

Amazon DynamoDB-Auto-Scaling verwendet den Application-Auto-Scaling-Service, um die bereitgestellte Durchsatzkapazität in Ihrem Namen als Reaktion auf tatsächliche Datenverkehrsmuster dynamisch anzupassen. Auf diese Weise kann eine Tabelle oder ein globaler sekundärer Index ihre bereitgestellte Lese- und Schreibkapazität erhöhen, um plötzliche Erhöhungen des Datenverkehrs ohne Drosselung zu bewältigen. Wenn der Workload abnimmt, senkt Application Auto Scaling Auto Scaling den Durchsatz, sodass Sie für ungenutzte Kapazität nicht zahlen müssen.

Sie können die Prüfkonfiguration mithilfe der Parameter in Ihren AWS Config Regeln anpassen.

Weitere Informationen finden Sie unter Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz136`

Quelle

AWS Config Verwaltete Regel: dynamodb-autoscaling-enabled

Warnungskriterien

Gelb: Auto Scaling ist für Ihre DynamoDB-Tabellen und/oder globalen sekundären Indizes nicht aktiviert.

Empfohlene Aktion

Wenn Sie nicht bereits über einen Mechanismus zur automatischen Skalierung des bereitgestellten Durchsatzes Ihrer DynamoDB-Tabelle und/oder globalen sekundären Indizes auf der Grundlage Ihrer Workload-Anforderungen verfügen, sollten Sie Auto Scaling für Ihre Amazon-DynamoDB-Tabellen aktivieren.

Weitere Informationen finden Sie unter Verwendung der AWS-Managementkonsole mit DynamoDB Auto Scaling.

Weitere Ressourcen

Automatische Verwaltung der Durchsatzkapazität mit DynamoDB-Auto-Scaling

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EBS-Optimierung nicht aktiviert

Beschreibung

Überprüft, ob die Amazon EBS-Optimierung für Ihre Amazon EC2-Instances aktiviert ist.

Eine Amazon EBS-optimierte Instance nutzt einen optimierten Konfigurations-Stack und bietet zusätzliche dedizierte Kapazität für I/O-Vorgänge in Amazon EBS. Diese Optimierung bietet die beste Leistung für Ihre Amazon EBS-Volumes, indem Konflikte zwischen I/O-Vorgängen in Amazon EBS und anderem Datenverkehr von Ihrer Instance minimiert werden.

Weitere Informationen finden Sie unter Amazon EBS-optimierte Instances.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

c18d2gz142

Quelle

AWS Config Verwaltete Regel: ebs-optimized-instance

Warnungskriterien

Gelb: Die Amazon EBS-Optimierung ist auf unterstützten Amazon EC2-Instances nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die Amazon EBS-Optimierung für unterstützte Instances.

Weitere Informationen finden Sie unter Aktivieren der EBS-Optimierung beim Start.

Weitere Ressourcen

Amazon EBS-optimierte Instances

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EBS bereitgestellte IOPS (SSD) Volume Attachment Konfiguration

Beschreibung

Prüft auf bereitgestellte IOPS (SSD)-Volumes, die an eine Amazon EBS-optimierbare Amazon Elastic Compute Cloud (Amazon EC2)-Instance angeschlossen sind, die nicht EBS-optimiert ist.

Bereitgestellte IOPS-Volumes (SSD) im Amazon Elastic Block Store (Amazon EBS) sind so konzipiert, dass sie nur dann die erwartete Leistung erbringen, wenn sie mit einer EBS-optimierten Instance verbunden sind.

Prüf-ID

`PPkZrjsH2q`

Warnungskriterien

Gelb: Eine Amazon-EC2-Instance, die EBS-optimiert werden kann, hat ein angehängtes bereitgestelltes IOPS-(SSD)-Volume, doch die Instance ist nicht EBS-optimiert.

Empfohlene Aktion

Erstellen Sie eine neue Instance, die EBS-optimiert ist, trennen Sie das Volume und fügen Sie das Volume erneut an Ihre neue Instance an. Weitere Informationen finden Sie unter Amazon-EBS-optimierte Instances und Zuordnen eines Amazon-EBS-Volumes zu einer Instance.

Weitere Ressourcen

- Amazon-EBS-Volume-Typen
- Leistung von Amazon-EBS-Volumes

Berichtsspalten

- Status
- Region/AZ
- Volume-ID
- Volume-Name
- Anhang des Volumes
- Instance-ID
- Instance-Typ
- Für EBS optimiert

Amazon EBS mit überlasteten Volumes

Beschreibung

Prüft die Amazon Elastic Block Store (Amazon EBS)-Volumes, die zu einem beliebigen Zeitpunkt während des Lookback-Zeitraums ausgeführt wurden. Diese Überprüfung warnt Sie, wenn eine zu geringe Kapazität für EBS-Volumes für Ihre Workloads bereitgestellt wurde. Eine gleichbleibend

hohe Auslastung kann auf eine optimierte, stetige Leistung oder darauf hinweisen, dass eine Anwendung nicht über genügend Ressourcen verfügt.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`C0r6dfpM04`

Warnungskriterien

Gelb: Ein EBS-Volume, das während des Lookback-Zeitraums überlastet war. Um festzustellen, ob ein Volume nicht ausreichend bereitgestellt ist, berücksichtigen wir alle CloudWatch Standardmetriken (einschließlich IOPS und Durchsatz). Der Algorithmus, der zur Identifizierung unzureichend bereitgestellter EBS-Volumes verwendet wird, folgt bewährten Methoden. AWS Der Algorithmus wird aktualisiert, wenn ein neues Muster identifiziert wurde.

Empfohlene Aktion

Sie sollten Volumes mit hoher Auslastung vergrößern.

Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Berichtsspalten

- Status
- Region
- Volume-ID
- Volume-Typ
- Volumegröße (GB)
- Volume-IOPS-Basisleistung
- Volume-IOPS-Spitzenleistung
- Volume-Spitzendurchsatz

- Empfohlener Volume-Typ
- Empfohlene Volume-Größe (GB)
- Empfohlene Volumen-IOPS-Basisleistung
- Empfohlene Volume-IOPS-Spitzenleistung
- Empfohlener Volume-Basisdurchsatz
- Empfohlener Volume-Spitzendurchsatz
- Lookback-Zeitraum (in Tagen)
- Leistungsrisiko
- Zeitpunkt der letzten Aktualisierung

Amazon EC2 Auto Scaling-Gruppe ist keiner Startvorlage zugeordnet

Beschreibung

Überprüft, ob eine Amazon EC2 Auto Scaling-Gruppe aus einer Amazon EC2-Startvorlage erstellt wurde.

Verwenden Sie eine Startvorlage zur Erstellung Ihrer Amazon EC2 Auto Scaling-Gruppen, um den Zugriff auf die neuesten Funktionen und Verbesserungen der Auto-Scaling-Gruppen sicherzustellen. Zum Beispiel Versionsverwaltung und mehrere Instance-Typen.

Weitere Informationen finden Sie unter Startvorlagen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz102`

Quelle

AWS Config Verwaltete Regel: autoscaling-launch-template

Warnungskriterien

Gelb: Die Amazon EC2 Auto Scaling-Gruppe ist nicht mit einer gültigen Startvorlage verknüpft.

Empfohlene Aktion

Verwenden Sie eine Amazon EC2-Startvorlage, um Ihre Amazon EC2 Auto Scaling-Gruppen zu erstellen.

Weitere Informationen finden Sie unter Erstellen einer Startvorlage für eine Auto-Scaling-Gruppe.

Weitere Ressourcen

- Startvorlagen
- Erstellen einer Startvorlage

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EC2 to EBS-Durchsatzoptimierung

Beschreibung

Prüft auf Amazon EBS-Volumes, deren Leistung durch die maximale Durchsatzkapazität der Amazon EC2-Instance, an die sie angeschlossen sind, beeinträchtigt werden könnte.

Um die Leistung zu optimieren, sollten Sie sicherstellen, dass der maximale Durchsatz einer Amazon EC2-Instance größer ist als der maximale Gesamtdurchsatz der angeschlossenen EBS-Volumes. Diese Prüfung berechnet den gesamten EBS-Volumendurchsatz für jeden Fünf-Minuten-Zeitraum des vorangegangenen Tages (basierend auf Coordinated Universal Time (UTC)) für jede EBS-optimierte Instance und warnt Sie, wenn die Nutzung in mehr als der Hälfte dieser Zeiträume mehr als 95 % des maximalen Durchsatzes der EC2-Instance betrug.

Prüf-ID

`Bh2xRR2FGH`

Warnungskriterien

Gelb: Am Vortag (UTC) überstieg der aggregierte Durchsatz (Mbit/s) der an die EC2-Instance angeschlossenen EBS-Volumes in mehr als 50 % der Fälle 95 % des veröffentlichten Durchsatzes zwischen der Instance und den EBS-Volumes.

Empfohlene Aktion

Vergleichen Sie den maximalen Durchsatz Ihrer Amazon-EBS-Volumes (siehe Amazon-EBS-Volume-Typen) mit dem maximalen Durchsatz der Amazon-EC2-Instance, der sie zugeordnet sind. Weitere Informationen finden Sie unter Anzeigen von Instance-Typen, die EBS-Optimierung unterstützen.

Sie sollten Ihre Volumes einer Instance zuordnen, die einen höheren Durchsatz an Amazon-EBS unterstützt, um eine optimale Leistung zu erzielen.

Weitere Ressourcen

- Amazon-EBS-Volume-Typen
- Verwenden von Amazon EBS-optimierten Instances
- Überwachen des Status Ihrer Volumes
- Zuordnen eines Amazon-EBS-Volumes zu einer Instance
- Trennen eines Amazon-EBS-Volumes von einer Instance
- Löschen eines Amazon-EBS-Volumes

Berichtsspalten

- Status
- Region
- Instance-ID
- Instance-Typ
- Zeitpunkt in der Nähe des Maximums

Der EC2-Virtualisierungstyp ist paravirtual

Beschreibung

Prüft, ob der Virtualisierungstyp einer Amazon EC2-Instance paravirtual ist.

Wenn möglich, sollten Sie Hardware Virtual Machine (HVM)-Instances anstelle von paravirtualen Instances verwenden. Dies ist auf die Verbesserungen bei der HVM-Virtualisierung und die

Verfügbarkeit von PV-Treibern für HVM-AMIs zurückzuführen, die die Leistungslücke zwischen PV- und HVM-Gästen geschlossen haben, die in der Vergangenheit bestand. Es ist wichtig zu wissen, dass die Instances der aktuellen Generation keine PV-AMIs unterstützen. Daher bietet die Wahl eines HVM-Instance-Typs die beste Leistung und Kompatibilität mit moderner Hardware.

Weitere Informationen finden Sie unter Linux AMI-Virtualisierungstypen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz148`

Quelle

AWS Config Verwaltete Regel: ec2-paravirtual-instance-check

Warnungskriterien

Gelb: Der Virtualisierungstyp von Amazon EC2-Instances ist paravirtual.

Empfohlene Aktion

Verwenden Sie HVM-Virtualisierung für Ihre Amazon EC2-Instances und einen kompatiblen Instance-Typ.

Informationen zur Auswahl des geeigneten Virtualisierungstyps finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Weitere Ressourcen

Kompatibilität zum Ändern des Instance-Typs

Berichtsspalten

- Status
- Region
- Ressource

- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Hard-Limit des Amazon ECS-Speichers

Beschreibung

Überprüft, ob Amazon ECS-Aufgabendefinitionen ein festgelegtes Speicherlimit für ihre Containerdefinitionen haben. Der gesamte Arbeitsspeicher, der für alle Container in einer Aufgabe reserviert ist, muss niedriger sein als der Wert des Aufgabenspeichers.

Weitere Informationen finden Sie unter Containerdefinitionen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz176`

Quelle

AWS Config Verwaltete Regel: ecs-task-definition-memory -hard-limit

Warnungskriterien

Gelb: Das Hard-Limit des Amazon ECS-Speichers ist nicht festgelegt.

Empfohlene Aktion

Weisen Sie Ihren Amazon ECS-Aufgaben Speicher zu, um einen Speichermangel zu vermeiden. Wenn Ihr Container versucht, den angegebenen Speicherplatz zu überschreiten, wird der Container beendet.

Weitere Informationen finden Sie unter Wie kann ich Aufgaben in Amazon ECS Speicher zuweisen?.

Weitere Ressourcen

Cluster-Reservierung

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EFS – Optimierung des Durchsatzmodus

Beschreibung

Überprüft, ob das Amazon EFS-Dateisystem des Kunden derzeit für die Verwendung des Durchsatzmodus „Bursting“ konfiguriert ist.

Dateisysteme im EFS-Durchsatzmodus „Bursting“ [1] liefern ein konsistentes Basisdurchsatzniveau (50 KiB/s pro GiB Daten im EFS-Standardspeicher) und verwenden ein Guthabenmodell, um ein höheres Niveau an „Burst-Durchsatz“-Leistung zu liefern, wenn „Burst Credits“ verfügbar sind. Wenn Sie Ihr Burst-Guthaben aufgebraucht haben, wird die Leistung Ihres Dateisystems auf dieses niedrigere Basisniveau gedrosselt, was zu Langsamkeit, Zeitüberschreitungen oder anderen Formen von Leistungseinbußen für Ihre Endbenutzer oder Anwendungen führen kann.

Prüf-ID

`c1dfprch02`

Warnungskriterien

- Gelb: Das Dateisystem verwendet den Bursting-Durchsatzmodus.

Empfohlene Aktion

Damit Ihre Benutzer und Anwendungen den gewünschten Durchsatz erreichen können, empfehlen wir Ihnen, Ihre Dateisystemkonfiguration auf den elastischen Durchsatzmodus [2] zu aktualisieren. Im elastischen Durchsatzmodus kann Ihr Dateisystem einen Lesedurchsatz von bis zu 10 GiB/s oder einen Schreibdurchsatz von bis zu 3 GiB/s erreichen – je nach AWS-

Region [3], und Sie zahlen nur für den genutzten Durchsatz. Bitte beachten Sie, dass Sie Ihre Dateisystemkonfiguration aktualisieren können, um bei Bedarf zwischen den Durchsatzmodi „Elastic“ und „Bursting“ zu wechseln, und dass für Dateisysteme im Elastic-Durchsatzmodus zusätzliche Gebühren für die Datenübertragung anfallen [4].

Weitere Ressourcen

- [1] Leistungsdurchsatzmodi von Amazon EFS
- [2] Elastic-Leistungsdurchsatzmodus von Amazon EFS
- [3] Amazon-EFS-Kontingente und -Limits
- [4] Amazon EFS – Preise

Berichtsspalten

- Status
- Region
- EFS-Dateisystem-ID
- Durchsatzmodus
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Autovakuum-Parameter ist ausgeschaltet

Beschreibung

Der Autovacuum-Parameter ist für Ihre DB-Instances ausgeschaltet. Wenn Sie die automatische Vakuumierung ausschalten, wird die Tabelle und der Index größer und die Leistung beeinträchtigt.

Wir empfehlen, dass Sie Autovacuum in Ihren DB-Parametergruppen aktivieren.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt025`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist die automatische Bereinigung ausgeschaltet.

Empfohlene Aktion

Schalten Sie den Autovacuum-Parameter in Ihren DB-Parametergruppen ein.

Weitere Ressourcen

PostgreSQL PostgreSQL-Datenbank erfordert eine regelmäßige Wartung, die als Staubsaugen bezeichnet wird. Autovacuum in PostgreSQL automatisiert die Ausführung der Befehle VACUUM und ANALYZE. Dieser Prozess sammelt die Tabellenstatistiken und löscht die toten Zeilen. Wenn Autovacuum ausgeschaltet ist, wirken sich die Zunahme der Tabelle, der Index und veraltete Statistiken auf die Datenbankleistung aus.

Weitere Informationen finden Sie unter Grundlegendes zu Autovacuum in Amazon RDS for PostgreSQL PostgreSQL-Umgebungen.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters

- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Cluster unterstützen nur ein Volumen von bis zu 64 TiB

Beschreibung

Ihre DB-Cluster unterstützen Volumes bis zu 64 TiB. Die neuesten Engine-Versionen unterstützen Volumes bis zu 128 TiB. Wir empfehlen, dass Sie die Engine-Version Ihres DB-Clusters auf die neuesten Versionen aktualisieren, um Volumes bis zu 128 TiB zu unterstützen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt017`

Warnungskriterien

Gelb: DB-Cluster unterstützen nur Volumes bis zu 64 TiB.

Empfohlene Aktion

Aktualisieren Sie die Engine-Version Ihrer DB-Cluster, um Volumes bis zu 128 TiB zu unterstützen.

Weitere Ressourcen

Wenn Sie Ihre Anwendung auf einem einzelnen Amazon Aurora Aurora-DB-Cluster skalieren, erreichen Sie das Limit möglicherweise nicht, wenn das Speicherlimit 128 TiB beträgt. Das erhöhte Speicherlimit trägt dazu bei, das Löschen der Daten oder das Aufteilen der Datenbank auf mehrere Instances zu vermeiden.

Weitere Informationen finden Sie unter Amazon Aurora Aurora-Größenbeschränkungen.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Motors
- Aktuelle Motorversion
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Instances in den Clustern mit heterogenen Instance-Klassen

Beschreibung

Wir empfehlen, dass Sie dieselbe DB-Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster verwenden.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt009`

Warnungskriterien

Rot: DB-Cluster haben DB-Instances mit heterogenen Instance-Klassen.

Empfohlene Aktion

Verwenden Sie dieselbe Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster.

Weitere Ressourcen

Wenn die DB-Instances in Ihrem DB-Cluster unterschiedliche DB-Instance-Klassen oder -Größen verwenden, kann es zu einem Ungleichgewicht in der Arbeitslast der DB-Instances kommen. Während eines Failovers wird eine der Leser-DB-Instances in eine Writer-DB-Instance umgewandelt. Wenn die DB-Instances dieselbe DB-Instance-Klasse und Größe verwenden, kann die Arbeitslast für die DB-Instances in Ihrem DB-Cluster ausgeglichen werden.

Weitere Informationen finden Sie unter Aurora Replicas.

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors

- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Instances in den Clustern mit heterogenen Instance-Größen

Beschreibung

Wir empfehlen, dass Sie dieselbe DB-Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster verwenden.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt008`

Warnungskriterien

Rot: DB-Cluster haben DB-Instances mit heterogenen Instance-Größen.

Empfohlene Aktion

Verwenden Sie dieselbe Instance-Klasse und Größe für alle DB-Instances in Ihrem DB-Cluster.

Weitere Ressourcen

Wenn die DB-Instances in Ihrem DB-Cluster unterschiedliche DB-Instance-Klassen oder -Größen verwenden, kann es zu einem Ungleichgewicht in der Arbeitslast der DB-Instances kommen. Während eines Failovers wird eine der Leser-DB-Instances in eine Writer-DB-Instance umgewandelt. Wenn die DB-Instances dieselbe DB-Instance-Klasse und Größe verwenden, kann die Arbeitslast für die DB-Instances in Ihrem DB-Cluster ausgeglichen werden.

Weitere Informationen finden Sie unter Aurora Replicas.

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Die Speicherparameter von Amazon RDS DB weichen vom Standard ab

Beschreibung

Die Speicherparameter der DB-Instances unterscheiden sich erheblich von den Standardwerten. Diese Einstellungen können sich auf die Leistung auswirken und zu Fehlern führen.

Wir empfehlen, die benutzerdefinierten Speicherparameter für die DB-Instance auf ihre Standardwerte in der DB-Parametergruppe zurückzusetzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt020`

Warnungskriterien

Gelb: DB-Parametergruppen haben Speicherparameter, die erheblich von den Standardwerten abweichen.

Empfohlene Aktion

Setzen Sie die Speicherparameter auf ihre Standardwerte zurück.

Weitere Ressourcen

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 1: Leistungsparameter.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter enable_indexonlyscan ist ausgeschaltet

Beschreibung

Der Abfrageplaner oder Optimierer kann den Plantyp „Nur Index-Scan“ nicht verwenden, wenn er ausgeschaltet ist.

Es wird empfohlen, den Wert des Parameters enable_indexonlyscan auf 1 festzulegen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt028`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist der Parameter enable_indexonlyscan deaktiviert.

Empfohlene Aktion

Setzen Sie den Parameter enable_indexonlyscan auf 1.

Weitere Ressourcen

Wenn Sie den Parameter enable_indexonlyscan deaktivieren, verhindert dies, dass der Abfrageplaner einen optimalen Ausführungsplan auswählt. Der Abfrageplaner verwendet einen anderen Plantyp, z. B. den Indexscan, wodurch die Abfragekosten und die Ausführungszeit erhöht werden können. Der Plantyp „Nur Index“ ruft die Daten ab, ohne auf die Tabellendaten zuzugreifen.

Weitere Informationen finden Sie unter enable_indexonlyscan (boolean) auf der PostgreSQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter enable_indexscan ist ausgeschaltet

Beschreibung

Der Abfrageplaner oder Optimierer kann den Indexscan-Plantyp nicht verwenden, wenn er ausgeschaltet ist.

Es wird empfohlen, den Wert des Parameters enable_indexscan auf 1 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt029`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist der Parameter enable_indexscan deaktiviert.

Empfohlene Aktion

Setzen Sie den Parameter enable_indexscan auf 1.

Weitere Ressourcen

Wenn Sie den Parameter enable_indexscan deaktivieren, verhindert dies, dass der Abfrageplaner einen optimalen Ausführungsplan auswählt. Der Abfrageplaner verwendet einen anderen Plantyp, z. B. den Indexscan, wodurch die Abfragekosten und die Ausführungszeit erhöht werden können.

Weitere Informationen finden Sie unter enable_indexscan (boolean) auf der PostgreSQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter general_logging ist aktiviert

Beschreibung

Die allgemeine Protokollierung ist für Ihre DB-Instance aktiviert. Diese Einstellung ist nützlich bei der Behebung von Datenbankproblemen. Das Aktivieren der allgemeinen Protokollierung erhöht jedoch die Anzahl der I/O-Operationen und den zugewiesenen Speicherplatz, was zu Konflikten und Leistungseinbußen führen kann.

Prüfen Sie Ihre Anforderungen für die allgemeine Nutzung der Protokollierung. Wir empfehlen, den Wert des Parameters general_logging auf 0 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt037`

Warnungskriterien

Gelb: Für DB-Parametergruppen ist general_logging aktiviert.

Empfohlene Aktion

Überprüfen Sie Ihre Anforderungen für die allgemeine Nutzung der Protokollierung. Wenn dies nicht verpflichtend ist, empfehlen wir Ihnen, den Wert des Parameters general_logging auf 0 zu setzen.

Weitere Ressourcen

Das allgemeine Abfrageprotokoll wird aktiviert, wenn der Wert des Parameters general_logging auf 1 gesetzt ist. Das allgemeine Abfrageprotokoll enthält Aufzeichnungen der Datenbankserveroperationen. Der Server schreibt Informationen in dieses Protokoll, wenn Clients eine Verbindung herstellen oder die Verbindung trennen, und die Protokolle enthalten jede von den Clients empfangene SQL-Anweisung. Das allgemeine Abfrageprotokoll ist nützlich, wenn Sie einen Fehler in einem Client vermuten und die Informationen finden möchten, die der Client an den Datenbankserver gesendet hat.

Weitere Informationen finden Sie unter Überblick über die Datenbankprotokolle von RDS for MySQL.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter InnoDB_Change_Buffering verwendet weniger als den optimalen Wert

Beschreibung

Durch die Pufferung von Änderungen kann eine MySQL-DB-Instance einige Schreibvorgänge zurückstellen, die zur Verwaltung sekundärer Indizes erforderlich sind. Diese Funktion war in Umgebungen mit langsamen Festplatten nützlich. Die geänderte Pufferkonfiguration verbesserte die Leistung der Datenbank geringfügig, führte jedoch zu Verzögerungen bei der Wiederherstellung nach einem Absturz und zu langen Shutdown-Zeiten während des Upgrades.

Wir empfehlen, den Wert des Parameters innodb_change_buffering auf NONE zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt021`

Warnungskriterien

Gelb: Für DB-Parametergruppen ist der Parameter innodb_change_buffering auf einen niedrigen optimalen Wert gesetzt.

Empfohlene Aktion

Setzen Sie den Parameterwert innodb_change_buffering in Ihren DB-Parametergruppen auf NONE.

Weitere Ressourcen

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 1: Leistungsparameter.

Berichtsspalten

- Status

- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter innodb_open_files ist niedrig

Beschreibung

Der Parameter innodb_open_files steuert die Anzahl der Dateien, die InnoDB gleichzeitig öffnen kann. InnoDB öffnet alle Protokoll- und System-Tablespace-Dateien, wenn mysqld läuft.

Ihre DB-Instance hat einen niedrigen Wert für die maximale Anzahl von Dateien, die InnoDB gleichzeitig öffnen kann. Wir empfehlen, den Parameter innodb_open_files auf einen Mindestwert von 65 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt033`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist die InnoDB-Einstellung zum Öffnen von Dateien falsch konfiguriert.

Empfohlene Aktion

Setzen Sie den Parameter innodb_open_files auf einen Mindestwert von 65.

Weitere Ressourcen

Der Parameter innodb_open_files steuert die Anzahl der Dateien, die InnoDB gleichzeitig öffnen kann. InnoDB hält alle Protokolldateien und die System-Tablespace-Dateien geöffnet, wenn mysqld ausgeführt wird. InnoDB muss auch einige.ibd-Dateien öffnen, wenn das file-per-table Speichermodell verwendet wird. Wenn die Einstellung innodb_open_files niedrig ist, wirkt sich dies auf die Datenbankleistung aus und der Server kann möglicherweise nicht gestartet werden.

Weitere Informationen finden Sie unter InnoDB-Startoptionen und Systemvariablen — innodb_open_files auf der Dokumentationswebsite. MySql

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter innodb_stats_persistent ist ausgeschaltet

Beschreibung

Ihre DB-Instance ist nicht dafür konfiguriert, die InnoDB-Statistiken auf der Festplatte zu speichern. Wenn die Statistiken nicht gespeichert werden, werden sie jedes Mal neu berechnet, wenn die Instance neu gestartet wird und auf die Tabelle zugegriffen wird. Dies führt zu Abweichungen im Abfrageausführungsplan. Sie können den Wert dieses globalen Parameters auf Tabellenebene ändern.

Es wird empfohlen, den Wert des Parameters innodb_stats_persistent auf ON zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt032`

Warnungskriterien

Gelb: DB-Parametergruppen haben Optimizer-Statistiken, die nicht dauerhaft auf der Festplatte gespeichert werden.

Empfohlene Aktion

Setzen Sie den Wert des Parameters innodb_stats_persistent auf ON.

Weitere Ressourcen

Wenn der Parameter innodb_stats_persistent auf ON gesetzt ist, werden die Optimizer-Statistiken beim Neustart der Instanz beibehalten. Dies verbessert die Stabilität des Ausführungsplans und die konsistente Abfrageleistung. Sie können die Persistenz globaler Statistiken auf Tabellenebene

ändern, indem Sie die Klausel STATS_PERSISTENT verwenden, wenn Sie eine Tabelle erstellen oder ändern.

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 1: Leistungsparameter.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-Instance mit unzureichender Systemkapazität

Beschreibung

Überprüft, ob die Amazon RDS-Instance oder die Amazon Aurora Aurora-DB-Instance über die für den Betrieb erforderliche Systemkapazität verfügt.

Prüf-ID

`c1qf5bt039`

Warnungskriterien

Gelb:

Fehlender Arbeitsspeicher: Wenn ein Prozess auf dem Datenbank-Host aufgrund einer Speicherreduzierung auf Betriebssystemebene gestoppt wird, erhöht sich der Zähler für Out-of-Memory-Kills (OOM).

Übermäßiges Auslagern: Die Metrikwerte os.memory.swap.in und os.memory.swap.out waren hoch.

Empfohlene Aktion

Wir empfehlen Ihnen, Ihre Abfragen so zu optimieren, dass sie weniger Speicher verbrauchen oder einen DB-Instance-Typ mit mehr zugewiesenem Speicher verwenden. Wenn der Instance

nur noch wenig Arbeitsspeicher zur Verfügung steht, wirkt sich dies auf die Datenbankleistung aus.

Weitere Ressourcen

ut-of-memory O-Kills wurden erkannt: Der Linux-Kernel ruft den Out of Memory (OOM) -Killer auf, wenn die auf dem Host laufenden Prozesse mehr als den vom Betriebssystem physisch verfügbaren Speicher benötigen. In diesem Fall überprüft der OOM-Killer alle laufenden Prozesse und stoppt einen oder mehrere Prozesse, um Systemspeicher freizugeben und das System am Laufen zu halten.

Ein Auslagern wird erkannt: Wenn der Arbeitsspeicher auf dem Datenbank-Host nicht ausreicht, sendet das Betriebssystem einige mindestens belegte Seiten an die Festplatte im Auslagerungsspeicher. Dieser Auslagerungsprozess wirkt sich auf die Datenbankleistung aus.

Weitere Informationen finden Sie unter Amazon RDS-Instance-Typen und Skalierung Ihrer Amazon RDS-Instance.

Berichtsspalten

- Status
- Region
- Ressource
- Keine ut-of-memory Fähigkeiten (Anzahl)
- Übermäßiges Tauschen (Anzahl)
- Letzter Erkennungszeitraum
- Zeitpunkt der letzten Aktualisierung

Amazon RDS Magnetic Volume wird verwendet

Beschreibung

Ihre DB-Instances verwenden Magnetspeicher. Magnetischer Speicher wird für die meisten DB-Instances nicht empfohlen. Wählen Sie einen anderen Speichertyp: General Purpose (SSD) oder Provisioned IOPS.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt000`

Warnungskriterien

Gelb: Amazon RDS-Ressourcen verwenden Magnetspeicher.

Empfohlene Aktion

Wählen Sie einen anderen Speichertyp: General Purpose (SSD) oder Provisioned IOPS.

Weitere Ressourcen

Magnetischer Speicher ist ein Speichertyp der früheren Generation. Der allgemeine Speichertyp (SSD) oder der bereitgestellte IOPS ist der empfohlene Speichertyp für neue Speicheranforderungen. Diese Speichertypen bieten eine höhere und konsistente Leistung sowie verbesserte Optionen für die Speichergröße.

Weitere Informationen finden Sie unter Volumes der vorherigen Generation.

Berichtsspalten

- Status
- Region
- Ressource

- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-Parametergruppen verwenden keine riesigen Seiten

Beschreibung

Große Seiten können die Skalierbarkeit der Datenbank erhöhen, aber Ihre DB-Instance verwendet keine großen Seiten. Wir empfehlen, dass Sie den Wert des Parameters use_large_pages in der DB-Parametergruppe für Ihre DB-Instance auf ONLY setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt024`

Warnungskriterien

Gelb: DB-Parametergruppen verwenden keine großen Seiten.

Empfohlene Aktion

Setzen Sie den Wert des Parameters use_large_pages in Ihren DB-Parametergruppen auf NUR.

Weitere Ressourcen

Weitere Informationen finden Sie unter Einschalten für eine RDS HugePages for Oracle-Instance.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Abfrage-Cache-Parameter ist aktiviert

Beschreibung

Wenn Änderungen erfordern, dass Ihr Abfrage-Cache gelöscht wird, scheint Ihre DB-Instance zum Stillstand zu kommen. Die meisten Workloads profitieren nicht von einem Abfrage-Cache. Der Abfrage-Cache wurde aus der MySQL-Version 8 entfernt. Wir empfehlen, den Parameter query_cache_type auf 0 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die

Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt022`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist der Abfrage-Cache aktiviert.

Empfohlene Aktion

Setzen Sie den Parameterwert query_cache_type in Ihren DB-Parametergruppen auf 0.

Weitere Ressourcen

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 1: Leistungsparameter.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Eine Aktualisierung der Amazon RDS-Ressourcen-Instance-Klasse ist erforderlich

Beschreibung

In Ihrer Datenbank wird eine DB-Instance-Klasse der vorherigen Generation ausgeführt. Wir haben DB-Instance-Klassen aus einer früheren Generation durch DB-Instance-Klassen mit besseren Kosten, besserer Leistung oder beidem ersetzt. Wir empfehlen, dass Sie Ihre DB-Instance mit einer DB-Instance-Klasse einer neueren Generation ausführen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt015`

Warnungskriterien

Rot: DB-Instances verwenden die DB-Instance-Klasse „End of Support“.

Empfohlene Aktion

Führen Sie ein Upgrade auf die neueste DB-Instance-Klasse durch.

Weitere Ressourcen

Weitere Informationen finden Sie unter Supported DB engines for DB instance classes (Unterstützte DB-Engines für DB-Instance-Klassen).

Berichtsspalten

- Status
- Region

- Ressource
- DB-Instance-Klasse
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Aktualisierung der Hauptversionen von Amazon RDS-Ressourcen ist erforderlich

Beschreibung

Datenbanken mit der aktuellen Hauptversion für die DB-Engine werden nicht unterstützt. Wir empfehlen Ihnen, auf die neueste Hauptversion zu aktualisieren, die neue Funktionen und Verbesserungen enthält.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt014`

Warnungskriterien

Rot: RDS-Ressourcen verwenden Hauptversionen, die nicht mehr unterstützt werden.

Empfohlene Aktion

Führen Sie ein Upgrade auf die neueste Hauptversion für die DB-Engine durch.

Weitere Ressourcen

Amazon RDS veröffentlicht neue Versionen für die unterstützten Datenbank-Engines, um Ihre Datenbanken auf der neuesten Version zu verwalten. Die neu veröffentlichten Versionen können Bugfixes, Sicherheitsverbesserungen und andere Verbesserungen für die Datenbank-Engine enthalten. Sie können die für das DB-Instance-Upgrade erforderlichen Ausfallzeiten minimieren, indem Sie eine blaue/grüne Bereitstellung verwenden.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Aktualisierung einer DB-Instance-Engine-Version
- Amazon Aurora Aurora-Aktualisierungen
- Verwenden von Amazon RDS Blue/Green Deployments für Datenbank-Updates

Berichtsspalten

- Status
- Region
- Ressource
- Name der Engine
- Aktuelle Version der Engine
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-Ressourcen, die die End-of-Support-Engine-Edition im Rahmen der inbegriffenen Lizenz verwenden

Beschreibung

Wir empfehlen Ihnen, die Hauptversion auf die neueste Engine-Version zu aktualisieren, die von Amazon RDS unterstützt wird, um mit der aktuellen Lizenzunterstützung fortzufahren. Die Engine-Version Ihrer Datenbank wird mit der aktuellen Lizenz nicht unterstützt.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt016`

Warnungskriterien

Rot: Amazon RDS-Ressourcen verwenden die End of Support Engine Edition im Rahmen eines Modells, das in der Lizenz enthalten ist.

Empfohlene Aktion

Wir empfehlen Ihnen, Ihre Datenbank auf die neueste unterstützte Version in Amazon RDS zu aktualisieren, um das lizenzierte Modell weiterhin verwenden zu können.

Weitere Ressourcen

Weitere Informationen finden Sie unter Oracle-Hauptversions-Upgrades.

Berichtsspalten

- Status

- Region
- Ressource
- Name der Engine
- Aktuelle Motorversion
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon Route 53 Alias Ressourceneintragsätze

Beschreibung

Sucht nach Ressourceneintragsätzen, die in Alias-Ressourceneintragsätze geändert werden können, um die Leistung zu verbessern und Geld zu sparen.

Ein Alias-Ressourcendatensatz leitet DNS-Abfragen an eine AWS Ressource (z. B. einen Elastic Load Balancing Load Balancer oder einen Amazon S3 S3-Bucket) oder an einen anderen Route 53-Ressourcendatensatz weiter. Wenn Sie Alias-Ressourcendatensätze verwenden, leitet Route 53 Ihre DNS-Abfragen kostenlos an AWS Ressourcen weiter.

Von AWS Diensten erstellte gehostete Zonen werden in Ihren Prüfergebnissen nicht angezeigt.

Prüf-ID

`B913Ef6fb4`

Warnungskriterien

- Gelb: Ein Ressourcendatensatz ist ein CNAME für eine Amazon-S3-Website.
- Gelb: Ein Ressourcendatensatz ist ein CNAME für eine CloudFront Amazon-Distribution.
- Gelb: Ein Ressourcendatensatz ist ein CNAME für einen Load Balancer für Elastic-Load-Balancing.

Empfohlene Aktion

Ersetzen Sie die aufgelisteten CNAME-Ressourcendatensätze durch Alias-Ressourcendatensätze. Weitere Informationen finden Sie unter Wählen zwischen Alias- und Nicht-Alias-Datensätzen.

Je nach Ressource müssen Sie auch den Datensatztyp von CNAME in A oder AAAA ändern. AWS Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Bearbeiten von Amazon-Route-53-Datensätzen angeben.

Weitere Ressourcen

Abfragen an Ressourcen weiterleiten AWS

Berichtsspalten

- Status
- Name der gehosteten Zone
- ID der gehosteten Zone
- Name des Ressourcendatensatzes
- Typ des Ressourcendatensatzes
- Kennung des Ressourcendatensatzes
- Alias-Ziel

AWS Lambda stellt zu wenig Funktionen für die Speichergröße bereit

Beschreibung

Überprüft die AWS Lambda Funktionen, die während der Lookback-Periode mindestens einmal aufgerufen wurden. Diese Überprüfung warnt Sie, wenn eine Ihrer Lambda-Funktionen für die Speichergröße zu geringfügig bereitgestellt wurde. Wenn Sie Lambda-Funktionen haben, die für die Speichergröße zu geringfügig bereitgestellt sind, dauert die vollständige Ausführung der Funktionen länger.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`C0r6dfpM06`

Warnungskriterien

Gelb: Eine Lambda-Funktion, die während des Lookback-Zeitraums für die Speichergröße überlastet war. Um festzustellen, ob eine Lambda-Funktion nicht ausreichend bereitgestellt ist, berücksichtigen wir alle CloudWatch Standardmetriken für diese Funktion. Der Algorithmus, der zur Identifizierung unzureichend bereitgestellter Lambda-Funktionen im Hinblick auf die Speichergröße verwendet wird, folgt AWS bewährten Methoden. Der Algorithmus wird aktualisiert, wenn ein neues Muster identifiziert wurde.

Empfohlene Aktion

Ziehen Sie in Erwägung, die Arbeitsspeichergröße Ihrer Lambda-Funktionen zu erhöhen.

Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Berichtsspalten

- Status
- Region
- Funktionsname
- Funktionsversion
- Speichergröße (MB)
- Empfohlene Speichergröße (MB)
- Lookback-Zeitraum (in Tagen)
- Leistungsrisiko
- Zeitpunkt der letzten Aktualisierung

AWS Lambda Funktionen ohne Parallelitätslimit konfiguriert

Beschreibung

Prüft, ob AWS Lambda Funktionen mit einem Limit für gleichzeitige Ausführung auf Funktionsebene konfiguriert sind.

Die Gleichzeitigkeit ist die Anzahl der Anforderungen, die Ihre AWS Lambda-Funktion gleichzeitig bearbeitet. Für jede gleichzeitige Anfrage stellt Lambda eine separate Instance Ihrer Ausführungsumgebung bereit.

Sie können das Mindest- und Höchstlimit für Parallelität mithilfe der Parameter Parallelität LimitLow und ConcurrencyLimitHoch in Ihren Regeln angeben. AWS Config

Weitere Informationen erhalten Sie unter Skalierung von Lambda-Funktionen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz181`

Quelle

AWS Config Verwaltete Regel: lambda-concurrency-check

Warnungskriterien

Gelb: Für die Lambda-Funktion ist keine Gleichzeitigkeitsbeschränkung konfiguriert.

Empfohlene Aktion

Stellen Sie sicher, dass für Ihre Lambda-Funktionen die Gleichzeitigkeit konfiguriert ist. Eine Gleichzeitigkeitsbeschränkung für Ihre Lambda-Funktionen stellt sicher, dass Ihre Funktion Anforderungen zuverlässig und vorhersehbar verarbeitet. Eine Gleichzeitigkeitsbeschränkung verringert das Risiko, dass Ihre Funktion durch einen plötzlichen Anstieg des Datenverkehrs überlastet wird.

Weitere Informationen finden Sie unter Konfigurieren reservierter Gleichzeitigkeit.

Weitere Ressourcen

- Skalierung einer Lambda-Funktion
- Konfigurieren reservierter Gleichzeitigkeit

Berichtsspalten

- Status

- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Well-Architected-Probleme mit hohem Risiko für die Leistung

Beschreibung

Prüft auf Probleme mit hohem Risiko (HRI) für Ihre Workloads hinsichtlich der Leistung. Diese Prüfung basiert auf Ihren AWS-Well Architected-Beurteilungen. Ihre Prüfergebnisse hängen davon ab, ob Sie die Workload-Bewertung mit AWS Well-Architected durchgeführt haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Wxdfp4B1L2`

Warnungskriterien

- Rot: In der Performance-Säule von AWS Well-Architected wurde mindestens ein aktives Problem mit hohem Risiko identifiziert.
- Grün: In der Performance-Säule von AWS Well-Architected wurden keine aktiven Probleme mit hohem Risiko festgestellt.

Empfohlene Aktion

AWS Well-Architected hat bei Ihrer Workload-Evaluierung Probleme mit hohem Risiko erkannt. Diese Probleme bieten Möglichkeiten, Risiken zu reduzieren und Geld zu sparen. Melden Sie sich bei AWS Well-Architected an, um Ihre Antworten zu überprüfen und Maßnahmen zur Lösung der aktiven Probleme zu ergreifen.

Berichtsspalten

- Status
- Region
- Workload-ARN
- Name der Workload
- Name des Reviewers
- Workload-Typ
- Startdatum der Workload
- Datum der letzten Änderung der Workload
- Anzahl der identifizierten HRI für die Leistung
- Anzahl der behobenen HRI für die Leistung
- Anzahl der für die Leistung beantworteten Fragen
- Gesamtzahl der Fragen hinsichtlich der Leistung
- Zeitpunkt der letzten Aktualisierung

CloudFront Alternative Domainnamen

Beschreibung

Überprüft CloudFront Amazon-Distributionen auf alternative Domainnamen (CNAMES), die falsch konfigurierte DNS-Einstellungen haben.

Wenn eine CloudFront Distribution alternative Domainnamen enthält, muss die DNS-Konfiguration für die Domains DNS-Abfragen an diese Distribution weiterleiten.

> **Note**
>
> Bei dieser Prüfung wird davon ausgegangen, dass Amazon Route 53 DNS und Amazon CloudFront Distribution auf dieselbe Weise konfiguriert sind AWS-Konto. Daher kann die Warnliste Ressourcen enthalten, die aufgrund von DNS-Einstellungen, die außerhalb dieser Liste liegen, nicht wie erwartet funktionieren AWS-Konto.

Prüf-ID

`N420c450f2`

Warnungskriterien

- Gelb: Eine CloudFront Distribution umfasst alternative Domainnamen, aber die DNS-Konfiguration ist mit einem CNAME-Eintrag oder einem Amazon Route 53-Aliasressourceneintrag nicht korrekt eingerichtet.
- Gelb: Eine CloudFront Distribution umfasst alternative Domainnamen, Trusted Advisor konnte aber die DNS-Konfiguration nicht auswerten, da es zu viele Weiterleitungen gab.
- Gelb: Eine CloudFront Distribution enthält alternative Domainnamen, Trusted Advisor konnte die DNS-Konfiguration jedoch aus einem anderen Grund nicht auswerten, wahrscheinlich aufgrund eines Timeouts.

Empfohlene Aktion

Aktualisieren Sie die DNS-Konfiguration, um DNS-Abfragen an die CloudFront Distribution weiterzuleiten. Weitere Informationen finden Sie unter Alternative Domainnamen (CNAMes) verwenden.

Wenn Sie Amazon Route 53 als Ihren DNS-Service verwenden, finden Sie weitere Informationen unter Weiterleiten von Traffic an eine Amazon CloudFront Web Distribution mithilfe Ihres Domainnamens. Wenn die Überprüfung zu einem Timeout geführt hat, versuchen Sie, die Überprüfung zu aktualisieren.

Weitere Ressourcen

CloudFront Amazon-Entwicklerhandbuch

Berichtsspalten

- Status
- Verteilungs-ID
- Verteilungs-Domänenname
- Alternativer Domainname
- Grund

CloudFront Optimierung der Inhaltsbereitstellung

Beschreibung

Sucht nach Fällen, in denen die Datenübertragung aus Amazon Simple Storage Service (Amazon S3) -Buckets durch die Nutzung von Amazon CloudFront, dem AWS globalen Content Delivery Service, beschleunigt werden könnte.

Wenn Sie CloudFront die Bereitstellung Ihrer Inhalte konfigurieren, werden Anfragen für Ihre Inhalte automatisch an den nächstgelegenen Edge-Standort weitergeleitet, an dem der Inhalt zwischengespeichert wird. Durch dieses Routing können die Inhalte mit der bestmöglichen Leistung an Ihre Nutzer geliefert werden. Ein hoher Anteil der ausgehenden Daten im Vergleich zu den im Bucket gespeicherten Daten deutet darauf hin, dass Sie von der Nutzung von Amazon für CloudFront die Bereitstellung der Daten profitieren könnten.

Prüf-ID

`796d6f3D83`

Warnungskriterien

- Gelb: Die Datenmenge, die in den 30 Tagen vor der Überprüfung durch GET-Anfragen aus dem Bucket an Ihre Benutzer übertragen wurde, ist mindestens 25-mal höher als die durchschnittliche Datenmenge, die im Bucket gespeichert ist.
- Rot: Die Datenmenge, die in den 30 Tagen vor der Überprüfung durch GET-Anfragen aus dem Bucket an Ihre Benutzer übertragen wurde, beträgt mindestens 10 TB und ist mindestens 25-mal höher als die durchschnittliche Datenmenge, die im Bucket gespeichert ist.

Empfohlene Aktion

Erwägen Sie CloudFront die Verwendung für eine bessere Leistung. Siehe CloudFront Amazon-Produktdetails.

Wenn die übertragenen Daten 10 TB pro Monat oder mehr betragen, finden Sie in den CloudFront Amazon-Preisen nach möglichen Kosteneinsparungen.

Weitere Ressourcen

- CloudFront Amazon-Entwicklerhandbuch
- AWS -Fallstudie: PBS

Berichtsspalten

- Status
- Region
- Bucket-Name
- S3-Speicher (GB)
- Ausgehende Datenübertragungen (GB)
- Verhältnis von Übertragung zu Speicher

CloudFront Header-Weiterleitung und Cache-Trefferquote

Beschreibung

Überprüft die HTTP-Anforderungsheader, die CloudFront derzeit vom Client empfangen werden, und leitet sie an Ihren Ursprungsserver weiter.

Einige Header, wie Datum oder User-Agent, reduzieren die Cache-Trefferquote (den Anteil der Anfragen, die von einem CloudFront Edge-Cache aus bedient werden) erheblich. Dies erhöht die Belastung Ihres Ursprungs und verringert die Leistung, da mehr Anfragen an Ihren Ursprung weitergeleitet CloudFront werden müssen.

Prüf-ID

`N415c450f2`

Warnungskriterien

Gelb: Ein oder mehrere Anforderungsheader, die an Ihren Ursprung CloudFront weiterleiten, können Ihre Cache-Trefferquote erheblich reduzieren.

Empfohlene Aktion

Überlegen Sie, ob die Anfrage-Header ausreichend Vorteile bieten, um die negativen Auswirkungen auf das Cache-Trefferverhältnis zu rechtfertigen. Wenn Ihr Ursprung unabhängig vom Wert eines bestimmten Headers dasselbe Objekt zurückgibt, empfehlen wir, dass Sie die Konfiguration nicht so konfigurieren, dass dieser Header CloudFront an den Ursprung weitergeleitet wird. Weitere Informationen finden Sie unter Konfiguration CloudFront zum Zwischenspeichern von Objekten auf der Grundlage von Anforderungsheadern.

Weitere Ressourcen

- Erhöhung des Anteils der Anfragen, die über CloudFront Edge-Caches bedient werden
- CloudFront Cache-Statistikberichte
- Header und CloudFront Verhalten von HTTP-Anfragen

Berichtsspalten

- Verteilungs-ID
- Verteilungs-Domainname
- Pfadmuster für das Cache-Verhalten
- Überschriften

Hohe Nutzung Amazon-EC2-Instances

Beschreibung

Prüft die Amazon Elastic Compute Cloud (Amazon EC2) Instances, die zu einem beliebigen Zeitpunkt in den letzten 14 Tagen ausgeführt wurden. Eine Warnung wird gesendet, wenn die tägliche CPU-Auslastung an vier oder mehr Tagen mehr als 90 % betrug.

Eine konstant hohe Auslastung kann auf eine optimierte, gleichmäßige Leistung hindeuten. Es kann aber auch darauf hinweisen, dass eine Anwendung nicht über genügend Ressourcen verfügt. Um tägliche CPU-Auslastungsdaten zu erhalten, laden Sie den Bericht für diese Prüfung herunter.

Prüf-ID

`ZRxQlPsb6c`

Warnungskriterien

Gelb: Eine Instance hatte an mindestens 4 der letzten 14 Tage eine durchschnittliche CPU-Auslastung von mehr als 90 %.

Empfohlene Aktion

Ziehen Sie in Erwägung, weitere Instances hinzuzufügen. Weitere Informationen zur bedarfsabhängigen Skalierung der Anzahl von Instances finden Sie unter Was ist Auto Scaling?

Weitere Ressourcen

- Überwachen von Amazon EC2
- Instance-Metadaten und Benutzerdaten
- CloudWatch Amazon-Benutzerhandbuch
- Benutzerhandbuch für Amazon EC2 Auto Scaling

Berichtsspalten

- Region/AZ
- Instance-ID
- Instance-Typ
- Instance-Name
- CPU-Auslastung im 14-Tage-Durchschnitt

- Anzahl der Tage mit mehr als 90 % CPU-Auslastung

Sicherheit

Sie können die folgenden Prüfungen für die Sicherheitskategorie verwenden.

> **Note**
>
> Wenn Sie Security Hub für Ihren aktiviert haben AWS-Konto, können Sie Ihre Ergebnisse in der Trusted Advisor Konsole einsehen. Weitere Informationen finden Sie unter Anzeigen von AWS Security Hub Steuerelemente in AWS Trusted Advisor.
> Sie können alle Kontrollen des Sicherheitsstandards AWS Foundation Security Best Practices anzeigen, mit Ausnahme der Kontrollen, die der Kategorie „Wiederherstellen“ > „Resilienz“ zugeordnet sind. Eine Liste der unterstützten Steuerelemente finden Sie unter AWS Foundational Security Best Practices-Steuerelemente im AWS Security Hub - Benutzerhandbuch.

Namen prüfen

- Aufbewahrungszeitraum für Amazon CloudWatch Log Group
- Amazon-EC2-Instances mit veraltetem Microsoft SQL Server (Ende des Supports)
- Amazon-EC2-Instances mit veraltetem Support für Microsoft Windows Server
- Ende der Standardunterstützung für Amazon EC2 EC2-Instances mit Ubuntu LTS
- Amazon EFS-Clients verwenden keine data-in-transit Verschlüsselung
- Amazon EBS-Snapshots
- Die Amazon RDS Aurora-Speicherverschlüsselung ist ausgeschaltet
- Ein Upgrade der Nebenversion der Amazon RDS-Engine ist erforderlich
- Öffentliche Amazon RDS-Snapshots
- Zugriffsrisiko für Amazon RDS-Sicherheitsgruppen
- Die Amazon RDS-Speicherverschlüsselung ist ausgeschaltet
- Amazon Route 53 stimmt nicht mit CNAME-Datensätzen überein, die direkt auf S3-Buckets verweisen
- Amazon Route 53 MX-Ressourceneintragsätze und Senderrichtlinien-Framework

- Amazon S3 Bucket-Berechtigungen
- Amazon S3Server-Zugriffsprotokolle aktiviert
- Amazon VPC-Peering-Verbindungen mit deaktivierter DNS-Auflösung
- AWS Backup Tresor ohne ressourcenbasierte Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten
- AWS CloudTrail Protokollierung
- AWS Lambda Funktionen, die veraltete Laufzeiten verwenden
- AWS Well-Architected-Probleme mit hohem Risiko für die Sicherheit
- CloudFrontBenutzerdefinierte SSL-Zertifikate im IAM-Zertifikatsspeicher
- CloudFront SSL-Zertifikat auf dem Ursprungsserver
- ELB-Listener-Sicherheit
- ELB-Sicherheitsgruppen
- Exposed Access Keys
- IAM-Zugriffsschlüssel-Rotation
- IAM–Passwortrichtlinie
- MFA auf Root-Konto
- Sicherheitsgruppen – Bestimmte Ports uneingeschränkt
- Sicherheitsgruppen – Uneingeschränkter Zugriff

Aufbewahrungszeitraum für Amazon CloudWatch Log Group

Beschreibung

Prüft, ob die Aufbewahrungsfrist für CloudWatch Amazon-Protokollgruppen auf 365 Tage oder eine andere angegebene Anzahl festgelegt ist.

Standardmäßig werden Protokolle unbegrenzt aufbewahrt und laufen nicht ab. Sie können jedoch die Aufbewahrungsrichtlinien für jede Protokollgruppe so anpassen, dass sie den Branchenvorschriften oder gesetzlichen Anforderungen für einen bestimmten Zeitraum entsprechen.

Sie können die Mindestaufbewahrungszeit und die Namen der Protokollgruppen mithilfe der Parameter LogGroupNames und MinRetentionTime in Ihren AWS Config Regeln angeben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz186`

Quelle

`AWS Config Managed Rule: cw-loggroup-retention-period-check`

Warnungskriterien

Gelb: Die Aufbewahrungsdauer einer CloudWatch Amazon-Protokollgruppe liegt unter der gewünschten Mindestanzahl von Tagen.

Empfohlene Aktion

Konfigurieren Sie eine Aufbewahrungsfrist von mehr als 365 Tagen für Ihre in Amazon CloudWatch Logs gespeicherten Protokolldaten, um die Compliance-Anforderungen zu erfüllen.

Weitere Informationen finden Sie unter Aufbewahrung von Protokolldaten ändern in CloudWatch Logs.

Weitere Ressourcen

Änderung der Aufbewahrung von CloudWatch Protokollen

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-EC2-Instances mit veraltetem Microsoft SQL Server (Ende des Supports)

Beschreibung

Überprüft die SQL Server-Versionen auf den Amazon-Elastic-Compute-Cloud(Amazon EC2)-Instances, die in den letzten 24 Stunden ausgeführt wurden. Diese Prüfung warnt Sie, wenn die Versionen das Ende des Supports erreicht haben oder kurz davor stehen. Jede SQL Server-Version wird 10 Jahre lang unterstützt. 5 Jahre Mainstream-Support und 5 Jahre verlängerter Support. Nach Ende des Supports erhält die SQL Server-Version keine regulären Sicherheitsupdates mehr. Das Ausführen von Anwendungen mit nicht unterstützten SQL Server-Versionen kann Sicherheits- oder Compliance-Risiken mit sich bringen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Qsdfp3A4L3`

Warnungskriterien

- Rot: Eine EC2-Instance weist eine SQL-Server-Version auf, die das Ende des Supports erreicht hat.
- Gelb: Eine EC2-Instance weist eine SQL-Server-Version auf, die in 12 Monaten das Ende des Supports erreicht.

Empfohlene Aktion

Um Ihre SQL-Server-Workloads zu modernisieren, sollten Sie einen Faktorwechsel auf AWS Cloud -native Datenbanken wie Amazon Aurora in Erwägung ziehen. Weitere Informationen finden Sie unter Modernisieren Sie Windows-Workloads mit. AWS

Um auf eine vollständig verwaltete Datenbank umzusteigen, sollten Sie einen Plattformwechsel auf Amazon Relational Database Service (Amazon RDS) in Erwägung ziehen. Weitere Informationen finden Sie unter Amazon RDS für SQL Server.

Wenn Sie Ihren SQL Server auf Amazon EC2 aktualisieren, sollten Sie das Automation-Runbook verwenden, um die Aktualisierung zu vereinfachen. Weitere Informationen finden Sie in der AWS Systems Manager -Dokumentation.

Wenn Sie Ihren SQL Server auf Amazon EC2 nicht aktualisieren können, ziehen Sie das End-of-Support Migration Program for Windows Server (EMP) in Erwägung. Weitere Informationen finden Sie auf der EMP-Website.

Weitere Ressourcen

- Bereiten Sie sich auf das Ende des Supports für SQL Server vor mit AWS
- Microsoft SQL Server auf AWS

Berichtsspalten

- Status
- Region
- Instance-ID
- SQL Server-Version
- Supportzyklus
- Ende des Supports
- Zeitpunkt der letzten Aktualisierung

Amazon-EC2-Instances mit veraltetem Support für Microsoft Windows Server

Beschreibung

Diese Prüfung warnt Sie, wenn die Versionen das Ende des Supports erreicht haben oder kurz davor stehen. Jede Windows-Server-Version bietet 10 Jahre Support. Dies umfasst 5 Jahre Mainstream-Support und 5 Jahre erweiterten Support. Nach dem Ende des Supports erhält die Windows-Server-Version keine regelmäßigen Sicherheitsupdates mehr. Wenn Sie Anwendungen mit nicht unterstützten Windows-Server-Versionen ausführen, riskieren Sie die Sicherheit oder Konformität dieser Anwendungen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Qsdfp3A4L4`

Warnungskriterien

- Rot: Eine EC2-Instance verfügt über eine Windows-Server-Version, die das Ende des Supports erreicht hat (Windows Server 2003, 2003 R2, 2008 und 2008 R2).
- Gelb: Eine EC2-Instance verfügt über eine Windows-Server-Version, die in weniger als 18 Monaten das Ende des Supports erreicht (Windows Server 2012 und 2012 R2).

Empfohlene Aktion

Um Ihre Windows Server-Workloads zu modernisieren, sollten Sie die verschiedenen Optionen in Betracht ziehen, die unter Windows-Workloads modernisieren mit verfügbar sind. AWS

Um Ihre Windows-Server-Workloads für die Ausführung auf neueren Versionen von Windows Server zu aktualisieren, können Sie ein Automatisierungs-Runbook verwenden. Weitere Informationen finden Sie in der AWS -Systems-Manager-Dokumentation.

Bitte befolgen Sie die folgenden Schritte:

- Aktualisieren Sie die Windows Server-Version
- Nach dem Upgrade müssen Sie das System anhalten und wieder starten
- Wenn Sie EC2Config verwenden, migrieren Sie bitte zu EC2Launch

Berichtsspalten

- Status
- Region
- Instance-ID
- Windows-Server-Version
- Supportzyklus
- Ende des Supports
- Zeitpunkt der letzten Aktualisierung

Ende der Standardunterstützung für Amazon EC2 EC2-Instances mit Ubuntu LTS

Beschreibung

Mit dieser Überprüfung werden Sie benachrichtigt, wenn die Standardunterstützung für die Versionen kurz bevorsteht oder das Ende bereits erreicht hat. Es ist wichtig, Maßnahmen zu ergreifen — entweder durch eine Migration auf das nächste LTS oder durch ein Upgrade auf Ubuntu Pro. Nach dem Ende des Supports erhalten Ihre 18.04 LTS-Computer keine Sicherheitsupdates. Mit einem Ubuntu Pro-Abonnement kann Ihre Ubuntu 18.04 LTS-Bereitstellung bis 2028 Expanded Security Maintenance (ESM) erhalten. Sicherheitslücken, die noch nicht behoben wurden, machen Ihre Systeme anfällig für Hacker und die Gefahr schwerwiegender Sicherheitslücken.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch15`

Warnungskriterien

Rot: Eine Amazon EC2 EC2-Instance hat eine Ubuntu-Version, die das Ende der Standardunterstützung erreicht hat (Ubuntu 18.04 LTS, 18.04.1 LTS, 18.04.2 LTS, 18.04.3 LTS, 18.04.4 LTS, 18.04.5 LTS und 18.04.6 LTS).

Gelb: Eine Amazon EC2 EC2-Instance hat eine Ubuntu-Version, deren Standardunterstützung in weniger als 6 Monaten ausläuft (Ubuntu 20.04 LTS, 20.04.1 LTS, 20.04.2 LTS, 20.04.3 LTS, 20.04.4 LTS, 20.04.5 LTS und 20.04.6 LTS).

Grün: Alle Amazon EC2 EC2-Instances sind konform.

Empfohlene Aktion

Um die Ubuntu 18.04 LTS-Instances auf eine unterstützte LTS-Version zu aktualisieren, folgen Sie bitte den in diesem Artikel genannten Schritten. Um die Ubuntu 18.04 LTS-Instanzen auf

Ubuntu Pro zu aktualisieren, besuchen Sie die AWS License Manager Konsole und folgen Sie den im Benutzerhandbuch genannten Schritten.AWS License Manager Sie können sich auch den Ubuntu-Blog ansehen, der eine schrittweise Demo zum Upgrade von Ubuntu-Instanzen auf Ubuntu Pro zeigt.

Weitere Ressourcen

Informationen zu den Preisen erhalten Sie unter AWS Support.

Berichtsspalten

- Status
- Region
- Ubuntu LTS-Version
- Voraussichtliches Ende des Support
- Instance-ID
- Supportzyklus
- Zeitpunkt der letzten Aktualisierung

Amazon EFS-Clients verwenden keine data-in-transit Verschlüsselung

Beschreibung

Prüft, ob das Amazon EFS-Dateisystem data-in-transit verschlüsselt eingehängt ist. AWS empfiehlt Kunden, data-in-transit Verschlüsselung für alle Datenflüsse zu verwenden, um Daten vor versehentlicher Offenlegung oder unbefugtem Zugriff zu schützen. Amazon EFS empfiehlt Kunden, die Mount-Einstellung '-o tls' mit dem Amazon EFS-Mount-Helper zu verwenden, um Daten während der Übertragung mit TLS v1.2 zu verschlüsseln.

Prüf-ID

`c1dfpnchv1`

Warnungskriterien

Gelb: Ein oder mehrere NFS-Clients für Ihr Amazon EFS-Dateisystem verwenden nicht die empfohlenen Mount-Einstellungen, die data-in-transit Verschlüsselung ermöglichen.

Grün: Alle NFS-Clients für Ihr Amazon EFS-Dateisystem verwenden die empfohlenen Mount-Einstellungen, die data-in-transit Verschlüsselung ermöglichen.

Empfohlene Aktion

Um die data-in-transit Verschlüsselungsfunktion von Amazon EFS nutzen zu können, empfehlen wir, Ihr Dateisystem mithilfe des Amazon EFS-Mount-Helpers und der empfohlenen Mount-Einstellungen erneut bereitzustellen.

> **Note**
>
> Einige Linux-Distributionen enthalten standardmäßig keine Version von Stunnel, die TLS-Funktionen unterstützt. Wenn Sie eine Linux-Distribution verwenden, die nicht unterstützt wird (siehe unterstützte Distributionen hier), empfehlen wir, sie vor dem erneuten Mounten mit der empfohlenen Mount-Einstellung zu aktualisieren.

Weitere Ressourcen

- Verschlüsselung von Daten während der Übertragung

Berichtsspalten

- Status
- Region
- EFS-Dateisystem-ID
- AZs mit unverschlüsselten Verbindungen
- Zeitpunkt der letzten Aktualisierung

Amazon EBS-Snapshots

Beschreibung

Überprüft die Berechtigungseinstellungen für Ihre Amazon Elastic Block Store (Amazon EBS) - Volume-Snapshots und warnt Sie, wenn Snapshots öffentlich zugänglich sind.

Wenn Sie einen Snapshot veröffentlichen, gewähren Sie allen AWS-Konten Benutzern Zugriff auf alle Daten im Snapshot. Um einen Snapshot nur für bestimmte Benutzer oder Konten freizugeben, markieren Sie den Snapshot als privat. Geben Sie dann den oder die Benutzer an, mit denen Sie die Snapshot-Daten teilen möchten. Beachten Sie, dass Ihre öffentlichen Schnappschüsse nicht öffentlich zugänglich sind und nicht in den Ergebnissen dieser Prüfung erscheinen, wenn Sie „Öffentlichen Zugriff blockieren“ im Modus „Alle Freigaben blockieren“ aktiviert haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden.

Prüf-ID

`ePs02jT06w`

Warnungskriterien

Rot: Der EBS-Volume-Snapshot ist öffentlich zugänglich.

Empfohlene Aktion

Sofern Sie nicht sicher sind, dass Sie alle Daten im Snapshot mit allen AWS-Konten Benutzern teilen möchten, ändern Sie die Berechtigungen: Markieren Sie den Snapshot als privat und geben Sie dann die Konten an, denen Sie Berechtigungen erteilen möchten. Weitere Informationen finden Sie unter Teilen eines Amazon-EBS-Snapshots. Verwenden Sie Block Public Access for EBS Snapshots, um die Einstellungen zu steuern, die den öffentlichen Zugriff auf Ihre Daten ermöglichen. Diese Prüfung kann nicht aus der Ansicht in der Trusted Advisor Konsole ausgeschlossen werden.

Verwenden Sie ein Runbook in der Konsole, um die Berechtigungen für Ihre Snapshots direkt zu ändern. AWS Systems Manager Weitere Informationen finden Sie unter `AWSSupport-ModifyEBSSnapshotPermission`.

Weitere Ressourcen

Amazon-EBS-Snapshots

Berichtsspalten

- Status
- Region
- Volume-ID
- Snapshot-ID
- Beschreibung

Die Amazon RDS Aurora-Speicherverschlüsselung ist ausgeschaltet

Beschreibung

Amazon RDS unterstützt Verschlüsselung im Ruhezustand für alle Datenbank-Engines mithilfe der Schlüssel, in denen Sie verwalten AWS Key Management Service. Auf einer aktiven DB-Instance mit Amazon RDS-Verschlüsselung werden die im Speicher gespeicherten Daten verschlüsselt, ähnlich wie bei automatisierten Backups, Read Replicas und Snapshots.

Wenn die Verschlüsselung beim Erstellen eines Aurora-DB-Clusters nicht aktiviert ist, müssen Sie einen entschlüsselten Snapshot in einem verschlüsselten DB-Cluster wiederherstellen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt005`

Warnungskriterien

Rot: Für Amazon RDS Aurora-Ressourcen ist keine Verschlüsselung aktiviert.

Empfohlene Aktion

Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand für Ihren DB-Cluster.

Weitere Ressourcen

Sie können die Verschlüsselung beim Erstellen einer DB-Instance aktivieren oder eine Problemumgehung verwenden, um die Verschlüsselung auf einer aktiven DB-Instance zu aktivieren. Sie können einen entschlüsselten DB-Cluster nicht in einen verschlüsselten DB-Cluster umwandeln. Sie können jedoch einen entschlüsselten Snapshot in einem verschlüsselten DB-Cluster wiederherstellen. Wenn Sie aus dem entschlüsselten Snapshot wiederherstellen, müssen Sie einen AWS KMS Schlüssel angeben.

Weitere Informationen finden Sie unter Verschlüsseln von Amazon Aurora-Ressourcen.

Berichtsspalten

- Status
- Region
- Eine Ressource
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Ein Upgrade der Nebenversion der Amazon RDS-Engine ist erforderlich

Beschreibung

Auf Ihren Datenbankressourcen wird nicht die neueste Nebenversion der DB-Engine ausgeführt. Die neueste Nebenversion enthält die neuesten Sicherheitsupdates und andere Verbesserungen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt003`

Warnungskriterien

Rot: Auf Amazon RDS-Ressourcen wird nicht die neueste kleinere DB-Engine-Version ausgeführt.

Empfohlene Aktion

Führen Sie ein Upgrade auf die neueste Engine-Version durch.

Weitere Ressourcen

Wir empfehlen, dass Sie Ihre Datenbank mit der neuesten DB-Engine-Nebenversion verwalten, da diese Version die neuesten Sicherheits- und Funktionskorrekturen enthält. Die Upgrades der DB-Engine-Nebenversionen enthalten nur die Änderungen, die mit früheren Nebenversionen derselben Hauptversion der DB-Engine abwärtskompatibel sind.

Weitere Informationen finden Sie unter Upgrade der Engine-Version für eine DB-Instance.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Motors
- Aktuelle Motorversion
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Öffentliche Amazon RDS-Snapshots

Beschreibung

Prüft die Berechtigungseinstellungen für Ihre Amazon Relational Database Service (Amazon RDS) DB-Snapshots und warnt Sie, wenn irgendwelche Snapshots als öffentlich markiert sind.

Wenn Sie einen Snapshot veröffentlichen, gewähren Sie allen AWS-Konten Benutzern Zugriff auf alle Daten im Snapshot. Wenn Sie einen Snapshot nur für bestimmte Benutzer oder Konten freigeben möchten, markieren Sie den Snapshot als privat. Geben Sie dann den Benutzer oder die Konten an, für die Sie die Snapshot-Daten freigeben möchten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden.

Prüf-ID

`rSs93HQwa1`

Warnungskriterien

Rot: Der Amazon-RDS-Snapshot ist als öffentlich markiert.

Empfohlene Aktion

Sofern Sie nicht sicher sind, dass Sie alle Daten im Snapshot mit allen AWS-Konten Benutzern teilen möchten, ändern Sie die Berechtigungen: Markieren Sie den Snapshot als privat und geben Sie dann die Konten an, denen Sie Berechtigungen erteilen möchten. Weitere Informationen finden Sie unter Freigeben eines DB-Snapshots oder DB-Cluster-Snapshots. Diese Prüfung kann nicht aus der Ansicht in der Trusted Advisor Konsole ausgeschlossen werden.

Um die Berechtigungen für Ihre Snapshots direkt zu ändern, können Sie ein Runbook in der AWS Systems Manager Konsole verwenden. Weitere Informationen finden Sie unter `AWSSupport-ModifyRDSSnapshotPermission`.

Weitere Ressourcen

Sichern und Wiederherstellen einer Amazon-RDS-DB-Instance

Berichtsspalten

- Status
- Region
- DB-Instance oder Cluster-ID
- Snapshot-ID

Zugriffsrisiko für Amazon RDS-Sicherheitsgruppen

Beschreibung

Prüft Sicherheitsgruppenkonfigurationen für Amazon Relational Database Service (Amazon RDS) und warnt, wenn eine Sicherheitsgruppenregel einen zu freizügigen Zugriff auf Ihre Datenbank gewährt. Die empfohlene Konfiguration für eine Sicherheitsgruppenregel besteht darin, den Zugriff nur von bestimmten Amazon Elastic Compute Cloud (Amazon EC2) Sicherheitsgruppen oder von einer bestimmten IP-Adresse zuzulassen.

Prüf-ID

`nNauJisYIT`

Warnungskriterien

- Gelb: Eine DB-Sicherheitsgruppenregel verweist auf eine Amazon-EC2-Sicherheitsgruppe, die globalen Zugriff auf einen dieser Ports gewährt: 20, 21, 22, 1433, 1434, 3306, 3389, 4333, 5432, 5500.
- Gelb: Eine DB-Sicherheitsgruppenregel gewährt Zugriff auf mehr als eine einzelne IP-Adresse (das CIDR-Regelsuffix ist nicht /0 oder /32).
- Rot: Eine DB-Sicherheitsgruppenregel gewährt globalen Zugriff (das CIDR-Regelsuffix ist /0).

Empfohlene Aktion

Überprüfen Sie die Sicherheitsgruppenregeln und beschränken Sie den Zugriff auf autorisierte IP-Adressen oder IP-Bereiche. Um eine Sicherheitsgruppe zu bearbeiten, verwenden Sie die AuthorizeDB SecurityGroup Ingress API oder die. AWS Management Console Weitere Informationen finden Sie unter Arbeiten mit DB-Sicherheitsgruppen.

Weitere Ressourcen

- Amazon RDS-Sicherheitsgruppen
- Classless Inter-Domain Routing

- Liste der TCP- und UDP-Portnummern

Berichtsspalten

- Status
- Region
- RDS-Sicherheitsgruppenname
- Regel für eingehenden Datenverkehr
- Grund

Die Amazon RDS-Speicherverschlüsselung ist ausgeschaltet

Beschreibung

Amazon RDS unterstützt Verschlüsselung im Ruhezustand für alle Datenbank-Engines mithilfe der Schlüssel, in denen Sie verwalten AWS Key Management Service. Auf einer aktiven DB-Instance mit Amazon RDS-Verschlüsselung werden die im Speicher gespeicherten Daten verschlüsselt, ähnlich wie bei automatisierten Backups, Read Replicas und Snapshots.

Wenn die Verschlüsselung beim Erstellen einer DB-Instance nicht aktiviert ist, müssen Sie eine verschlüsselte Kopie des entschlüsselten Snapshots wiederherstellen, bevor Sie die Verschlüsselung aktivieren.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.

Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt006`

Warnungskriterien

Rot: Für Amazon RDS-Ressourcen ist keine Verschlüsselung aktiviert.

Empfohlene Aktion

Aktivieren Sie die Verschlüsselung von Daten im Ruhezustand für Ihre DB-Instance.

Weitere Ressourcen

Sie können eine DB-Instance nur verschlüsseln, wenn Sie die DB-Instance erstellen. Um eine bestehende aktive DB-Instance zu verschlüsseln:

Erstellen Sie eine verschlüsselte Kopie der ursprünglichen DB-Instance

1. Erstellen Sie einen Snapshot Ihrer DB-Instance.
2. Erstellen Sie eine verschlüsselte Kopie des in Schritt 1 erstellten Snapshots.
3. Stellen Sie eine DB-Instance aus dem verschlüsselten Snapshot wieder her.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Verschlüsseln von Amazon RDS-Ressourcen
- Einen DB-Snapshot kopieren

Berichtsspalten

- Status
- Region
- Eine Ressource
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon Route 53 stimmt nicht mit CNAME-Datensätzen überein, die direkt auf S3-Buckets verweisen

Beschreibung

Überprüft die Amazon Route 53 Hosted Zones mit CNAME-Einträgen, die direkt auf Amazon S3 S3-Bucket-Hostnamen verweisen, und warnt, wenn Ihr CNAME nicht mit Ihrem S3-Bucket-Namen übereinstimmt.

Prüf-ID

`c1ng44jvbm`

Warnungskriterien

Rot: Amazon Route 53 Hosted Zone hat CNAME-Einträge, die auf nicht übereinstimmende S3-Bucket-Hostnamen hinweisen.

Grün: In Ihrer Amazon Route 53 Hosted Zone wurden keine nicht übereinstimmenden CNAME-Einträge gefunden.

Empfohlene Aktion

Wenn Sie CNAME-Einträge auf S3-Bucket-Hostnamen verweisen, müssen Sie sicherstellen, dass für jeden von Ihnen konfigurierten CNAME- oder Alias-Datensatz ein passender Bucket vorhanden ist. Auf diese Weise vermeiden Sie das Risiko, dass Ihre CNAME-Einträge gefälscht werden. Sie verhindern auch, dass unbefugte AWS Benutzer fehlerhafte oder bösartige Webinhalte mit Ihrer Domain hosten.

Um zu vermeiden, dass CNAME-Einträge direkt auf S3-Bucket-Hostnamen verweisen, sollten Sie die Origin Access Control (OAC) verwenden, um über Amazon auf Ihre S3-Bucket-Webressourcen zuzugreifen. CloudFront

Weitere Informationen zur Verknüpfung von CNAME mit einem Amazon S3 S3-Bucket-Hostnamen finden Sie unter Amazon S3 S3-URLs mit CNAME-Einträgen anpassen.

Weitere Ressourcen

- So verknüpfen Sie einen Hostnamen mit einem Amazon S3 S3-Bucket
- Beschränken des Zugriffs auf einen Amazon S3 S3-Ursprung mit CloudFront

Berichtsspalten

- Status
- ID der gehosteten Zone

- ARN für gehostete Zonen
- Passende CNAME-Einträge
- CNAME-Einträge stimmen nicht überein
- Zeitpunkt der letzten Aktualisierung

Amazon Route 53 MX-Ressourceneintragsätze und Senderrichtlinien-Framework

Beschreibung

Überprüft für jeden MX-Ressourcendatensatz, ob der TXT- oder SPF-Ressourcendeintragsatz einen gültigen SPF-Eintrag enthält. Der Eintrag muss mit “`v=spf1`„ beginnen. Der SPF-Eintrag gibt die Server an, die berechtigt sind, E-Mails für Ihre Domain zu versenden, was dazu beiträgt, Spoofing von E-Mail-Adressen zu erkennen und zu verhindern und Spam zu reduzieren. Route 53 empfiehlt die Verwendung eines TXT-Eintrags anstelle eines SPF-Eintrags. Trusted Advisor meldet dieses Häkchen grün, solange jeder MX-Ressourcendatensatz mindestens einen SPF- oder TXT-Eintrag hat.

Prüf-ID

`c9D319e7sG`

Warnungskriterien

Gelb: Ein MX-Ressourcendatensatz hat keinen TXT- oder SPF-Ressourcendatensatz, der einen gültigen SPF-Wert enthält.

Empfohlene Aktion

Erstellen Sie für jeden MX-Ressourcendatensatz einen TXT-Ressourcendatensatz, der einen gültigen SPF-Eintrag enthält. Weitere Informationen finden Sie unter Sender Policy Framework: SPF Record Syntax (Sender Policy Framework: SPF-Datensatz-Syntax) und Erstellen von Ressourcendatensätzen mithilfe der Amazon-Route-53-Konsole.

Weitere Ressourcen

- Sender Policy Framework
- MX-Datensatz

Berichtsspalten

- Name der gehosteten Zone
- ID der gehosteten Zone
- Name des Ressourcendatensatzes

- Status

Amazon S3 Bucket-Berechtigungen

Beschreibung

Überprüft Buckets in Amazon Simple Storage Service (Amazon S3), die über offene Zugriffsberechtigungen verfügen oder die jedem authentifizierten Benutzer AWS Zugriff gewähren.

Diese Prüfung untersucht explizite Bucket-Berechtigungen sowie Bucket-Richtlinien, die diese Berechtigungen außer Kraft setzen können. Es wird nicht empfohlen, allen Benutzern Listenzugriffsrechte für einen Amazon S3-Bucket zu gewähren. Diese Berechtigungen können dazu führen, dass unbeabsichtigte Benutzer sehr häufig Objekte in den Bucket aufnehmen, was zu höheren Gebühren als erwartet führen kann. Berechtigungen, die jedem Zugriff auf den Upload und Löschen gewähren, können zu Sicherheitslücken in Ihrem Bucket führen.

Prüf-ID

`Pfx0RwqBli`

Warnungskriterien

- Gelb: Die Bucket-ACL erlaubt das Auflisten für alle oder alle authentifizierten AWS -Benutzer.
- Gelb: Eine Bucket-Richtlinie ermöglicht jede Art von offenem Zugriff.
- Gelb: Die Bucket-Richtlinie enthält Anweisungen, die öffentlichen Zugriff gewähren. Die Einstellung Block public and cross-account access to buckets that have public policies (Öffentlichen und kontoübergreifenden Zugriff auf Buckets mit öffentlichen Richtlinien blockieren) ist aktiviert, sodass nur autorisierte Benutzer dieses Kontos Zugriff haben, bis die öffentlichen Anweisungen entfernt werden.
- Gelb: ist Trusted Advisor nicht berechtigt, die Richtlinie zu überprüfen, oder die Richtlinie konnte aus anderen Gründen nicht bewertet werden.
- Rot: Die Bucket-ACL erlaubt das Hochladen und Löschen für alle oder alle authentifizierten AWS -Benutzer.

Empfohlene Aktion

Wenn ein Bucket den offenen Zugriff zulässt, müssen Sie überprüfen, ob der offene Zugriff wirklich erforderlich ist. Falls nicht, aktualisieren Sie die Bucket-Berechtigungen, um den Zugriff auf den Eigentümer oder bestimmte Benutzer einzuschränken. Verwenden Sie Amazon S3 Block Public Access, um die Einstellungen für öffentlichen Zugriff auf Ihre Daten zu steuern. Weitere Informationen finden Sie unter Einrichten der Zugriffsberechtigungen für Bucket und Objekt.

Weitere Ressourcen

Verwaltung der Zugriffsberechtigungen für Ihre Amazon-S3-Ressourcen

Berichtsspalten

- Status
- Name der Region
- Regionen-API-Parameter
- Bucket-Name
- ACL erlaubt Auflisten
- ACL erlaubt Hochladen/Löschen
- Richtlinie erlaubt Zugriff

Amazon S3Server-Zugriffsprotokolle aktiviert

Beschreibung

Überprüft die Protokollierungskonfiguration von Amazon Simple Storage Service-Buckets.

Wenn die Serverzugriffsprotokollierung aktiviert ist, werden stündlich detaillierte Zugriffsprotokolle an einen von Ihnen gewählten Bucket übermittelt. Ein Zugriffsprotokoll enthält Details zu jeder Anfrage, wie z. B. den Anfragetyp, die in der Anfrage angegebenen Ressourcen sowie die Uhrzeit und das Datum der Bearbeitung der Anfrage. Standardmäßig ist die Bucket-Protokollierung nicht aktiviert. Sie sollten die Protokollierung aktivieren, wenn Sie Sicherheitsprüfungen durchführen oder mehr über Benutzer und Nutzungsmuster erfahren möchten.

Bei der erstmaligen Aktivierung der Protokollierung wird die Konfiguration automatisch validiert. Zukünftige Änderungen können jedoch zu Protokollierungsfehlern führen. Bei dieser Prüfung werden explizite Amazon S3-Bucket-Berechtigungen untersucht. Es hat sich bewährt, Bucket-Richtlinien zur Steuerung von Bucket-Berechtigungen zu verwenden, es können jedoch auch ACLs verwendet werden.

Prüf-ID

`c1fd6b96l4`

Warnungskriterien

- Gelb: Die Serverzugriffsprotokollierung ist für den Bucket nicht aktiviert.

- Gelb: Die Berechtigungen des Ziel-Buckets umfassen das Root-Konto nicht, weshalb Trusted Advisor es nicht überprüfen kann.
- Rot: Der Ziel-Bucket ist nicht vorhanden.
- Rot: Der Ziel-Bucket und der Quell-Bucket haben unterschiedliche Eigentümer.
- Rot: Der Protokollbereitsteller hat keine Schreibberechtigung für den Ziel-Bucket.
- Grün: Für den Bucket ist die Serverzugriffsprotokollierung aktiviert, das Ziel ist vorhanden und es sind Schreibberechtigungen für das Ziel vorhanden

Empfohlene Aktion

Aktivieren Sie die Bucket-Protokollierung für die meisten Buckets. Weitere Informationen finden Sie unter Aktivieren der Protokollierung mithilfe der Konsole und Aktivieren der programmgesteuerten Protokollierung.

Wenn die Berechtigungen des Ziel-Buckets das Root-Konto nicht umfassen und Trusted Advisor den Protokollierungsstatus überprüfen soll, fügen Sie das Root-Konto als Empfänger hinzu. Weitere Informationen finden Sie unter Editing Bucket Permissions (Bearbeiten von Bucket-Berechtigungen).

Wenn der Ziel-Bucket nicht existiert, wählen Sie einen vorhandenen Bucket als Ziel aus oder erstellen Sie einen neuen und wählen Sie ihn aus. Weitere Informationen finden Sie unter Managing Bucket Logging (Verwalten der Bucket-Protokollierung).

Wenn das Ziel und die Quelle unterschiedliche Eigentümer haben, ändern Sie den Ziel-Bucket in einen Bucket mit demselben Eigentümer wie der Quell-Bucket. Weitere Informationen finden Sie unter Managing Bucket Logging (Verwalten der Bucket-Protokollierung).

Wenn der Protokollzusteller keine Schreibberechtigungen für das Ziel hat (Schreiben nicht aktiviert), gewähren Sie der Protokollbereitstellungsgruppe die Berechtigungen zum Hochladen/Löschen. Es wird empfohlen, Bucket-Richtlinien anstelle von ACLs zu verwenden. Weitere Informationen finden Sie unter Bearbeiten von Bucket-Berechtigungen und Berechtigungen für die Protokollzustellung.

Weitere Ressourcen

Mit Buckets arbeiten

Server access logging (Server-Zugriffsprotokollierung)

Format des Serverzugriffsprotokolls

Löschen von Protokolldateien

Berichtsspalten

- Status
- Region
- ARN-Ressourcen
- Bucket-Name
- Ziel-Name
- Ziel ist vorhanden
- Derselbe Eigentümer
- Schreiben aktiviert
- Grund
- Zeitpunkt der letzten Aktualisierung

Amazon VPC-Peering-Verbindungen mit deaktivierter DNS-Auflösung

Beschreibung

Überprüft, ob bei Ihren VPC-Peering-Verbindungen die DNS-Auflösung sowohl für die Anforderer-VPCs als auch die Annahme-VPCs aktiviert ist.

Die DNS-Auflösung für eine VPC-Peering-Verbindung ermöglicht die Auflösung von öffentlichen DNS-Hostnamen in private IPv4-Adressen, wenn diese von Ihrem VPC aus abgefragt werden. Dies ermöglicht die Verwendung von DNS-Namen für die Kommunikation zwischen Ressourcen in durch Peering verbundenen VPCs. Die DNS-Auflösung in Ihren VPC-Peering-Verbindungen macht die Anwendungsentwicklung und -verwaltung einfacher und weniger fehleranfällig und stellt sicher, dass Ressourcen immer privat über die VPC-Peering-Verbindung kommunizieren.

Sie können die vpcIds mithilfe der VPCIDS-Parameter in Ihren Regeln angeben. AWS Config

Weitere Informationen finden Sie unter Aktivieren einer DNS-Auflösung für eine VPC-Peering-Verbindung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz124`

Quelle

`AWS Config Managed Rule: vpc-peering-dns-resolution-check`

Warnungskriterien

Gelb: Die DNS-Auflösung ist sowohl für die Anforderer-VPCs als auch die Annahme-VPCs in einer VPC-Peering-Verbindung nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die DNS-Auflösung für Ihre VPC-Peering-Verbindungen.

Weitere Ressourcen

- Ändern der Optionen für VPC-Peering-Verbindungen
- DNS-Attribute in Ihrer VPC

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Backup Tresor ohne ressourcenbasierte Richtlinie zur Verhinderung des Löschens von Wiederherstellungspunkten

Beschreibung

Überprüft, ob AWS Backup Tresore über eine zugeordnete ressourcenbasierte Richtlinie verfügen, die das Löschen von Wiederherstellungspunkten verhindert.

Die ressourcenbasierte Richtlinie verhindert das unerwartete Löschen von Wiederherstellungspunkten, wodurch Sie eine Zugriffskontrolle mit den geringsten Berechtigungen auf Ihre Sicherungsdaten durchsetzen können.

Sie können die AWS Identity and Access Management ARNs, die die Regel nicht einchecken soll, im ArnListHauptparameter Ihrer Regeln angeben. AWS Config

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz152`

Quelle

`AWS Config Managed Rule: backup-recovery-point-manual-deletion-disabled`

Warnungskriterien

Gelb: Es gibt AWS Backup Tresore, für die es keine ressourcenbasierte Richtlinie gibt, um das Löschen von Wiederherstellungspunkten zu verhindern.

Empfohlene Aktion

Erstellen Sie ressourcenbasierte Richtlinien für Ihre AWS Backup Tresore, um das unerwartete Löschen von Wiederherstellungspunkten zu verhindern.

Die Richtlinie muss eine „Deny“ -Anweisung mit den Berechtigungen backup: DeleteRecovery point, backup: UpdateRecovery PointLifecycle und backup: enthalten. PutBackupVaultAccessPolicy

Weitere Informationen finden Sie unter Festlegen von Zugriffsrichtlinien für Sicherungstresore.

Berichtsspalten

- Status

- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CloudTrail Protokollierung

Beschreibung

Überprüft Ihre Verwendung von AWS CloudTrail. CloudTrail bietet einen besseren Einblick in Ihre Aktivitäten, AWS-Konto indem Informationen über AWS API-Aufrufe aufgezeichnet werden, die auf dem Konto getätigt wurden. Anhand dieser Protokolle können Sie beispielsweise feststellen, welche Aktionen ein bestimmter Benutzer während eines bestimmten Zeitraums durchgeführt hat oder welche Benutzer während eines bestimmten Zeitraums Aktionen auf einer bestimmten Ressource durchgeführt haben.

Da CloudTrail Protokolldateien an einen Amazon Simple Storage Service (Amazon S3) -Bucket übermittelt CloudTrail werden, sind Schreibberechtigungen für den Bucket erforderlich. Wenn ein Trail für alle Regionen gilt (die Standardeinstellung beim Erstellen eines neuen Trails), wird der Trail mehrfach im Trusted Advisor -Bericht angezeigt.

Prüf-ID

`vjafUGJ9H0`

Warnungskriterien

- Gelb: CloudTrail meldet Fehler bei der Protokollzustellung für einen Trail.
- Rot: Für eine Region wurde kein Trail erstellt oder die Protokollierung ist für einen Trail deaktiviert.

Empfohlene Aktion

Um einen Trail zu erstellen und die Protokollierung von der Konsole aus zu starten, rufen Sie die AWS CloudTrail -Konsole auf.

Informationen zur Protokollierung finden Sie unter Anhalten und Starten der Protokollierung für einen Trail.

Wenn Sie Fehler bei der Protokollzustellung erhalten, stellen Sie sicher, dass der Bucket vorhanden ist und dass die erforderliche Richtlinie dem Bucket angefügt ist. Weitere Informationen finden Sie unter Amazon-S3-Bucket-Richtlinien.

Weitere Ressourcen

- AWS CloudTrail Benutzerhandbuch
- Unterstützte Regionen
- Unterstützte Services

Berichtsspalten

- Status
- Region
- Trail-Name
- Status der Protokollierung
- Bucket-Name
- Datum der letzten Bereitstellung

AWS Lambda Funktionen, die veraltete Laufzeiten verwenden

Beschreibung

Sucht nach Lambda-Funktionen, deren $LATEST-Version so konfiguriert ist, dass sie eine Laufzeit verwendet, die bald veraltet ist oder veraltet ist. Veraltete Laufzeiten kommen nicht für Sicherheitsupdates oder technischen Support in Frage

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Veröffentlichte Versionen der Lambda-Funktion sind unveränderlich, was bedeutet, dass sie aufgerufen, aber nicht aktualisiert werden können. Nur die `$LATEST`-Version der Lambda-Funktion kann aktualisiert werden. Weitere Informationen finden Sie unter Versionen der Lambda-Funktion.

Prüf-ID

`L4dfs2Q4C5`

Warnungskriterien

- Rot: Die $LATEST-Version der Funktion ist so konfiguriert, dass sie eine Laufzeit verwendet, die bereits veraltet ist.
- Gelb: Die $LATEST-Version der Funktion läuft auf einer Laufzeit, die innerhalb von 180 Tagen veraltet sein wird.

Empfohlene Aktion

Wenn Ihre Funktionen mit einer Laufzeit ausgeführt werden, die bald veraltet ist, sollten Sie sich auf die Migration zu einer unterstützten Laufzeit vorbereiten. Weitere Informationen finden Sie in der Richtlinie für den Laufzeitablauf.

Wir empfehlen Ihnen, frühere Funktionsversionen zu löschen, die Sie nicht mehr verwenden.

Weitere Ressourcen

Lambda-Laufzeiten

Berichtsspalten

- Status
- Region
- Funktion-ARN
- Laufzeit
- Tage bis zur Veraltung
- Datum der Veraltung
- Durchschnittliche tägliche Aufrufe
- Zeitpunkt der letzten Aktualisierung

AWS Well-Architected-Probleme mit hohem Risiko für die Sicherheit

Beschreibung

Prüft auf Probleme mit hohem Risiko (HRI) für Ihre Workloads hinsichtlich der Sicherheit. Diese Prüfung basiert auf Ihren AWS-Well Architected-Beurteilungen. Ihre Prüfergebnisse hängen davon ab, ob Sie die Workload-Bewertung mit AWS Well-Architected durchgeführt haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Wxdfp4B1L3`

Warnungskriterien

- Rot: In der Sicherheitssäule von AWS Well-Architected wurde mindestens ein aktives Problem mit hohem Risiko identifiziert.
- Grün: In der Sicherheitssäule von AWS Well-Architected wurden keine aktiven Probleme mit hohem Risiko festgestellt.

Empfohlene Aktion

AWS Well-Architected hat bei Ihrer Workload-Evaluierung Probleme mit hohem Risiko erkannt. Diese Probleme bieten Möglichkeiten, Risiken zu reduzieren und Geld zu sparen. Melden Sie sich bei AWS Well-Architected an, um Ihre Antworten zu überprüfen und Maßnahmen zur Lösung der aktiven Probleme zu ergreifen.

Berichtsspalten

- Status
- Region
- Workload-ARN
- Name der Workload
- Name des Reviewers
- Workload-Typ
- Startdatum der Workload
- Datum der letzten Änderung der Workload
- Anzahl der identifizierten HRI für die Sicherheit
- Anzahl der behobenen HRI für die Sicherheit

- Anzahl der für die Sicherheit beantworteten Fragen
- Gesamtzahl der Fragen hinsichtlich der Sicherheit
- Zeitpunkt der letzten Aktualisierung

CloudFrontBenutzerdefinierte SSL-Zertifikate im IAM-Zertifikatsspeicher

Beschreibung

Überprüft die SSL-Zertifikate im IAM-Zertifikatsspeicher auf CloudFront alternative Domainnamen. Diese Prüfung warnt Sie, wenn ein Zertifikat abgelaufen ist, in Kürze abläuft, eine veraltete Verschlüsselung verwendet oder nicht korrekt für die Verteilung konfiguriert ist.

Wenn ein benutzerdefiniertes Zertifikat für einen alternativen Domainnamen abläuft, zeigen Browser, die Ihre CloudFront Inhalte anzeigen, möglicherweise eine Warnmeldung über die Sicherheit Ihrer Website an. Zertifikate, die mit dem SHA-1-Hashing-Algorithmus verschlüsselt sind, werden von Webbrowsern wie Chrome und Firefox nicht mehr unterstützt.

Ein Zertifikat muss einen Domainnamen enthalten, der entweder mit dem Ursprungsdomainnamen oder dem Domainnamen im Host-Header einer Viewer-Anforderung übereinstimmt. Wenn es nicht übereinstimmt, wird dem Benutzer der HTTP-Statuscode 502 (schlechtes Gateway) CloudFront zurückgegeben. Weitere Informationen finden Sie unter Verwenden alternativer Domainnamen in Verbindung mit HTTPS.

Prüf-ID

`N425c450f2`

Warnungskriterien

- Rot: Ein benutzerdefiniertes SSL-Zertifikat ist abgelaufen.
- Gelb: Ein benutzerdefiniertes SSL-Zertifikat läuft in den nächsten sieben Tagen ab.
- Gelb: Ein benutzerdefiniertes SSL-Zertifikat wurde mit dem SHA-1-Hashing-Algorithmus verschlüsselt.
- Gelb: Mindestens ein alternativer Domainname in der Verteilung wird entweder im Feld Common Name (Allgemeiner Name) oder im Feld Subject Alternative Names (Alternative Subjektnamen) des benutzerdefinierten SSL-Zertifikats nicht angezeigt.

Empfohlene Aktion

Erneuern Sie ein abgelaufenes Zertifikat oder ein Zertifikat, das bald abläuft.

Ersetzen Sie ein Zertifikat, das mithilfe des SHA-1-Hashing-Algorithmus verschlüsselt wurde, durch ein Zertifikat, das mithilfe des SHA-256-Hashing-Algorithmus verschlüsselt wurde.

Ersetzen Sie das Zertifikat durch ein Zertifikat, das die entsprechenden Werte im Feld Common Name (Allgemeiner Name) oder im Feld Subject Alternative Domain Names (Alternative Domainnamen des Subjekts) enthält.

Weitere Ressourcen

Zugriff auf Ihre Objekte unter Verwendung einer HTTPS-Verbindung

Berichtsspalten

- Status
- Verteilungs-ID
- Verteilungs-Domainname
- Name des Zertifikats
- Grund

CloudFront SSL-Zertifikat auf dem Ursprungsserver

Beschreibung

Überprüft Ihren Ursprungsserver auf SSL-Zertifikate, die abgelaufen sind, demnächst ablaufen, fehlen oder eine veraltete Verschlüsselung verwenden. Wenn ein Zertifikat eines dieser Probleme aufweist, CloudFront reagiert es auf Anfragen nach Ihren Inhalten mit dem HTTP-Statuscode 502, Bad Gateway.

Zertifikate, die mit dem SHA-1-Hashing-Algorithmus verschlüsselt wurden, werden von Webbrowsern wie Chrome und Firefox nicht mehr unterstützt. Abhängig von der Anzahl der SSL-Zertifikate, die Sie mit Ihren CloudFront Distributionen verknüpft haben, kann diese Prüfung Ihre Rechnung bei Ihrem Webhosting-Anbieter um einige Cent pro Monat erhöhen, z. B. AWS wenn Sie Amazon EC2 oder Elastic Load Balancing als Quelle für Ihre CloudFront Distribution verwenden. Bei dieser Prüfung werden die Ursprungszertifikatskette und die Zertifizierungsstellen nicht überprüft. Sie können diese in Ihrer CloudFront Konfiguration überprüfen.

Prüf-ID

`N430c450f2`

Warnungskriterien

- Rot: Ein SSL-Zertifikat für Ihren Ursprung ist abgelaufen oder fehlt.

- Gelb: Ein SSL-Zertifikat für Ihren Ursprung läuft in den nächsten dreißig Tagen ab.
- Gelb: Ein SSL-Zertifikat für Ihren Ursprung wurde mit dem SHA-1-Hashing-Algorithmus verschlüsselt.
- Gelb: Ein SSL-Zertifikat für Ihren Ursprung kann nicht gefunden werden. Die Verbindung ist möglicherweise aufgrund eines Timeouts oder anderer HTTPS-Verbindungsprobleme fehlgeschlagen.

Empfohlene Aktion

Erneuern Sie das Zertifikat für Ihren Ursprung, wenn es abgelaufen ist oder bald abläuft.

Fügen Sie ein Zertifikat hinzu, wenn keines vorhanden ist.

Ersetzen Sie ein Zertifikat, das mithilfe des SHA-1-Hashing-Algorithmus verschlüsselt wurde, durch ein Zertifikat, das mithilfe des SHA-256-Hashing-Algorithmus verschlüsselt wurde.

Weitere Ressourcen

Verwenden alternativer Domainnamen in Verbindung mit HTTPS

Berichtsspalten

- Status
- Verteilungs-ID
- Verteilungs-Domänenname
- Ursprung
- Grund

ELB-Listener-Sicherheit

Beschreibung

Sucht nach Load Balancern mit Listenern, die keine empfohlenen Sicherheitskonfigurationen für verschlüsselte Kommunikation verwenden. AWS empfiehlt die Verwendung eines sicheren Protokolls (HTTPS oder SSL), up-to-date Sicherheitsrichtlinien sowie sicherer Verschlüsselungen und Protokolle.

Wenn Sie ein sicheres Protokoll für eine Front-End-Verbindung (Client zu Load Balancer) verwenden, werden die Anfragen zwischen Ihren Clients und dem Load Balancer verschlüsselt,

was eine sicherere Umgebung schafft. Elastic Load Balancing bietet vordefinierte Sicherheitsrichtlinien mit Chiffren und Protokollen, die den bewährten AWS Sicherheitsmethoden entsprechen. Neue Versionen der vordefinierten Richtlinien werden veröffentlicht, sobald neue Konfigurationen verfügbar sind.

Prüf-ID

`a2sEc6ILx`

Warnungskriterien

- Gelb: Ein Load Balancer hat keinen Listener, der ein sicheres Protokoll (HTTPS oder SSL) verwendet.
- Gelb: Ein Load-Balancer-Listener verwendet eine veraltete vordefinierte SSL-Sicherheitsrichtlinie.
- Gelb: Ein Load-Balancer-Listener verwendet eine Verschlüsselung oder ein Protokoll, die bzw. das nicht empfohlen wird.
- Rot: Ein Load-Balancer-Listener verwendet eine unsichere Verschlüsselung oder ein unsicheres Protokoll.

Empfohlene Aktion

Wenn der Datenverkehr zu Ihrem Load Balancer sicher sein muss, verwenden Sie entweder das HTTPS- oder das SSL-Protokoll für die Frontend-Verbindung.

Aktualisieren Sie Ihren Load Balancer auf die neueste Version der vordefinierten SSL-Sicherheitsrichtlinie.

Verwenden Sie nur die empfohlenen Verschlüsselungsverfahren und Protokolle.

Weitere Informationen finden Sie unter Listener Configurations for Elastic Load Balancing (Listener-Konfigurationen für Elastic Load Balancing).

Weitere Ressourcen

- Kurzanleitung zu Listener-Konfigurationen
- Update SSL Negotiation Configuration of Your Load Balancer (Aktualisieren der SSL-Aushandlungskonfiguration Ihres Load Balancers)
- SSL Negotiation Configurations for Elastic Load Balancing (SSL-Aushandlungskonfigurationen für Elastic Load Balancing)
- SSL Security Policy Table (Tabelle der SSL-Sicherheitsrichtlinien)

Berichtsspalten

- Status
- Region
- Load-Balancer-Name
- Load-Balancer-Port
- Grund

ELB-Sicherheitsgruppen

Beschreibung

Prüft auf Load Balancer, die mit einer fehlenden Sicherheitsgruppe konfiguriert sind, oder auf eine Sicherheitsgruppe, die den Zugriff auf Ports erlaubt, die nicht für den Load Balancer konfiguriert sind.

Wenn eine Sicherheitsgruppe, die mit einem Load Balancer verbunden ist, gelöscht wird, funktioniert der Load Balancer nicht wie erwartet. Wenn eine Sicherheitsgruppe den Zugriff auf Ports zulässt, die nicht für den Load Balancer konfiguriert sind, steigt das Risiko von Datenverlusten oder bösartigen Angriffen.

Prüf-ID

`xSqX82fQu`

Warnungskriterien

- Gelb: Die eingehenden Regeln einer Amazon-VPC-Sicherheitsgruppe, die mit einem Load Balancer verknüpft ist, ermöglichen den Zugriff auf Ports, die nicht in der Listener-Konfiguration des Load Balancers definiert sind.
- Rot: Eine mit einem Load Balancer verknüpfte Sicherheitsgruppe ist nicht vorhanden.

Empfohlene Aktion

Konfigurieren Sie die Sicherheitsgruppenregeln so, dass der Zugriff auf die Ports und Protokolle beschränkt wird, die in der Listener-Konfiguration des Load Balancers festgelegt sind, sowie auf das ICMP-Protokoll zur Unterstützung von Path MTU Discovery. Weitere Informationen finden Sie unter Listener für Ihren Classic Load Balancer und Sicherheitsgruppen für Load Balancer in einer VPC.

Fehlt eine Sicherheitsgruppe, wenden Sie eine neue Sicherheitsgruppe auf den Load Balancer an. Erstellen Sie Sicherheitsgruppenregeln, die den Zugriff auf die Ports und Protokolle

beschränken, die in der Listener-Konfiguration des Load Balancers festgelegt sind. Weitere Informationen finden Sie unter Sicherheitsgruppen für Load Balancer in einer VPC.

Weitere Ressourcen

- Elastic-Load-Balancing-Benutzerhandbuch
- Konfigurieren Ihres Classic Load Balancers

Berichtsspalten

- Status
- Region
- Load-Balancer-Name
- Sicherheitsgruppen-IDs
- Grund

Exposed Access Keys

Beschreibung

Prüft beliebte Code-Repositories auf Zugangsschlüssel, die öffentlich zugänglich gemacht wurden, und auf unregelmäßige Amazon Elastic Compute Cloud (Amazon EC2)-Nutzung, die das Ergebnis eines kompromittierten Zugangsschlüssels sein könnte.

Ein Zugangsschlüssel besteht aus einer Zugangsschlüssel-ID und dem entsprechenden geheimen Zugangsschlüssel. Ungeschützte Zugangsschlüssel stellen ein Sicherheitsrisiko für Ihr Konto und andere Nutzer dar, können zu überhöhten Gebühren durch unbefugte Aktivitäten oder Missbrauch führen und verstoßen gegen die AWS Kundenvereinbarung.

Wenn Ihr Zugangsschlüssel offengelegt wurde, ergreifen Sie sofort Maßnahmen zur Sicherung Ihres Kontos. Um Ihr Konto vor übermäßigen Gebühren zu schützen, wird Ihre Fähigkeit, einige AWS Ressourcen zu erstellen, AWS vorübergehend eingeschränkt. Dies macht Ihr Konto nicht sicher. Dies schränkt die unerlaubte Nutzung, die Ihnen in Rechnung gestellt werden könnte, nur teilweise ein.

> **Note**
>
> Diese Prüfung garantiert nicht die Identifizierung offener Zugangsschlüssel oder kompromittierter EC2-Instances. Letztlich sind Sie für die Sicherheit Ihrer Zugangsschlüssel und AWS Ressourcen verantwortlich.

Die Ergebnisse dieser Prüfung werden automatisch aktualisiert und Aktualisierungsanforderungen sind nicht zulässig. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Wenn für einen Zugangsschlüssel eine Frist angegeben ist, AWS können Sie Ihren Schlüssel sperren, AWS-Konto sofern die unbefugte Nutzung bis zu diesem Datum nicht gestoppt wird. Wenn Sie der Meinung sind, dass es sich bei einer Warnung um einen Fehler handelt, wenden Sie sich an AWS Support.

Die unter angezeigten Informationen geben Trusted Advisor möglicherweise nicht den aktuellen Status Ihres Kontos wieder. Kompromittierte Zugriffsschlüssel werden erst als aufgelöst markiert, wenn alle kompromittierten Zugriffsschlüssel des Kontos aufgelöst wurden. Diese Datensynchronisierung kann bis zu einer Woche dauern.

Prüf-ID

`12Fnkpl8Y5`

Warnungskriterien

- Rot: Potenziell gefährdet — AWS hat eine Zugriffsschlüssel-ID und einen entsprechenden geheimen Zugriffsschlüssel identifiziert, die im Internet veröffentlicht und möglicherweise kompromittiert (verwendet) wurden.
- Rot: Offengelegt — AWS hat eine Zugangsschlüssel-ID und den entsprechenden geheimen Zugriffsschlüssel identifiziert, die im Internet offengelegt wurden.
- Rot: Verdächtig – Eine unregelmäßige Nutzung von Amazon EC2 deutet darauf hin, dass ein Zugriffsschlüssel möglicherweise kompromittiert wurde, aber nicht als im Internet offengelegt identifiziert wurde.

Empfohlene Aktion

Löschen Sie den betroffenen Zugriffsschlüssel schnellstmöglich. Wenn der Schlüssel mit einem IAM-Benutzer verknüpft ist, finden Sie weitere Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer.

Überprüfen Sie, ob Ihr Konto unbefugt genutzt wurde. Melden Sie sich bei der AWS Management Console an und überprüfen Sie jede Servicekonsole auf verdächtige Ressourcen. Achten Sie besonders auf die Ausführung von Amazon-EC2-Instances, Spot-Instance-Anfragen, Zugriffsschlüssel und IAM-Benutzer. Sie können die Gesamtnutzung auch in der Konsole für Fakturierung und Kostenmanagement überprüfen.

Weitere Ressourcen

- Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln
- AWS Richtlinien für Sicherheitsaudits

Berichtsspalten

- Access Key ID
- Benutzername (IAM oder Stammbenutzer)
- Art des Betrugs
- Fall-ID
- Aktualisierungszeitpunkt
- Ort
- Frist
- Nutzung (USD pro Tag)

IAM-Zugriffsschlüssel-Rotation

Beschreibung

Prüft auf aktiven IAM-Zugangsschlüsseln, die in den letzten 90 Tagen nicht rotiert wurden.

Wenn Sie Ihre Zugangsschlüssel regelmäßig wechseln, verringern Sie die Wahrscheinlichkeit, dass ein kompromittierter Schlüssel ohne Ihr Wissen für den Zugriff auf Ressourcen verwendet werden kann. Für die Zwecke dieser Prüfung ist das Datum und die Uhrzeit der letzten Rotation der Zeitpunkt, an dem der Zugangsschlüssel erstellt oder zuletzt aktiviert wurde. Die Nummer und das Datum des Zugriffsschlüssels stammen aus den `access_key_1_last_rotated` und `access_key_2_last_rotated` Informationen aus dem letzten IAM-Berechtigungsbericht.

Da die Regenerierungshäufigkeit eines Berichts mit Anmeldeinformationen eingeschränkt ist, spiegelt das Aktualisieren dieser Prüfung möglicherweise nicht die letzten Änderungen wider. Weitere Informationen finden Sie unter Abrufen von Berichten zu Anmeldeinformationen für Ihr AWS-Konto-Konto.

Um Zugriffsschlüssel erstellen und rotieren zu können, muss ein Benutzer über die entsprechenden Berechtigungen verfügen. Weitere Informationen finden Sie unter Benutzern erlauben, ihre eigenen Passwörter, Zugriffsschlüssel und SSH-Schlüssel zu verwalten.

Prüf-ID

DqdJqYeRm5

Warnungskriterien

- Grün: Der Zugriffsschlüssel ist aktiv und wurde in den letzten 90 Tagen rotiert.
- Gelb: Der Zugriffsschlüssel ist aktiv und wurde in den letzten 2 Jahren, aber vor mehr als 90 Tagen, rotiert.
- Rot: Der Zugriffsschlüssel ist aktiv und wurde in den letzten 2 Jahren nicht rotiert.

Empfohlene Aktion

Rotieren Sie die Zugriffsschlüssel regelmäßig. Weitere Informationen finden Sie unter Rotieren von Zugriffsschlüsseln und Verwalten der Zugriffsschlüssel für IAM-Benutzer.

Weitere Ressourcen

- IAM Best Practices
- Rotieren von Zugriffsschlüsseln für IAM-Benutzer

Berichtsspalten

- Status
- IAM-Benutzer
- Zugriffsschlüssel
- Letzte Rotation des Schlüssels
- Grund

IAM–Passwortrichtlinie

Beschreibung

Prüft die Passwortrichtlinie für Ihr Konto und warnt, wenn keine Passwortrichtlinie aktiviert ist oder wenn die Anforderungen an den Kennwortinhalt nicht aktiviert wurden.

Die Anforderungen an den Inhalt von Passwörtern erhöhen die allgemeine Sicherheit Ihrer AWS Umgebung, indem sie die Erstellung von sicheren Benutzerpasswörtern erzwingen. Wenn Sie eine Passwortrichtlinie erstellen oder ändern, wird die Änderung sofort für neue Benutzer erzwungen, aber bestehende Benutzer müssen ihre Passwörter nicht ändern.

Prüf-ID

Yw2K9puPzl

Warnungskriterien

- Gelb: Eine Passwortrichtlinie ist aktiviert, aber mindestens eine Inhaltsanforderung ist nicht aktiviert.
- Rot: Es ist keine Passwortrichtlinie aktiviert.

Empfohlene Aktion

Wenn einige Inhaltsanforderungen nicht aktiviert sind, sollten Sie die Aktivierung in Erwägung ziehen. Wenn keine Passwortrichtlinie aktiviert ist, erstellen und konfigurieren Sie eine. Weitere Informationen finden Sie unter Einrichten einer Kontopasswortrichtlinie für IAM-Benutzer.

Weitere Ressourcen

Verwalten von Passwörtern

Berichtsspalten

- Kennwortrichtlinien
- Großbuchstaben
- Kleinschreibung
- Zahl
- Nicht-alphanumerisch

MFA auf Root-Konto

Beschreibung

Prüft das Root-Konto und warnt, wenn die Multi-Faktor-Authentifizierung (MFA) nicht aktiviert ist.

Um die Sicherheit zu erhöhen, empfehlen wir Ihnen, Ihr Konto mithilfe von MFA zu schützen. Dabei muss ein Benutzer bei der Interaktion mit den AWS Management Console und den zugehörigen Websites einen eindeutigen Authentifizierungscode von seiner MFA-Hardware oder seinem virtuellen Gerät eingeben.

Prüf-ID

`7DAFEmoDos`

Warnungskriterien

Rot: MFA ist für das Root-Konto nicht aktiviert.

Empfohlene Aktion

Loggen Sie sich in Ihr Root-Konto ein und aktivieren Sie ein MFA-Gerät. Weitere Informationen finden Sie unter Überprüfen des MFA-Status und Einrichten eines MFA-Gerätes.

Weitere Ressourcen

Verwenden von Geräten mit Multi-Factor Authentication (MFA) mit AWS

Sicherheitsgruppen – Bestimmte Ports uneingeschränkt

Beschreibung

Prüft Sicherheitsgruppen auf Regeln, die den uneingeschränkten Zugriff (0.0.0.0/0) auf bestimmte Ports erlauben.

Uneingeschränkter Zugriff erhöht die Wahrscheinlichkeit bösartiger Aktivitäten (Hacking, denial-of-service Angriffe, Datenverlust). Die Häfen mit dem höchsten Risiko sind rot gekennzeichnet, die Häfen mit einem geringeren Risiko sind gelb gekennzeichnet. Grün markierte Ports werden in der Regel von Anwendungen verwendet, die einen uneingeschränkten Zugriff erfordern, wie z. B. HTTP und SMTP.

Wenn Sie Ihre Sicherheitsgruppen absichtlich auf diese Weise konfiguriert haben, empfehlen wir zusätzliche Sicherheitsmaßnahmen zur Sicherung Ihrer Infrastruktur (z. B. IP-Tabellen).

> **Note**
>
> Bei dieser Prüfung werden nur von Ihnen erstellte Sicherheitsgruppen und deren eingehende Regeln für IPv4-Adressen ausgewertet. Sicherheitsgruppen, die von AWS Directory Service erstellt wurden, werden als rot oder gelb gekennzeichnet, stellen aber kein Sicherheitsrisiko dar und können getrost ignoriert oder ausgeschlossen werden. Weitere Informationen finden Sie unter Trusted Advisor FAQ.

> **Note**
>
> Diese Prüfung umfasst nicht den Anwendungsfall, in dem eine vom Kunden verwaltete Präfixliste Zugriff auf 0.0.0.0/0 gewährt und als Quelle mit einer Sicherheitsgruppe verwendet wird.

Prüf-ID

HCP4007jGY

Warnungskriterien

- Grün: Der Zugriff auf Port 80, 25, 443 oder 465 ist nicht eingeschränkt.
- Rot: Der Zugriff auf Port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432 oder 5500 ist nicht eingeschränkt.
- Gelb: Der Zugriff auf alle anderen Ports ist nicht eingeschränkt.

Empfohlene Aktion

Beschränken Sie den Zugriff auf die IP-Adressen, für die dies erforderlich ist. Um den Zugriff auf eine bestimmte IP-Adresse einzuschränken, legen Sie das Suffix auf /32 fest (z. B. 192.0.2.10/32). Achten Sie darauf, übermäßig freizügige Regeln zu löschen, nachdem Sie restriktivere Regeln erstellt haben.

Weitere Ressourcen

- Amazon-EC2-Sicherheitsgruppen

  Liste der TCP- und UDP-Portnummern
- Classless Inter-Domain Routing

Berichtsspalten

- Status
- Region
- Name der Sicherheitsgruppe
- Sicherheitsgruppen-ID
- Protokoll
- Von Port
- An Port

Sicherheitsgruppen – Uneingeschränkter Zugriff

Beschreibung

Prüft Sicherheitsgruppen auf Regeln, die den uneingeschränkten Zugriff auf eine Ressource erlauben.

Uneingeschränkter Zugriff erhöht die Wahrscheinlichkeit bösartiger Aktivitäten (Hacking, denial-of-service Angriffe, Datenverlust).

> **Note**
>
> Bei dieser Prüfung werden nur von Ihnen erstellte Sicherheitsgruppen und deren eingehende Regeln für IPv4-Adressen ausgewertet. Sicherheitsgruppen, die von AWS Directory Service erstellt wurden, werden als rot oder gelb gekennzeichnet, stellen aber kein Sicherheitsrisiko dar und können getrost ignoriert oder ausgeschlossen werden. Weitere Informationen finden Sie unter Trusted Advisor FAQ.

> **Note**
>
> Diese Prüfung umfasst nicht den Anwendungsfall, in dem eine vom Kunden verwaltete Präfixliste Zugriff auf 0.0.0.0/0 gewährt und als Quelle mit einer Sicherheitsgruppe verwendet wird.

Prüf-ID

`1iG5NDGVre`

Warnungskriterien

Rot: Eine Sicherheitsgruppenregel hat eine Quell-IP-Adresse mit einem /0-Suffix für andere Ports als 25, 80 oder 443.

Empfohlene Aktion

Beschränken Sie den Zugriff auf die IP-Adressen, für die dies erforderlich ist. Um den Zugriff auf eine bestimmte IP-Adresse einzuschränken, legen Sie das Suffix auf /32 fest (z. B. 192.0.2.10/32). Achten Sie darauf, übermäßig freizügige Regeln zu löschen, nachdem Sie restriktivere Regeln erstellt haben.

Weitere Ressourcen

- Amazon-EC2-Sicherheitsgruppen
- Classless Inter-Domain Routing

Berichtsspalten

- Status

- Region
- Name der Sicherheitsgruppe
- Sicherheitsgruppen-ID
- Protokoll
- Von Port
- An Port
- IP-Bereich

Fehlertoleranz

Für die Kategorie Fehlertoleranz können Sie die folgenden Prüfungen verwenden.

Namen prüfen

- ALB Multi-AZ
- Amazon-Aurora-MySQL-Cluster-Rückverfolgung nicht aktiviert
- Barrierefreiheit von Amazon Aurora-DB-Instances
- Amazon CloudFront Origin Failover
- Amazon Comprehend Endpunkt-Zugriffsrisiko
- Amazon DocumentDB Single-AZ-Cluster
- Wiederherstellung von Amazon DynamoDB P oint-in-time
- Amazon-DynamoDB-Tabelle ist nicht im Backup-Plan enthalten
- Amazon EBS ist nicht im AWS Backup Plan enthalten
- Amazon EBS-Snapshots
- Bei Amazon EC2 Auto Scaling ist die ELB-Zustandsprüfung nicht aktiviert
- Für Amazon-EC2-Auto-Scaling-Gruppe ist Kapazitätsausgleich aktiviert
- Amazon EC2 Auto Scaling wird nicht in mehreren Availability Zones bereitgestellt oder erreicht nicht die Mindestanzahl von Availability Zones
- Amazon EC2 Availability Zone Balance
- Detaillierte Amazon-EC2-Überwachung nicht aktiviert
- Amazon ECS AWS Logs-Treiber im Blockierungsmodus
- Amazon-ECS-Service mit einer einzigen Availability Zone
- Amazon-ECS-Multi-AZ-Platzierungsstrategie

- Amazon EFS – Keine Mount-Ziel-Redundanz
- Amazon EFS ist nicht im AWS Backup Plan enthalten
- Amazon ElastiCache Multi-AZ-Cluster
- Automatische Backup ElastiCache von Amazon Redis-Clustern
- Amazon-MemoryDB-Multi-AZ-Cluster
- Amazon-MSK-Broker, die zu viele Partitionen hosten
- Amazon OpenSearch Service-Domains mit weniger als drei Datenknoten
- Amazon RDS-Backups
- Amazon RDS-DB-Cluster haben eine DB-Instance
- Amazon RDS-DB-Cluster mit allen Instances in derselben Availability Zone
- Amazon RDS-DB-Cluster mit allen Reader-Instances in derselben Availability Zone
- Erweiterte Überwachung der Amazon-RDS-DB-Instance ist nicht aktiviert
- Bei Amazon RDS-DB-Instances ist die automatische Speicherskalierung deaktiviert
- Amazon RDS-DB-Instances, die keine Multi-AZ-Bereitstellung verwenden
- Amazon RDS DiskQueueDepth
- Amazon RDS FreeStorageSpace
- Der Amazon RDS-Parameter log_output ist auf Tabelle gesetzt
- Die Amazon RDS-Parametereinstellung innodb_default_row_format ist unsicher
- Der Amazon RDS-Parameter innodb_flush_log_at_trx_commit ist nicht 1
- Der Amazon RDS-Parameter max_user_connections ist niedrig
- Amazon RDS Multi-AZ
- Amazon RDS nicht im AWS Backup Plan
- Amazon RDS Read Replicas sind im schreibbaren Modus geöffnet
- Automatisierte Amazon RDS-Ressourcen-Backups sind deaktiviert
- Der Amazon RDS-Parameter sync_binlog ist ausgeschaltet
- Für den RDS-DB-Cluster ist keine Multi-AZ-Replikation aktiviert
- RDS-Multi-AZ-Standby-Instance ist nicht aktiviert
- Amazon RDS ReplicaLag
- Der Amazon RDS-Parameter synchronous_commit ist ausgeschaltet
- Automatisierte Amazon-Redshift-Cluster-Snapshots

- Amazon Route 53 gelöschte Integritätsprüfungen
- Amazon Route 53 Failover-Ressourceneintragsätze
- Amazon Route 53 Hohe TTL Ressourceneintragsätze
- Amazon Route 53-Namenserver-Delegationen
- Amazon Route 53 Resolver Redundanz der Endpunkt-Verfügbarkeitszonen
- Amazon S3 Bucket-Protokollierung
- Replikation des Amazon-S3-Buckets ist nicht aktiviert
- Amazon S3 Bucket-Versioning
- Application Load Balancer, Network Load Balancer und Gateway Load Balancer, die sich nicht über mehrere Availability Zones erstrecken
- Für Auto Scaling verfügbare IPs in Subnetzen
- Auto-Scaling-Gruppe Zustandsprüfungen
- Auto-Scaling-Gruppe-Ressourcen
- AWS CloudHSM -Cluster, auf denen HSM-Instances in einer einzigen AZ ausgeführt werden
- AWS Direct Connect Ausfallsicherheit des Standorts
- AWS Lambda funktioniert, ohne dass eine Warteschlange für unzustellbare Nachrichten konfiguriert ist
- AWS Lambda Ziele für Ereignisse bei einem Ausfall
- AWS Lambda VPC-fähige Funktionen ohne Multi-AZ-Redundanz
- AWS Resilience Hub Überprüfung der Anwendungskomponenten
- AWS Resilience Hub Richtlinie verletzt
- AWS Resilience Hub Resilienzwerte
- AWS Resilience Hub Alter der Bewertung
- AWS Site-to-Site VPN hat mindestens einen Tunnel im Status DOWN
- AWS Well-Architected-Probleme mit hohem Risiko für die Zuverlässigkeit
- Für Classic Load Balancer sind nicht mehrere AZs konfiguriert.
- ELB Connection Draining
- Load Balancer Optimization
- NAT-Gateway-AZ-Unabhängigkeit
- Network Load Balancer – Zonenübergreifender Lastausgleich
- NLB — Mit dem Internet verbundene Ressource in einem privaten Subnetz

- NLB Multi-AZ
- Nummer von AWS-Regionen in einem Incident Manager-Replikationssatz
- Einzelne AZ-Anwendungsprüfung
- VPC-Schnittstelle, Endpunkt-Netzwerkschnittstellen in mehreren AZs
- VPN-Tunnelredundanz
- Redundanz der ActiveMQ-Availability-Zone
- RabbitMQ-Availability-Zone-Redundanz

ALB Multi-AZ

Beschreibung

Überprüft, ob Ihre Application Load Balancer so konfiguriert sind, dass sie mehr als eine Availability Zone (AZ) verwenden. Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Konfigurieren Sie Ihren Load Balancer in mehreren AZs in derselben Region, um Ihre Workload-Verfügbarkeit zu verbessern.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch08`

Warnungskriterien

Gelb: ALB befindet sich in einer einzigen AZ.

Grün: ALB hat zwei oder mehr AZs.

Empfohlene Aktion

Stellen Sie sicher, dass Ihr Load Balancer mit mindestens zwei Availability Zones konfiguriert ist.

Weitere Informationen finden Sie unter Availability Zones für Ihren Application Load Balancer.

Weitere Ressourcen

Weitere Informationen finden Sie in der folgenden -Dokumentation:

- So funktioniert Elastic Load Balancing
- Regionen, Availability Zones und lokale Zonen

Berichtsspalten

- Status
- Region
- ALB-Name
- ALB-Regel
- ALB ARN
- Anzahl der AZs
- Zeitpunkt der letzten Aktualisierung

Amazon-Aurora-MySQL-Cluster-Rückverfolgung nicht aktiviert

Beschreibung

Prüft, ob für einen Amazon-Aurora-MySQL-Cluster die Rückverfolgung aktiviert ist.

Amazon-Aurora-MySQL-Cluster-Rückverfolgung ist eine Funktion, mit der Sie einen Aurora-DB-Cluster auf einen früheren Zeitpunkt zurücksetzen können, ohne einen neuen Cluster zu erstellen. Sie können Ihre Datenbank innerhalb eines Aufbewahrungszeitraums auf einen bestimmten Zeitpunkt zurücksetzen, ohne dass eine Wiederherstellung aus einem Snapshot notwendig ist.

Sie können das Backtracking-Zeitfenster (Stunden) im BacktrackWindowInHoursParameter der AWS Config Regeln anpassen.

Weitere Informationen finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz131`

Quelle

`AWS Config Managed Rule: aurora-mysql-backtracking-enabled`

Warnungskriterien

Gelb: Die Amazon-Aurora-MySQL-Cluster-Rückverfolgung ist nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die Rückverfolgung für Ihren Amazon-Aurora-MySQL-Cluster.

Weitere Informationen finden Sie unter Rückverfolgen eines Aurora-DB-Clusters.

Weitere Ressourcen

Rückverfolgen eines Aurora-DB-Clusters

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Barrierefreiheit von Amazon Aurora-DB-Instances

Beschreibung

Prüft auf Fälle, in denen ein Amazon Aurora DB-Cluster sowohl private als auch öffentliche Instances hat.

Wenn Ihre primäre Instance ausfällt, kann ein Replikat zu einer primären Instance befördert werden. Wenn diese Replik privat ist, können Benutzer, die nur öffentlichen Zugriff haben, nach dem Failover keine Verbindung mehr zur Datenbank herstellen. Wir empfehlen, dass alle DB-Instances in einem Cluster die gleiche Zugänglichkeit haben.

Prüf-ID

`xuy7H1avtl`

Warnungskriterien

Gelb: Die Instances in einem Aurora-DB-Cluster sind auf unterschiedliche Weise zugänglich (eine Mischung aus öffentlich und privat).

Empfohlene Aktion

Ändern Sie die `Publicly Accessible`-Einstellung der Instances im DB-Cluster, sodass sie alle entweder öffentlich oder privat sind. Weitere Informationen finden Sie in den Anweisungen für MySQL-Instances unter Ändern einer DB-Instance mit ausgeführter MySQL-Datenbank-Engine.

Weitere Ressourcen

Fehlertoleranz für einen Aurora-DB-Cluster

Berichtsspalten

- Status
- Region
- Cluster
- Öffentliche DB-Instances
- Private DB-Instances
- Grund

Amazon CloudFront Origin Failover

Beschreibung

Überprüft, ob eine Ursprungsgruppe für Distributionen konfiguriert ist, die zwei Ursprünge in Amazon CloudFront enthalten.

Weitere Informationen finden Sie unter Optimierung der Hochverfügbarkeit mit CloudFront Origin-Failover.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz112`

Quelle

`AWS Config Managed Rule: cloudfront-origin-failover-enabled`

Warnungskriterien

Gelb: Amazon CloudFront Origin Failover ist nicht aktiviert.

Empfohlene Aktion

Stellen Sie sicher, dass Sie die Origin-Failover-Funktion für Ihre CloudFront Distributionen aktivieren, um eine hohe Verfügbarkeit Ihrer Inhalte für Endbenutzer sicherzustellen. Wenn Sie diese Funktion aktivieren, wird der Datenverkehr automatisch an den Backup-Ursprungsserver weitergeleitet, falls der primäre Ursprungsserver nicht verfügbar ist. Dadurch werden potenzielle Ausfallzeiten minimiert und die kontinuierliche Verfügbarkeit Ihrer Inhalte gewährleistet.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon Comprehend Endpunkt-Zugriffsrisiko

Beschreibung

Prüft die Schlüsselberechtigungen AWS Key Management Service (AWS KMS) für einen Endpunkt, auf dem das zugrunde liegende Modell mithilfe von vom Kunden verwalteten Schlüsseln verschlüsselt wurde. Wenn der kundenverwaltete Schlüssel deaktiviert ist, oder die

Schlüsselrichtlinie geändert wurde, um die erlaubten Berechtigungen für Amazon Comprehend zu ändern, könnte die Verfügbarkeit des Endpunkts beeinträchtigt werden.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Cm24dfsM13`

Warnungskriterien

Rot: Der kundenverwaltete Schlüssel ist deaktiviert oder die Schlüsselrichtlinie wurde geändert, um die erlaubten Berechtigungen für den Zugriff auf Amazon Comprehend zu ändern.

Empfohlene Aktion

Wenn der vom Kunden verwaltete Schlüssel deaktiviert wurde, empfehlen wir die Aktivierung. Weitere Informationen finden Sie unter Aktivieren von Schlüsseln. Wenn die Schlüsselrichtlinie geändert wurde und Sie den Endpunkt weiterhin verwenden möchten, empfehlen wir Ihnen, die AWS KMS Schlüsselrichtlinie zu aktualisieren. Weitere Informationen finden Sie unter Changing a key policy (Ändern einer Schlüsselrichtlinie).

Weitere Ressourcen

AWS KMS Berechtigungen

Berichtsspalten

- Status
- Region
- Endpunkt-ARN
- Modell-ARN
- KMS KeyId
- Zeitpunkt der letzten Aktualisierung

Amazon DocumentDB Single-AZ-Cluster

Beschreibung

Überprüft, ob Amazon DocumentDB-Cluster als Single-AZ konfiguriert sind.

Die Ausführung von Amazon DocumentDB DocumentDB-Workloads in einer Single-AZ-Architektur reicht für hochkritische Workloads nicht aus, und es kann bis zu 10 Minuten dauern, bis die Wiederherstellung nach einem Komponentenausfall abgeschlossen ist. Kunden sollten Replikat-Instances in zusätzlichen Availability Zones bereitstellen, um die Verfügbarkeit bei Wartungsarbeiten, Instance-Ausfällen, Komponentenausfällen oder Verfügbarkeitszonenausfällen sicherzustellen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden automatisch ein- oder mehrmals täglich aktualisiert, und Aktualisierungsanforderungen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c15vnddn2x`

Warnungskriterien

Gelb: Der Amazon DocumentDB-Cluster hat Instances in weniger als drei Availability Zones.

Grün: Der Amazon DocumentDB-Cluster hat Instances in drei Availability Zones.

Empfohlene Aktion

Wenn Ihre Anwendung eine hohe Verfügbarkeit erfordert, ändern Sie Ihre DB-Instance, um Multi-AZ mithilfe von Replikat-Instances zu aktivieren. Siehe Amazon DocumentDB Hochverfügbarkeit und Replikation

Weitere Ressourcen

Grundlegendes zur Amazon DocumentDB-Cluster-Fehlertoleranz

Regionen und Availability Zones

Berichtsspalten

- Status
- Region
- Availability Zone
- DB Cluster Identifier (DB-Cluster-ID)
- DB-Cluster-ARN
- Zeitpunkt der letzten Aktualisierung

Wiederherstellung von Amazon DynamoDB P oint-in-time

Beschreibung

Prüft, ob die zeitpunktbezogene Wiederherstellung für Ihre Amazon-DynamoDB-Tabellen aktiviert ist.

Mit der zeitpunktbezogenen Wiederherstellung schützen Sie Ihre DynamoDB-Tabellen vor versehentlichen Schreib- und Löschoperationen. Mit der zeitpunktbezogenen Wiederherstellung müssen Sie sich keine Gedanken über das Erstellen, Warten oder Planen von On-Demand-Backups machen. Mit der zeitpunktbezogenen Wiederherstellung können Sie Tabellen in den Zustand eines beliebigen Zeitpunkts innerhalb der vergangenen 35 Tage wiederherstellen. DynamoDB verwaltet inkrementelle Backups Ihrer Tabelle.

Weitere Informationen finden Sie unter oint-in-time P-Wiederherstellung für DynamoDB.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz138
```

Quelle

```
AWS Config Managed Rule: dynamodb-pitr-enabled
```

Warnungskriterien

Gelb: Die oint-in-time P-Wiederherstellung ist für Ihre DynamoDB-Tabellen nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die point-in-time Wiederherstellung in Amazon DynamoDB, um Ihre Tabellendaten kontinuierlich zu sichern.

Weitere Informationen finden Sie unter oint-in-time P-Wiederherstellung: So funktioniert's.

Weitere Ressourcen

oint-in-time P-Wiederherstellung für DynamoDB

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-DynamoDB-Tabelle ist nicht im Backup-Plan enthalten

Beschreibung

Prüft, ob Amazon DynamoDB-Tabellen Teil eines AWS Backup Plans sind.

AWS Backup stellt inkrementelle Backups für DynamoDB-Tabellen bereit, die die seit der letzten Sicherung vorgenommenen Änderungen aufzeichnen. Die Aufnahme von DynamoDB-Tabellen in einen AWS Backup Plan trägt dazu bei, Ihre Daten vor versehentlichen Datenverlusten zu schützen und den Backup-Prozess zu automatisieren. Dies bietet eine zuverlässige und skalierbare Backup-Lösung für Ihre DynamoDB-Tabellen und trägt dazu bei, dass Ihre wertvollen Daten geschützt sind und bei Bedarf wiederhergestellt werden können.

Weitere Informationen finden Sie unter Erstellen von Backups von DynamoDB-Tabellen mit AWS Backup

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz107`

Quelle

`AWS Config Managed Rule: dynamodb-in-backup-plan`

Warnungskriterien

Gelb: Die Amazon DynamoDB-Tabelle ist nicht im AWS Backup Plan enthalten.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre Amazon DynamoDB-Tabellen Teil eines AWS Backup Plans sind.

Weitere Ressourcen

Geplante Backups

Was ist? AWS Backup

Erstellen von Backup-Plänen mit der AWS-Backup-Konsole

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EBS ist nicht im AWS Backup Plan enthalten

Beschreibung

Prüft, ob Amazon EBS-Volumes in den Backup-Plänen für AWS Backup vorhanden sind.

Nehmen Sie Amazon EBS-Volumes in einen AWS Backup Plan auf, um regelmäßige Backups der auf diesen Volumes gespeicherten Daten zu automatisieren. Dies schützt Sie vor einem möglichen Datenverlust, erleichtert die Datenverwaltung und ermöglicht bei Bedarf die Wiederherstellung von Daten. Ein Backup-Plan trägt dazu bei, dass Ihre Daten sicher sind und dass Sie in der Lage sind, die Ziele für Wiederherstellungszeit und -punkte (Recovery Time and Point Objectives, RTO/RPO) für Ihre Anwendung und Services einzuhalten.

Weitere Informationen finden Sie unter Erstellen eines Sicherungsplans.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz106`

Quelle

`AWS Config Managed Rule: ebs-in-backup-plan`

Warnungskriterien

Gelb: Das Amazon EBS-Volumen ist nicht im AWS Backup Plan enthalten.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre Amazon EBS-Volumes Teil eines AWS Backup Plans sind.

Weitere Ressourcen

Erstellen von Backup-Plänen mithilfe der Konsole AWS Backup

Was ist AWS Backup?

Erste Schritte, Schritt 3: Erstellen einer geplanten Sicherung

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EBS-Snapshots

Beschreibung

Prüft das Alter der Snapshots für Ihre Amazon Elastic Block Store (Amazon EBS) Volumes (entweder verfügbar oder in Verwendung).

Auch wenn Amazon EBS-Volumes repliziert werden, kann es zu Ausfällen kommen. Snapshots werden auf Amazon Simple Storage Service (Amazon S3) gespeichert, um sie dauerhaft zu speichern und point-in-time wiederherzustellen.

Prüf-ID

`H7IgTzjTYb`

Warnungskriterien

- Gelb: Der neueste Volume-Snapshot ist zwischen 7 und 30 Tage alt.
- Rot: Der neueste Volume-Snapshot ist mehr als 30 Tage alt.
- Rot: Das Volume hat keinen Snapshot.

Empfohlene Aktion

Erstellen Sie wöchentliche oder monatliche Schnappschüsse Ihrer Volumes. Weitere Informationen finden Sie unter Erstellen von Amazon-EBS-Snapshots.

Weitere Ressourcen

Amazon Elastic Block Store (Amazon EBS)

Berichtsspalten

- Status
- Region
- Volume-ID
- Volume-Name
- Snapshot-ID
- Snapshot-Name
- Snapshot-Alter
- Anhang des Volumes
- Grund

Bei Amazon EC2 Auto Scaling ist die ELB-Zustandsprüfung nicht aktiviert

Beschreibung

Prüft, ob Ihre Amazon-EC2-Auto-Scaling-Gruppen, die einem Classic Load Balancer zugeordnet sind, Elastic-Load-Balancing-Zustandsprüfungen verwenden. Die Standardzustandsprüfungen für eine Auto-Scaling-Gruppe sind ausschließlich Amazon-EC2-Zustandsprüfungen. Wenn eine Instance diese Zustandsprüfungen nicht besteht, wird sie als fehlerhaft markiert und beendet. Amazon EC2 Auto Scaling startet eine neue Ersatz-Instance. Die Elastic-Load-Balancing-Zustandsprüfung überwacht regelmäßig Amazon-EC2-Instances, um fehlerhafte Instances zu erkennen und zu beenden und dann neue Instances zu starten.

Weitere Informationen finden Sie unter Elastic Load Balancing Health Checks hinzufügen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz104
```

Quelle

`AWS Config Managed Rule: autoscaling-group-elb-healthcheck-required`

Warnungskriterien

Gelb: Amazon-EC2-Auto-Scaling-Gruppe ist an einen Classic Load Balancer angefügt, für den Elastic-Load-Balancing-Zustandsprüfungen nicht aktiviert sind.

Empfohlene Aktion

Vergewissern Sie sich, dass Ihre Auto-Scaling-Gruppen, die einem Classic Load Balancer zugeordnet sind, Elastic-Load-Balancing-Zustandsprüfungen verwenden.

Elastic-Load-Balancing-Zustandsprüfungen melden, ob der Load Balancer fehlerfrei ist und für die Bearbeitung von Anfragen verfügbar ist. So wird eine Hochverfügbarkeit Ihrer Anwendung gewährleistet.

Weitere Informationen finden Sie unter Hinzufügen von Zustandsprüfungen für Elastic Load Balancing zu einer Auto-Scaling-Gruppe.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Für Amazon-EC2-Auto-Scaling-Gruppe ist Kapazitätsausgleich aktiviert

Beschreibung

Prüft, ob der Kapazitätsausgleich für Amazon-EC2-Auto-Scaling-Gruppen aktiviert ist, die mehrere Instance-Typen verwenden.

Durch die Konfiguration von Amazon-EC2-Auto-Scaling-Gruppen mit Kapazitätsausgleich wird sichergestellt, dass Amazon-EC2-Instances unabhängig von Instance-Typen und Kaufoptionen gleichmäßig auf die Availability Zones verteilt werden. Dazu wird eine der Gruppe

zugeordnete Ziel-Nachverfolgungsrichtlinie verwendet, z. B. für die CPU-Nutzung oder den Netzwerkdatenverkehr.

Weitere Informationen finden Sie unter Auto-Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`AWS Config c18d2gz103`

Quelle

AWS Config Verwaltete Regel: autoscaling-capacity-rebalancing

Warnungskriterien

Gelb: Für die Amazon-EC2-Auto-Scaling-Gruppe ist der Kapazitätsausgleich nicht aktiviert.

Empfohlene Aktion

Stellen Sie sicher, dass der Kapazitätsausgleich für Amazon-EC2-Auto-Scaling-Gruppen aktiviert ist, die mehrere Instance-Typen verwenden.

Weitere Informationen finden Sie unter Aktivieren des Kapazitätsausgleichs (Konsole).

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EC2 Auto Scaling wird nicht in mehreren Availability Zones bereitgestellt oder erreicht nicht die Mindestanzahl von Availability Zones

Beschreibung

Prüft, ob die Amazon-EC2-Auto-Scaling-Gruppe in mehreren Availability Zones bereitgestellt wird oder ob die angegebene Mindestanzahl von Availability Zones eingehalten wird. Stellen Sie Amazon-EC2-Instances in mehreren Availability Zones bereit, um Hochverfügbarkeit sicherzustellen.

Sie können die Mindestanzahl von Availability Zones mithilfe des AvailibilityZones Parameters min in Ihren AWS Config Regeln anpassen.

Weitere Informationen finden Sie unter Auto-Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen.

Prüf-ID

```
c18d2gz101
```

Quelle

```
AWS Config Managed Rule: autoscaling-multiple-az
```

Warnungskriterien

Rot: Für die Amazon-EC2-Auto-Scaling-Gruppe sind nicht mehrere Availability Zones konfiguriert oder sie erfüllt nicht die angegebene Mindestanzahl an Availability Zones.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre Amazon-EC2-Auto-Scaling-Gruppe mit mehreren Availability Zones konfiguriert ist. Stellen Sie Amazon-EC2-Instances in mehreren Availability Zones bereit, um Hochverfügbarkeit sicherzustellen.

Weitere Ressourcen

Erstellen einer Auto-Scaling-Gruppe mithilfe einer Startvorlage

Erstellen einer Auto-Scaling-Gruppe mithilfe einer Startkonfiguration

Berichtsspalten

- Status
- Region

- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EC2 Availability Zone Balance

Beschreibung

Prüft die Verteilung von Amazon Elastic Compute Cloud (Amazon EC2) Instances über Availability Zones in einer Region.

Availability Zones sind eigenständige Standorte, die von Ausfällen in anderen Availability Zones isoliert sind. Dies ermöglicht eine kostengünstige Netzwerkkonnektivität mit geringer Latenz zwischen Availability Zones in derselben Region. Indem Sie Instances in mehreren Availability Zones in derselben Region starten, können Sie Ihre Anwendungen vor einem einzelnen Ausfallpunkt schützen.

Prüf-ID

`wuy7G1zxql`

Warnungskriterien

- Gelb: Die Region hat Instances in mehreren Zonen, aber die Verteilung ist ungleichmäßig (der Unterschied zwischen der höchsten und niedrigsten Anzahl von Instances in genutzten Availability Zones ist größer als 20 %).
- Rot: Die Region hat nur Instances in einer einzelnen Availability Zone.

Empfohlene Aktion

Verteilen Sie Ihre Amazon-EC2-Instances gleichmäßig auf mehrere Availability Zones. Sie können dies tun, indem Sie Instances manuell oder automatisch mit Auto Scaling starten. Weitere Informationen finden Sie unter Starten Ihrer Instance und Load Balance Your Auto Scaling Group (Load Balancing Ihrer Auto-Scaling-Gruppe).

Weitere Ressourcen

Benutzerhandbuch für Amazon EC2 Auto Scaling

Berichtsspalten

- Status

- Region
- Zone-A-Instances
- Zone-B-Instances
- Zone-C-Instances
- Zone-E-Instances
- Zone-F-Instances
- Grund

Detaillierte Amazon-EC2-Überwachung nicht aktiviert

Beschreibung

Prüft, ob für Ihre Amazon-EC2-Instances eine detaillierte Überwachung aktiviert ist.

Die detaillierte Überwachung von Amazon EC2 bietet häufigere Metriken, die in Intervallen von einer Minute veröffentlicht werden, statt den Fünf-Minuten-Intervallen, die in der Amazon-EC2-Basisüberwachung verwendet werden. Durch das Aktvieren einer detaillierten Überwachung für Amazon EC2 können Sie Ihre Amazon-EC2-Ressourcen besser verwalten, damit Sie Trends finden und schneller Maßnahmen ergreifen können.

Weitere Informationen finden Sie unter Grundlegende Überwachung und detaillierte Überwachung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
AWS Config c18d2gz144
```

Quelle

AWS Config Verwaltete Regel: ec2-instance-detailed-monitoring-enabled

Warnungskriterien

Gelb: Die detaillierte Überwachung ist für Amazon-EC2-Instances nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die detaillierte Überwachung für Ihre Amazon EC2-Instances, um die Häufigkeit zu erhöhen, mit der Amazon EC2-Metrikdaten an Amazon veröffentlicht werden CloudWatch (von Intervallen von 5 bis 1 Minute).

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon ECS AWS Logs-Treiber im Blockierungsmodus

Beschreibung

Sucht nach Amazon ECS-Aufgabendefinitionen, die mit dem AWS Log-Logging-Treiber im Blockierungsmodus konfiguriert sind. Ein im Blockierungsmodus konfigurierter Treiber gefährdet die Systemverfügbarkeit.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden automatisch ein- oder mehrmals täglich aktualisiert, und Aktualisierungsanforderungen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dvkm4z6b`

Warnungskriterien

Gelb: Der Konfigurationsparametermodus für die AWSlogs-Treiberprotokollierung ist auf Blockieren gesetzt oder fehlt. Ein fehlender Modusparameter weist auf eine standardmäßige Blockierungskonfiguration hin.

Grün: Die Amazon ECS-Aufgabendefinition verwendet den awslogs-Treiber nicht oder der awslogs-Treiber ist im blockierungsfreien Modus konfiguriert.

Empfohlene Aktion

Um das Verfügbarkeitsrisiko zu minimieren, sollten Sie erwägen, die Konfiguration des AWS Protokolltreibers für die Aufgabendefinition von blockierend auf nicht blockierend zu ändern. Im nicht blockierenden Modus müssen Sie einen Wert für den Parameter festlegen. max-buffer-size Weitere Informationen und Anleitungen zu Konfigurationsparametern finden Sie unter. Weitere Informationen finden Sie unter Verhinderung von Protokollverlusten im Modus „Blockierung“ im Protokolltreiber des Containers „ AWS Logs“

Weitere Ressourcen

Verwenden des AWS Protokolltreibers

Auswahl von Optionen zur Protokollierung von Containern, um Gegendruck zu vermeiden

Verhinderung von Protokollverlusten im Blockierungsmodus des AWS Logs-Container-Protokolltreibers

Berichtsspalten

- Status
- Region
- Aufgabendefinition ARN
- Namen der Container-Definitionen
- Zeitpunkt der letzten Aktualisierung

Amazon-ECS-Service mit einer einzigen Availability Zone

Beschreibung

Prüft, ob Ihre Servicekonfiguration eine einzige Availability Zone (AZ) verwendet.

Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Dies unterstützt kostengünstige Netzwerkkonnektivität mit geringer Latenz zwischen Availability Zones in derselben AWS-Region. Indem Sie Instances in mehreren Availability Zones in derselben Region starten, können Sie Ihre Anwendungen vor einem einzelnen Ausfallpunkt schützen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1z7dfpz01`

Warnungskriterien

- Gelb: Ein Amazon-ECS-Service führt alle Aufgaben in einer einzigen AZ aus.
- Grün: Ein Amazon-ECS-Service führt Aufgaben in mindestens zwei verschiedenen AZs aus.

Empfohlene Aktion

Erstellen Sie mindestens eine weitere Aufgabe für den Service in einer anderen AZ.

Weitere Ressourcen

Kapazität und Verfügbarkeit von Amazon ECS

Berichtsspalten

- Status
- Region
- ECS-Clustername/ECS-Servicename
- Anzahl der Availability Zones
- Zeitpunkt der letzten Aktualisierung

Amazon-ECS-Multi-AZ-Platzierungsstrategie

Beschreibung

Überprüft, ob Ihr Amazon-ECS-Service die auf der Availability Zone (AZ) basierende Spread-Platzierungsstrategie verwendet. Diese Strategie verteilt Aufgaben auf die Availability Zones in derselben Weise AWS-Region und kann dazu beitragen, Ihre Anwendungen vor einem einzelnen Ausfallpunkt zu schützen.

Für Aufgaben, die als Teil eines Amazon-ECS-Service ausgeführt werden, ist „Spread“ die Standard-Aufgabenplatzierungsstrategie.

Mit dieser Prüfung wird auch überprüft, ob Spread die erste oder die einzige Strategie in Ihrer Liste der aktivierten Platzierungsstrategien ist.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1z7dfpz02`

Warnungskriterien

- Gelb: Die Verteilung (Spread) nach Availability Zone ist deaktiviert oder steht nicht an erster Stelle in Ihrer Liste der aktivierten Platzierungsstrategien für Ihren Amazon-ECS-Service.
- Grün: Die Verteilung (Spread) nach Availability Zone steht nicht an erster Stelle in Ihrer Liste der aktivierten Platzierungsstrategien oder ist die einzige für Ihren Amazon-ECS-Service aktivierte Platzierungsstrategie.

Empfohlene Aktion

Aktivieren Sie die Spread-Aufgabenplatzierungsstrategie, um Aufgaben auf mehrere AZs zu verteilen. Stellen Sie sicher, dass die Verteilung (Spread) nach Availability Zone die erste Strategie für alle aktivierten Aufgabenplatzierungsstrategien oder die einzige verwendete

Strategie ist. Wenn Sie sich dafür entscheiden, die AZ-Platzierung zu verwalten, können Sie einen gespiegelten Service in einer anderen Availability Zone verwenden, um diese Risiken zu minimieren.

Weitere Ressourcen

Strategien für die Platzierung von Aufgaben in Amazon ECS

Berichtsspalten

- Status
- Region
- ECS-Clustername/ECS-Servicename
- Spread-Aufgabenplatzierungsstrategie aktiviert und korrekt angewendet
- Zeitpunkt der letzten Aktualisierung

Amazon EFS – Keine Mount-Ziel-Redundanz

Beschreibung

Prüft, ob Mount-Ziele in mehreren Availability Zones für ein Amazon-EFS-Dateisystem vorhanden sind.

Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Durch die Erstellung von Mount-Zielen in mehreren geografisch getrennten Availability Zones innerhalb einer AWS-Region können Sie ein Höchstmaß an Verfügbarkeit und Beständigkeit für Ihre Amazon-EFS-Dateisysteme erreichen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c1dfprch01
```

Warnungskriterien

- Gelb: Das Dateisystem hat 1 Mount-Ziel, das in einer einzelnen Availability Zone erstellt wurde.

  Grün: Das Dateisystem hat mindestens 2 Mount-Ziele, die in mehreren Availability Zones erstellt wurden.

Empfohlene Aktion

Für EFS-Dateisysteme, die One-Zone-Speicherklassen verwenden, empfehlen wir, neue Dateisysteme zu erstellen, die Standardspeicherklassen verwenden, indem eine Sicherung in einem neuen Dateisystem wiederhergestellt wird. Erstellen Sie dann Mount-Ziele in mehreren Availability Zones.

Für EFS-Dateisysteme, die Standardspeicherklassen verwenden, empfehlen wir, Mount-Ziele in mehreren Availability Zones zu erstellen.

Weitere Ressourcen

- Verwalten von Mount-Zielen mit der Amazon-EFS-Konsole
- Amazon-EFS-Kontingente und -Limits

Berichtsspalten

- Status
- Region
- EFS-Dateisystem-ID
- Anzahl der Mounting-Ziele
- Anzahl der AZs
- Zeitpunkt der letzten Aktualisierung

Amazon EFS ist nicht im AWS Backup Plan enthalten

Beschreibung

Überprüft, ob Amazon EFS-Dateisysteme in Backup-Plänen mit enthalten sind AWS Backup.

AWS Backup ist ein einheitlicher Backup-Service, der die Erstellung, Migration, Wiederherstellung und Löschung von Backups vereinfacht und gleichzeitig verbesserte Berichte und Prüfungen bietet.

Weitere Informationen finden Sie unter Sichern Ihrer Amazon-EFS-Dateisysteme.

Prüf-ID

`c18d2gz117`

Quelle

`AWS Config Managed Rule: EFS_IN_BACKUP_PLAN`

Warnungskriterien

Rot: Amazon EFS sind nicht im AWS Backup Plan enthalten.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre Amazon EFS-Dateisysteme in Ihrem AWS Backup Plan enthalten sind, um sich vor versehentlichem Datenverlust oder Datenbeschädigung zu schützen.

Weitere Ressourcen

Sichern Ihrer Amazon-EFS-Dateisysteme

Amazon EFS Backup and Restore mit AWS Backup.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon ElastiCache Multi-AZ-Cluster

Beschreibung

Sucht nach ElastiCache Clustern, die in einer einzigen Availability Zone (AZ) bereitgestellt werden. Diese Prüfung warnt Sie, wenn Multi-AZ in einem Cluster inaktiv ist.

Bereitstellungen in mehreren AZs verbessern die ElastiCache Cluster-Verfügbarkeit, indem asynchron auf schreibgeschützte Replikate in einer anderen AZ repliziert wird. Wenn eine geplante Clusterwartung stattfindet oder ein primärer Knoten nicht verfügbar ist, wird ein Replikat

ElastiCache automatisch zum primären Knoten hochgestuft. Dieses Failover ermöglicht die Wiederaufnahme von Cluster-Schreibvorgängen, ohne dass ein Administrator eingreifen muss.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`ECHdfsQ402`

Warnungskriterien

- Grün: Multi-AZ ist im Cluster aktiv.
- Gelb: Multi-AZ ist im Cluster inaktiv.

Empfohlene Aktion

Erstellen Sie mindestens ein Replikat pro Shard in einer AZ, die sich von der primären unterscheidet.

Weitere Ressourcen

Weitere Informationen finden Sie unter Minimierung von Ausfallzeiten in ElastiCache für Redis mit Multi-AZ.

Berichtsspalten

- Status
- Region
- Cluster-Name
- Zeitpunkt der letzten Aktualisierung

Automatische Backup ElastiCache von Amazon Redis-Clustern

Beschreibung

Überprüft, ob für die Amazon ElastiCache for Redis-Cluster die automatische Sicherung aktiviert ist und ob die Aufbewahrungsfrist für Snapshots über dem angegebenen Standardlimit oder dem

Standardlimit von 15 Tagen liegt. Wenn automatische Backups aktiviert sind, ElastiCache erstellt täglich ein Backup des Clusters.

Sie können das gewünschte Aufbewahrungslimit für Snapshots mithilfe der RetentionPeriodSnapshot-Parameter Ihrer AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Backup und Wiederherstellung ElastiCache für Redis.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz178`

Quelle

`AWS Config Managed Rule: elasticache-redis-cluster-automatic-backup-check`

Warnungskriterien

Rot: ElastiCache Bei Amazon for Redis-Clustern ist kein automatisches Backup aktiviert oder die Aufbewahrungsfrist für Snapshots liegt unter dem Grenzwert.

Empfohlene Aktion

Stellen Sie sicher, dass bei Amazon ElastiCache for Redis-Clustern die automatische Sicherung aktiviert ist und dass die Aufbewahrungsfrist für Snapshots über dem angegebenen Standardlimit von 15 Tagen liegt. Automatische Backups schützen vor Datenverlust. Bei einem Ausfall können Sie einen neuen Cluster erstellen, indem Sie Ihre Daten aus der aktuellen Sicherung wiederherstellen.

Weitere Informationen finden Sie unter Backup und Wiederherstellung ElastiCache für Redis.

Weitere Ressourcen

Weitere Informationen finden Sie unter Planen automatischer Sicherungen.

Berichtsspalten

- Status
- Region
- Cluster-Name
- Zeitpunkt der letzten Aktualisierung

Amazon-MemoryDB-Multi-AZ-Cluster

Beschreibung

Prüft auf MemoryDB-Cluster, die in einer einzigen Availability Zone (AZ) bereitgestellt werden. Diese Prüfung warnt Sie, wenn Multi-AZ in einem Cluster inaktiv ist.

Bereitstellungen in mehreren AZs verbessern die MemoryDB-Clusterverfügbarkeit, indem sie asynchron auf schreibgeschützte Replikate in einer anderen AZ repliziert werden. Wenn eine geplante Cluster-Wartung stattfindet oder ein Primärknoten nicht verfügbar ist, stuft MemoryDB ein Replikat automatisch zum Primärknoten herauf. Dieses Failover ermöglicht die Wiederaufnahme von Cluster-Schreibvorgängen, ohne dass ein Administrator eingreifen muss.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`MDBdfsQ401`

Warnungskriterien

- Grün: Multi-AZ ist im Cluster aktiv.
- Gelb: Multi-AZ ist im Cluster inaktiv.

Empfohlene Aktion

Erstellen Sie mindestens ein Replikat pro Shard in einer AZ, die sich von der primären unterscheidet.

Weitere Ressourcen

Weitere Informationen finden Sie unter Minimieren von Ausfallzeiten in MemoryDB mit Multi-AZ.

Berichtsspalten

- Status
- Region
- Cluster-Name
- Zeitpunkt der letzten Aktualisierung

Amazon-MSK-Broker, die zu viele Partitionen hosten

Beschreibung

Überprüft, ob den Brokern eines MSK-Clusters (Managed Streaming for Kafka) nicht mehr als die empfohlene Anzahl von Partitionen zugewiesen wurde.

Prüf-ID

`Cmsvnj8vf1`

Warnungskriterien

- Rot: Ihr MSK-Broker hat 100 % des empfohlenen maximalen Partitionslimits erreicht oder überschritten
- Gelb: Ihr MSK-Broker hat 80 % des empfohlenen maximalen Partitionslimits erreicht

Empfohlene Aktion

Folgen Sie den von MSK empfohlenen bewährten Methoden, um Ihren MSK-Cluster zu skalieren oder ungenutzte Partitionen zu löschen.

Weitere Ressourcen

- Auswahl der richtigen Größe für Ihren Cluster

Berichtsspalten

- Status
- Region
- Cluster-ARN
- Broker-ID
- Anzahl der Partitionen

Amazon OpenSearch Service-Domains mit weniger als drei Datenknoten

Beschreibung

Überprüft, ob Amazon OpenSearch Service-Domains mit mindestens drei Datenknoten konfiguriert sind und ZoneAwarenessEnabled ist wahr. ZoneAwarenessEnabled Wenn diese Option aktiviert ist, stellt Amazon OpenSearch Service sicher, dass jeder primäre Shard und sein entsprechendes Replikat verschiedenen Availability Zones zugewiesen werden.

Weitere Informationen finden Sie unter Konfiguration einer Multi-AZ-Domain in Amazon OpenSearch Service.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz183`

Quelle

`AWS Config Managed Rule: opensearch-data-node-fault-tolerance`

Warnungskriterien

Gelb: Amazon OpenSearch Service-Domains sind mit weniger als drei Datenknoten konfiguriert.

Empfohlene Aktion

Stellen Sie sicher, dass Amazon OpenSearch Service-Domains mit mindestens drei Datenknoten konfiguriert sind. Konfigurieren Sie eine Multi-AZ-Domain, um die Verfügbarkeit des Amazon OpenSearch Service-Clusters zu verbessern, indem Sie Knoten zuweisen und Daten über drei Availability Zones innerhalb derselben Region replizieren. Dies verhindert Datenverluste und minimiert Ausfallzeiten im Falle eines Knoten- und Rechenzentrumsausfalls.

Weitere Informationen finden Sie unter Erhöhen Sie die Verfügbarkeit von Amazon OpenSearch Service durch Bereitstellung in drei Availability Zones.

Weitere Ressourcen

- Erhöhen Sie die Verfügbarkeit von Amazon OpenSearch Service durch Bereitstellung in drei Availability Zones

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-Backups

Beschreibung

Prüft auf automatische Backups von Amazon RDS DB-Instances.

Standardmäßig sind Backups mit einer Aufbewahrungsfrist von einem Tag aktiviert. Backups reduzieren das Risiko eines unerwarteten Datenverlusts und ermöglichen eine point-in-time Wiederherstellung.

Prüf-ID

`opQPADkZvH`

Warnungskriterien

Rot: Die Aufbewahrungsfrist für Backups einer DB-Instance ist auf 0 Tage festgelegt.

Empfohlene Aktion

Legen Sie den Aufbewahrungszeitraum für das automatische DB-Instance-Backup entsprechend den Anforderungen Ihrer Anwendung auf 1 bis 35 Tage fest. Weitere Informationen finden Sie unter Arbeiten mit automatischen Sicherungen.

Weitere Ressourcen

Erste Schritte mit Amazon RDS

Berichtsspalten

- Status

- Region/AZ
- DB-Instance
- VPC-ID
- Aufbewahrungszeitraum für Backups

Amazon RDS-DB-Cluster haben eine DB-Instance

Beschreibung

Fügen Sie dem DB-Cluster mindestens eine weitere DB-Instance hinzu, um die Verfügbarkeit und Leistung zu verbessern.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt011`

Warnungskriterien

Gelb: DB-Cluster haben nur eine DB-Instance.

Empfohlene Aktion

Fügen Sie dem DB-Cluster eine Reader-DB-Instance hinzu.

Weitere Ressourcen

In der aktuellen Konfiguration wird eine DB-Instance sowohl für Lese- als auch für Schreibvorgänge verwendet. Sie können eine weitere DB-Instance hinzufügen, um die Umverteilung von Lesevorgängen und eine Failover-Option zu ermöglichen.

Weitere Informationen finden Sie unter Hochverfügbarkeit für Amazon Aurora.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Motors
- DB-Instance-Klasse
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Cluster mit allen Instances in derselben Availability Zone

Beschreibung

Die DB-Cluster befinden sich derzeit in einer einzigen Availability Zone. Verwenden Sie mehrere Availability Zones, um die Verfügbarkeit zu verbessern.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach

fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt007`

Warnungskriterien

Gelb: DB-Cluster haben alle Instances in derselben Availability Zone.

Empfohlene Aktion

Fügen Sie die DB-Instances mehreren Availability Zones in Ihrem DB-Cluster hinzu.

Weitere Ressourcen

Wir empfehlen, dass Sie die DB-Instances mehreren Availability Zones in einem DB-Cluster hinzufügen. Das Hinzufügen von DB-Instances zu mehreren Availability Zones verbessert die Verfügbarkeit Ihres DB-Clusters.

Weitere Informationen finden Sie unter Hochverfügbarkeit für Amazon Aurora.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Cluster mit allen Reader-Instances in derselben Availability Zone

Beschreibung

Ihr DB-Cluster hat alle DB-Instances in derselben Availability Zone. Wir empfehlen, dass Sie die Reader-Instances auf mehrere Availability Zones in Ihrem DB-Cluster verteilen.

Die Verteilung erhöht die Verfügbarkeit der Datenbank und verbessert die Reaktionszeit, indem die Netzwerklatenz zwischen den Clients und der Datenbank reduziert wird.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt018`

Warnungskriterien

Rot: Bei DB-Clustern befinden sich die Reader-Instances in derselben Availability Zone.

Empfohlene Aktion

Verteilen Sie die Reader-Instances auf mehrere Availability Zones.

Weitere Ressourcen

Availability Zones (AZs) sind Standorte, die sich voneinander unterscheiden, um bei Ausfällen innerhalb der einzelnen AWS Regionen für Isolation zu sorgen. Wir empfehlen, dass Sie die primäre Instance und die Reader-Instances in Ihrem DB-Cluster auf mehrere AZs verteilen, um die Verfügbarkeit Ihres DB-Clusters zu verbessern. Sie können einen Multi-AZ-Cluster mithilfe der

AWS Management Console AWS CLI, oder Amazon RDS-API erstellen, wenn Sie den Cluster erstellen. Sie können den vorhandenen Aurora-Cluster in einen Multi-AZ-Cluster ändern, indem Sie eine neue Reader-Instance hinzufügen und eine andere AZ angeben.

Weitere Informationen finden Sie unter Hochverfügbarkeit für Amazon Aurora.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Erweiterte Überwachung der Amazon-RDS-DB-Instance ist nicht aktiviert

Beschreibung

Prüft, ob für Ihre Amazon-RDS-DB-Instances die erweiterte Überwachung aktiviert wurde.

Die erweiterte Überwachung für Amazon RDS stellt Metriken in Echtzeit für das Betriebssystem (BS) bereit, unter dem Ihre DB-Instance ausgeführt wird. Alle Systemmetriken und Prozessinformationen für Ihre Amazon-RDS-DB-Instances können in der Konsole angezeigt werden. Und Sie können das Dashboard anpassen. Mit erweiterter Überwachung haben Sie nahezu in Echtzeit Einblick in den Betriebsstatus Ihrer Amazon-RDS-Instance, sodass Sie schneller auf betriebliche Probleme reagieren können.

Sie können das gewünschte monitoringInterval mit dem MonitoringInterval-Parameter Ihrer Regeln angeben. AWS Config

Weitere Informationen finden Sie unter Übersicht über „Erweiterte Überwachung“ und Betriebssystemmetriken in „Erweiterte Überwachung“.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz158
```

Quelle

```
AWS Config Managed Rule: rds-enhanced-monitoring-enabled
```

Warnungskriterien

Gelb: Für Ihre Amazon-RDS-DB-Instances ist „Erweiterte Überwachung“ nicht aktiviert oder sie sind nicht mit dem gewünschten Intervall konfiguriert.

Empfohlene Aktion

Aktivieren Sie „Erweiterte Überwachung“ für Ihre Amazon-RDS-DB-Instances, um die Sichtbarkeit des Betriebsstatus Ihrer Amazon-RDS-Instance zu verbessern.

Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Erweitere Überwachung“.

Weitere Ressourcen

Betriebssystemmetriken in „Erweiterte Überwachung“

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Bei Amazon RDS-DB-Instances ist die automatische Speicherskalierung deaktiviert

Beschreibung

Die automatische Skalierung des Amazon RDS-Speichers ist für Ihre DB-Instance nicht aktiviert. Wenn die Datenbank-Arbeitslast zunimmt, skaliert RDS Storage Autoscaling die Speicherkapazität automatisch und ohne Ausfallzeiten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt013`

Warnungskriterien

Rot: Bei DB-Instances ist die automatische Speicherskalierung nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die automatische Skalierung des Amazon RDS-Speichers mit einem angegebenen maximalen Speicherschwellenwert.

Weitere Ressourcen

Die automatische Skalierung des Amazon RDS-Speichers skaliert die Speicherkapazität automatisch ohne Ausfallzeiten, wenn die Datenbank-Arbeitslast zunimmt. Storage Autoscaling überwacht die Speichernutzung und skaliert die Kapazität automatisch, wenn die Nutzung der bereitgestellten Speicherkapazität nahe kommt. Sie können ein maximales Limit für den Speicher angeben, den Amazon RDS der DB-Instance zuweisen kann. Für die automatische

Speicherskalierung fallen keine zusätzlichen Kosten an. Sie zahlen nur für die Amazon RDS-Ressourcen, die Ihrer DB-Instance zugewiesen sind. Wir empfehlen, die automatische Skalierung des Amazon RDS-Speichers zu aktivieren.

Weitere Informationen finden Sie unter Managing capacity automatically with Amazon RDS storage autoscaling (Automatische Kapazitätsverwaltung mit Speicher-Autoscaling).

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Instances, die keine Multi-AZ-Bereitstellung verwenden

Beschreibung

Wir empfehlen Ihnen, die Multi-AZ-Bereitstellung zu verwenden. Die Multi-AZ-Bereitstellungen verbessern die Verfügbarkeit und Dauerhaftigkeit der DB-Instance.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.

Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt019`

Warnungskriterien

Gelb: DB-Instances verwenden keine Multi-AZ-Bereitstellung.

Empfohlene Aktion

Richten Sie Multi-AZ für die betroffenen DB-Instances ein.

Weitere Ressourcen

In einer Amazon RDS Multi-AZ-Bereitstellung erstellt Amazon RDS automatisch eine primäre Datenbank-Instance und repliziert die Daten auf eine Instance in einer anderen Availability Zone. Wenn Amazon RDS einen Fehler erkennt, wechselt Amazon RDS automatisch und ohne manuelles Eingreifen zu einer Standby-Instance.

Weitere Informationen finden Sie unter -Preisgestaltung.

Berichtsspalten

- Status
- Region
- Ressource
- Name der Engine
- Zeitpunkt der letzten Aktualisierung

Amazon RDS DiskQueueDepth

Beschreibung

Überprüft, ob die CloudWatch Metrik DiskQueueDepth zeigt, dass die Anzahl der Schreibvorgänge in der Warteschlange auf den Datenbankspeicher der RDS-Instance ein Niveau erreicht hat, bei dem eine operative Untersuchung vorgeschlagen werden sollte.

Prüf-ID

`Cmsvnj8db3`

Warnungskriterien

- Rot: Die DiskQueueDepth CloudWatch Metrik hat 10 überschritten
- Gelb: Die DiskQueueDepth CloudWatch Metrik ist größer als 5, aber kleiner oder gleich 10
- Grün: Die DiskQueueDepth CloudWatch Metrik ist kleiner oder gleich 5

Empfohlene Aktion

Erwägen Sie die Umstellung auf Instances und Speichervolumes, die die Lese-/Schreibeigenschaften unterstützen.

Berichtsspalten

- Status
- Region
- DB-Instance-ARN
- DiskQueueDepth Metrisch

Amazon RDS FreeStorageSpace

Beschreibung

Überprüft, ob die FreeStorageSpace CloudWatch Metrik für eine RDS-Datenbank-Instance über einen betrieblich angemessenen Schwellenwert gestiegen ist.

Prüf-ID

`Cmsvnj8db2`

Warnungskriterien

- Rot: FreeStorageSpace hat 90% der Gesamtkapazität erreicht/überschritten
- Gelb: FreeStorageSpace liegt zwischen 80 und 90% der Gesamtkapazität
- Grün: FreeStorageSpace ist weniger als 80% der Gesamtkapazität

Empfohlene Aktion

Skalieren Sie den Speicherplatz für die RDS-Datenbank-Instance, deren freier Speicherplatz knapp wird, mithilfe der Amazon RDS Management Console, der Amazon RDS-API oder der AWS-Befehlszeilenschnittstelle.

Berichtsspalten

- Status
- Region
- DB-Instance-ARN
- FreeStorageSpace Metrisch (MB)
- Zugewiesener Speicher der DB-Instance (MB)
- Verwendeter Speicher der DB-Instance in Prozent

Der Amazon RDS-Parameter log_output ist auf Tabelle gesetzt

Beschreibung

Wenn log_output auf TABLE gesetzt ist, wird mehr Speicherplatz verwendet als wenn log_output auf FILE gesetzt ist. Wir empfehlen, den Parameter auf FILE zu setzen, um zu verhindern, dass die Speichergrößenbeschränkung erreicht wird.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt023`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist der Parameter log_output auf TABLE gesetzt.

Empfohlene Aktion

Setzen Sie den Wert des Parameters log_output in Ihren DB-Parametergruppen auf FILE.

Weitere Ressourcen

Weitere Informationen finden Sie unter Logdateien der MySQL-Datenbank.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Die Amazon RDS-Parametereinstellung innodb_default_row_format ist unsicher

Beschreibung

Bei Ihrer DB-Instance tritt ein bekanntes Problem auf: Auf eine Tabelle, die in einer MySQL-Version vor 8.0.26 erstellt wurde und deren row_format auf COMPACT oder REDUNDANT gesetzt ist, kann nicht zugegriffen werden und sie kann nicht wiederhergestellt werden, wenn der Index 767 Byte überschreitet.

Wir empfehlen, den Wert des Parameters innodb_default_row_format auf DYNAMIC zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt036`

Warnungskriterien

Rot: DB-Parametergruppen haben eine unsichere Einstellung für den Parameter innodb_default_row_format.

Empfohlene Aktion

Setzen Sie den Parameter innodb_default_row_format auf DYNAMIC.

Weitere Ressourcen

Wenn eine Tabelle mit einer MySQL-Version unter 8.0.26 erstellt wird und row_format auf COMPACT oder REDUNDANT gesetzt ist, wird die Erstellung von Indizes mit einem key prefix, das kürzer als 767 Byte ist, nicht erzwungen. Nach dem Neustart der Datenbank kann nicht auf diese Tabellen zugegriffen oder sie wiederhergestellt werden.

Weitere Informationen finden Sie unter Änderungen in MySQL 8.0.26 (20.07.2021, Allgemeine Verfügbarkeit) n auf der MySQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region

- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter innodb_flush_log_at_trx_commit ist nicht 1

Beschreibung

Der Wert des Parameters innodb_flush_log_at_trx_commit Ihrer DB-Instance ist kein sicherer Wert. Dieser Parameter steuert die Persistenz von Commit-Operationen auf der Festplatte.

Wir empfehlen, den Parameter innodb_flush_log_at_trx_commit auf 1 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt030`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist innodb_flush_log_at_trx_commit auf einen anderen Wert als 1 gesetzt.

Empfohlene Aktion

Setzen Sie den Parameterwert innodb_flush_log_at_trx_commit auf 1

Weitere Ressourcen

Die Datenbanktransaktion ist dauerhaft, wenn der Protokollpuffer im dauerhaften Speicher gespeichert wird. Das Speichern auf der Festplatte beeinträchtigt jedoch die Leistung. Abhängig vom Wert, der für den Parameter innodb_flush_log_at_trx_commit festgelegt wurde, kann das Verhalten beim Schreiben und Speichern von Protokollen auf die Festplatte variieren.

- Wenn der Parameterwert 1 ist, werden die Protokolle nach jeder festgeschriebenen Transaktion geschrieben und auf der Festplatte gespeichert.
- Wenn der Parameterwert 0 ist, werden die Protokolle einmal pro Sekunde auf die Festplatte geschrieben und gespeichert.
- Wenn der Parameterwert 2 ist, werden die Protokolle geschrieben, nachdem jede Transaktion festgeschrieben und einmal pro Sekunde auf der Festplatte gespeichert wurde. Die Daten werden vom InnoDB-Speicherpuffer in den Cache des Betriebssystems verschoben, der sich ebenfalls im Speicher befindet.

> **Note**
>
> Wenn der Parameterwert nicht 1 ist, garantiert InnoDB keine ACID-Eigenschaften. Die letzten Transaktionen der letzten Sekunde können verloren gehen, wenn die Datenbank abstürzt.

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 1: Leistungsparameter.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters

- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter max_user_connections ist niedrig

Beschreibung

Ihre DB-Instance hat einen niedrigen Wert für die maximale Anzahl gleichzeitiger Verbindungen für jedes Datenbankkonto.

Wir empfehlen, den Parameter max_user_connections auf eine Zahl größer als 5 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt034`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist max_user_connections falsch konfiguriert.

Empfohlene Aktion

Erhöhen Sie den Wert des Parameters max_user_connections auf eine Zahl größer als 5.

Weitere Ressourcen

Die Einstellung max_user_connections steuert die maximale Anzahl gleichzeitiger Verbindungen, die für ein MySQL-Benutzerkonto zulässig sind. Das Erreichen dieses Verbindungslimits führt zu Fehlern bei den Verwaltungsvorgängen der Amazon RDS-Instance, z. B. bei Backups, Patches und Parameteränderungen.

Weitere Informationen finden Sie unter Setting Account Resource Limits auf der MySQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon RDS Multi-AZ

Beschreibung

Prüft auf DB-Instances, die in einer einzigen Availability Zone (AZ) eingesetzt werden.

Multi-AZ-Bereitstellungen verbessern die Datenbankverfügbarkeit durch synchrone Replikation auf eine Standby-Instance in einer anderen Availability Zone. Bei geplanter Datenbankwartung oder dem Ausfall einer DB-Instance oder Availability Zone wechselt Amazon RDS automatisch zum Standby. Dieses Failover ermöglicht eine schnelle Wiederaufnahme des Datenbankbetriebs ohne administrative Eingriffe. Da Amazon RDS keine Multi-AZ-Bereitstellung für Microsoft SQL Server unterstützt, werden bei dieser Prüfung keine SQL-Server-Instances untersucht.

Prüf-ID

`f2iK5R6Dep`

Warnungskriterien

Gelb: Eine DB-Instance wird in einer einzelnen Availability Zone bereitgestellt.

Empfohlene Aktion

Wenn Ihre Anwendung hohe Verfügbarkeit erfordert, ändern Sie Ihre DB-Instance, um die Multi-AZ-Bereitstellung zu ermöglichen. Weitere Informationen finden Sie unter Hohe Verfügbarkeit (Multi-AZ).

Weitere Ressourcen

Regionen und Availability Zones

Berichtsspalten

- Status
- Region/AZ
- DB-Instance
- VPC-ID
- Multi-AZ

Amazon RDS nicht im AWS Backup Plan

Beschreibung

Überprüft, ob Ihre Amazon-RDS-DB-Instances in einem Backup-Plan in AWS Backup enthalten sind.

AWS Backup ist ein vollständig verwalteter Backup-Service, der es einfach macht, die Sicherung von Daten über verschiedene AWS Dienste hinweg zu zentralisieren und zu automatisieren.

Die Aufnahme Ihrer Amazon-RDS-DB-Instance in einen Backup-Plan ist wichtig für die Einhaltung gesetzlicher Vorschriften, die Notfallwiederherstellung, die Unternehmensrichtlinien für den Datenschutz und die Ziele der Geschäftskontinuität.

Weitere Informationen finden Sie unter Was ist AWS Backup?.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz159`

Quelle

`AWS Config Managed Rule: rds-in-backup-plan`

Warnungskriterien

Gelb: Eine Amazon RDS-DB-Instance ist nicht in einem Backup-Plan mit enthalten AWS Backup.

Empfohlene Aktion

Nehmen Sie Ihre Amazon RDS-DB-Instances in einen Backup-Plan mit auf AWS Backup.

Weitere Informationen finden Sie unter Amazon-RDS-Backup und -Wiederherstellung mit AWS Backup.

Weitere Ressourcen

Zuweisen von Ressourcen zu einem Sicherungsplan

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon RDS Read Replicas sind im schreibbaren Modus geöffnet

Beschreibung

Ihre DB-Instance verfügt über eine Read Replica im Schreibmodus, der Updates von Clients ermöglicht.

Wir empfehlen, den Parameter read_only auf TrueIfReplica zu setzen, damit sich die Read Replicas nicht im schreibbaren Modus befinden.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt035`

Warnungskriterien

Gelb: DB-Parametergruppen aktivieren den Schreibmodus für die Read Replicas.

Empfohlene Aktion

Setzen Sie den Wert des read_only-Parameters auf Replica. TrueIf

Weitere Ressourcen

Der Parameter read_only steuert die Schreibberechtigung der Clients für eine Datenbankinstanz. Der Standardwert für diesen Parameter ist TrueIf Replica. Für eine Replikatinstanz setzt TrueIfReplica den read_only-Wert auf ON (1) und deaktiviert jegliche Schreibaktivität der Clients.

Für eine Master-/Writer-Instanz setzt TrueIfReplica den Wert auf OFF (0) und aktiviert die Schreibaktivität der Clients für die Instanz. Wenn die Read Replica im schreibbaren Modus geöffnet wird, können die in dieser Instanz gespeicherten Daten von der primären Instanz abweichen, was zu Replikationsfehlern führt.

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 2: Parameter im Zusammenhang mit der Replikation auf der MySQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Automatisierte Amazon RDS-Ressourcen-Backups sind deaktiviert

Beschreibung

Automatisierte Backups sind auf Ihren DB-Ressourcen deaktiviert. Automatisierte Backups ermöglichen die point-in-time Wiederherstellung Ihrer DB-Instance.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die

Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt001`

Warnungskriterien

Rot: Für Amazon RDS-Ressourcen sind automatische Backups nicht aktiviert

Empfohlene Aktion

Aktivieren Sie automatische Backups mit einer Aufbewahrungsfrist von bis zu 14 Tagen.

Weitere Ressourcen

Automatisierte Backups ermöglichen die point-in-time Wiederherstellung Ihrer DB-Instances. Wir empfehlen, automatische Backups zu aktivieren. Wenn Sie automatische Backups für eine DB-Instance aktivieren, führt Amazon RDS täglich während Ihres bevorzugten Backup-Fensters automatisch eine vollständige Sicherung Ihrer Daten durch. Das Backup erfasst Transaktionsprotokolle, wenn Aktualisierungen an Ihrer DB-Instance vorgenommen werden. Sie erhalten Backup-Speicher bis zur Speichergröße Ihrer DB-Instance ohne zusätzliche Kosten.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Aktivierung automatisierter Backups
- Entmystifizierung der Amazon RDS-Backup-Speicherkosten

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter sync_binlog ist ausgeschaltet

Beschreibung

Die Synchronisation des Binärprotokolls mit der Festplatte wird nicht erzwungen, bevor die Transaktions-Commits in Ihrer DB-Instance bestätigt wurden.

Wir empfehlen, den Wert des sync_binlog-Parameters auf 1 zu setzen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt031`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist die synchrone binäre Protokollierung deaktiviert.

Empfohlene Aktion

Setzen Sie den Parameter sync_binlog auf 1.

Weitere Ressourcen

Der Parameter sync_binlog steuert, wie MySQL das Binärprotokoll auf die Festplatte überträgt. Wenn der Wert dieses Parameters auf 1 gesetzt ist, wird die Synchronisation des Binärprotokolls mit der Festplatte aktiviert, bevor Transaktionen festgeschrieben werden. Wenn der Wert dieses Parameters auf 0 gesetzt ist, wird die Synchronisation des Binärprotokolls mit der Festplatte deaktiviert. Normalerweise hängt der MySQL-Server davon ab, dass das Betriebssystem das Binärprotokoll regelmäßig auf die Festplatte überträgt, ähnlich wie bei anderen Dateien. Der Wert des sync_binlog-Parameters, der auf 0 gesetzt ist, kann die Leistung verbessern. Bei einem Stromausfall oder einem Betriebssystemabsturz verliert der Server jedoch alle festgeschriebenen Transaktionen, die nicht mit den Binärprotokollen synchronisiert wurden.

Weitere Informationen finden Sie unter Bewährte Methoden für die Konfiguration von Parametern für Amazon RDS for MySQL, Teil 2: Parameter im Zusammenhang mit der Replikation.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Für den RDS-DB-Cluster ist keine Multi-AZ-Replikation aktiviert

Beschreibung

Prüft, ob in Ihren Amazon-RDS-DB-Clustern die Multi-AZ-Replikation aktiviert ist.

Ein Multi-AZ-DB-Cluster verfügt über eine Writer-DB-Instance und zwei Reader-DB-Instances in drei separaten Availability Zones. Multi-AZ-DB-Cluster bieten hohe Verfügbarkeit, erhöhte Kapazität für Lese-Workloads und eine geringere Latenz im Vergleich zu Multi-AZ-Bereitstellungen.

Weitere Informationen finden Sie unter Erstellen eines Multi-AZ-DB-Clusters.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz161`

Quelle

`AWS Config Managed Rule: rds-cluster-multi-az-enabled`

Warnungskriterien

Gelb: In Ihrem Amazon-RDS-DB-Cluster ist keine Multi-AZ-Replikation konfiguriert

Empfohlene Aktion

Aktivieren Sie die Multi-AZ-DB-Cluster-Bereitstellung, wenn Sie einen Amazon-RDS-DB-Cluster erstellen.

Weitere Informationen finden Sie unter Erstellen eines Multi-AZ-DB-Clusters.

Weitere Ressourcen

Multi-AZ-DB-Cluster-Bereitstellungen

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

RDS-Multi-AZ-Standby-Instance ist nicht aktiviert

Beschreibung

Überprüft, ob für Ihre Amazon-RDS-DB-Instances ein Multi-AZ-Standby-Replikat konfiguriert ist.

Amazon RDS Multi-AZ sorgt für eine hohe Verfügbarkeit und Haltbarkeit von Datenbank-Instances, indem Daten auf ein Standby-Replikat in einer anderen Availability Zone repliziert werden. Dies ermöglicht ein automatisches Failover und verbessert die Leistung und Beständigkeit der Daten. Bei einer Multi-AZ-Bereitstellung einer DB-Instance sorgt Amazon RDS für eine automatische Bereitstellung und Verwaltung eines synchronen Standby-Replikats in einer anderen Availability Zone. Die primäre DB-Instance wird synchron über Availability Zones hinweg auf ein Standby-Replikat repliziert, um Datenredundanz bereitzustellen und Latenzspitzen während Systemsicherungen zu minimieren. Wenn Sie eine DB-Instance mit hoher Verfügbarkeit ausführen, verbessert dies die Verfügbarkeit bei geplanten Systemwartungen. Sie kann auch Ihre Datenbanken bei Ausfällen der DB-Instance und bei Nichtverfügbarkeit von Availability Zones schützen.

Weitere Informationen finden Sie unter Multi-AZ-DB-Instance-Bereitstellungen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz156`

Quelle

`AWS Config Managed Rule: rds-multi-az-support`

Warnungskriterien

Gelb: Für eine Amazon-RDS-DB-Instance ist kein Multi-AZ-Replikat konfiguriert.

Empfohlene Aktion

Aktivieren Sie die Multi-AZ-Bereitstellung, wenn Sie eine Amazon-RDS-DB-Instance erstellen.

Diese Prüfung kann nicht aus der Ansicht in der Trusted Advisor Konsole ausgeschlossen werden.

Weitere Ressourcen

Multi-AZ-DB-Instance-Bereitstellungen

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon RDS ReplicaLag

Beschreibung

Überprüft, ob die ReplicaLag CloudWatch Metrik für eine RDS-Datenbank-Instance in der letzten Woche über einen betrieblich vertretbaren Schwellenwert gestiegen ist.

ReplicaLag Die Metrik misst die Anzahl der Sekunden, für die sich eine Read Replica hinter der primären Instance befindet. Eine Verzögerung bei der Replikation tritt auf, wenn die asynchronen Aktualisierungen des Lesereplikats nicht mit den Aktualisierungen in der primären Datenbank-Instance Schritt halten können. Im Falle eines Ausfalls der primären Instance könnten Daten in der Read Replica fehlen, wenn sie über einem betrieblich ReplicaLag vertretbaren Schwellenwert liegen.

Prüf-ID

`Cmsvnj8db1`

Warnungskriterien

- Rot: Die ReplicaLag Metrik hat mindestens einmal in der Woche 60 Sekunden überschritten.
- Gelb: Die ReplicaLag Metrik hat in der Woche mindestens einmal 10 Sekunden überschritten.
- Grün: ReplicaLag weniger als 10 Sekunden.

Empfohlene Aktion

Es gibt mehrere mögliche Ursachen für ReplicaLag einen Anstieg über betriebssichere Werte. Dies kann beispielsweise durch kürzlich ersetzte/gestartete Replikat-Instances aus älteren Backups verursacht werden und diese Replikate benötigen viel Zeit, um den Fortschritt der primären Datenbank-Instance und der Live-Transaktionen „aufzuholen“. Dies ReplicaLag kann im Laufe der Zeit abnehmen, wenn ein Aufholprozess stattfindet. Ein anderes Beispiel könnte sein, dass die Transaktionsgeschwindigkeit, die in der primären Datenbank-Instance erreicht werden kann, höher ist als der Replikationsprozess oder die Replikatinfrastruktur. Dies ReplicaLag kann im Laufe der Zeit zunehmen, da die Replikation nicht mit der Leistung der Primärdatenbank Schritt hält. Schließlich kann die Arbeitslast zu unterschiedlichen Tages-/Monatszeiten usw. stark beansprucht werden, was gelegentlich zu Verzögerungen führen kann. ReplicaLag Ihr Team sollte untersuchen, welche mögliche Ursache zu dem hohen Wert ReplicaLag für die Datenbank beigetragen hat, und eventuell den Typ der Datenbankinstanz oder andere Merkmale der Arbeitslast ändern, um sicherzustellen, dass die Datenkontinuität auf dem Replikat Ihren Anforderungen entspricht.

Weitere Ressourcen

- Arbeiten mit Lesereplikaten in Amazon RDS für PostgreSQL
- Arbeiten mit MySQL-Replikation in Amazon RDS
- Arbeiten mit MySQL-Lesereplikaten

Berichtsspalten

- Status
- Region
- DB-Instance-ARN
- ReplicaLag Metrik

Der Amazon RDS-Parameter synchronous_commit ist ausgeschaltet

Beschreibung

Wenn der Parameter synchronous_commit ausgeschaltet ist, können Daten bei einem Datenbankabsturz verloren gehen. Die Haltbarkeit der Datenbank ist gefährdet.

Es wird empfohlen, den Parameter synchronous_commit zu aktivieren.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen nicht in Trusted Advisor oder in der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt026`

Warnungskriterien

Rot: Bei DB-Parametergruppen ist der Parameter synchronous_commit ausgeschaltet.

Empfohlene Aktion

Aktivieren Sie den Parameter synchronous_commit in Ihren DB-Parametergruppen.

Weitere Ressourcen

Der Parameter synchronous_commit definiert den Abschluss des Write-Ahead Logging (WAL) -Prozesses, bevor der Datenbankserver eine erfolgreiche Benachrichtigung an den Client sendet. Dieser Commit wird als asynchroner Commit bezeichnet, da der Client den Commit bestätigt, bevor WAL die Transaktion auf der Festplatte speichert. Wenn der Parameter synchronous_commit ausgeschaltet ist, können die Transaktionen verloren gehen, die Haltbarkeit der DB-Instance kann beeinträchtigt werden und Daten können verloren gehen, wenn eine Datenbank abstürzt.

Weitere Informationen finden Sie unter Logdateien der MySQL-Datenbank.

Berichtsspalten

- Status
- Region
- Ressource
- Name des Parameters
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Automatisierte Amazon-Redshift-Cluster-Snapshots

Beschreibung

Prüft, ob automatische Snapshots für Ihre Amazon-Redshift-Cluster aktiviert sind.

Amazon Redshift erstellt in regelmäßigen Abständen inkrementelle Snapshots und verfolgt so Änderungen am Cluster seit dem letzten automatisierten Snapshot nach. Automatisierte Snapshots speichern alle Daten, die erforderlich sind, um einen Cluster anhand eines Snapshots wiederherzustellen. Zum Deaktivieren von automatischen Snapshots setzen Sie den Wert für den Aufbewahrungszeitraum auf null. Sie können automatische Snapshots für RA3-Knotentypen nicht deaktivieren.

Sie können die gewünschte Mindest- und Höchstdauer der Aufbewahrung mithilfe der Parameter MinRetentionMaxRetentionZeitraum und Zeitraum Ihrer AWS Config Regeln angeben.

Amazon-Redshift-Snapshots und -Sicherungen

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz135
```

Quelle

```
AWS Config Managed Rule: redshift-backup-enabled
```

Warnungskriterien

Rot: Amazon Redshift hat keine automatisierten Snapshots, die innerhalb des gewünschten Aufbewahrungszeitraums konfiguriert wurden.

Empfohlene Aktion

Stellen Sie sicher, dass automatische Snapshots für Ihre Amazon-Redshift-Cluster aktiviert sind.

Weitere Informationen finden Sie unter Verwalten von Snapshots mithilfe der Konsole.

Weitere Ressourcen

Amazon-Redshift-Snapshots und -Sicherungen

Weitere Informationen finden Sie unter Arbeiten mit Sicherungen.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon Route 53 gelöschte Integritätsprüfungen

Beschreibung

Prüft auf Ressourcendatensätzen, die mit gelöschten Zustandsprüfungen verbunden sind.

Route 53 hindert Sie nicht daran, eine Zustandsprüfung zu löschen, die mit einem oder mehreren Ressourceneintragsätzen verbunden ist. Wenn Sie eine Zustandsprüfung löschen, ohne die zugehörigen Ressourceneintragsätze zu aktualisieren, funktioniert die Weiterleitung von DNS-Anfragen für Ihre DNS-Failover-Konfiguration nicht wie vorgesehen.

Von AWS Diensten erstellte gehostete Zonen werden nicht in Ihren Prüfergebnissen angezeigt.

Prüf-ID

`Cb877eB72b`

Warnungskriterien

Gelb: Ein Ressourcendatensatz ist mit einer Zustandsprüfung verknüpft, die gelöscht wurde.

Empfohlene Aktion

Erstellen Sie eine neue Zustandsprüfung und ordnen Sie sie dem Ressourcendatensatz zu. Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen und Hinzufügen von Zustandsprüfungen zu Ressourcendatensätzen.

Weitere Ressourcen

- Erstellen von Amazon-Route-53-Zustandsprüfungen und Konfigurieren des DNS-Failovers
- So funktionieren Zustandsprüfungen in einfachen Amazon-Route-53-Konfigurationen

Berichtsspalten

- Name der gehosteten Zone
- ID der gehosteten Zone
- Name des Ressourcendatensatzes
- Typ des Ressourcendatensatzes
- Kennung des Ressourcendatensatzes

Amazon Route 53 Failover-Ressourceneintragsätze

Beschreibung

Prüft auf Amazon Route 53 Failover-Ressourceneintragsätze, die eine Fehlkonfiguration aufweisen.

Wenn Amazon Route 53 Zustandsprüfungen feststellen, dass die primäre Ressource ungesund ist, antwortet Amazon Route 53 auf Anfragen mit einem sekundären Backup-Ressourceneintragsatz. Sie müssen korrekt konfigurierte primäre und sekundäre Ressourceneintragsätze erstellen, damit das Failover funktioniert.

Von AWS Diensten erstellte Hosting-Zonen werden nicht in Ihren Prüfergebnissen angezeigt.

Prüf-ID

`b73EEdD790`

Warnungskriterien

- Gelb: Ein primärer Failover-Ressourcendatensatz hat keinen entsprechenden sekundären Ressourcendatensatz.
- Gelb: Ein sekundärer Failover-Ressourcendatensatz hat keinen entsprechenden primären Ressourcendatensatz.
- Gelb: Primäre und sekundäre Ressourcendatensätze mit demselben Namen werden derselben Zustandsprüfung zugeordnet.

Empfohlene Aktion

Wenn ein Failover-Ressourcensatz fehlt, erstellen Sie den entsprechenden Ressourcendatensatz. Weitere Informationen finden Sie unter Erstellen von Failover-Ressourcendatensätzen.

Wenn Ihre Ressourcendatensätze derselben Zustandsprüfung zugeordnet sind, erstellen Sie für jeden einzelnen eine separate Zustandsprüfung. Weitere Informationen finden Sie unter Erstellen, Aktualisieren und Löschen von Zustandsprüfungen.

Weitere Ressourcen

Erstellen von Amazon-Route-53-Zustandsprüfungen und Konfigurieren des DNS-Failovers

Berichtsspalten

- Name der gehosteten Zone
- ID der gehosteten Zone
- Name des Ressourcendatensatzes
- Typ des Ressourcendatensatzes
- Grund

Amazon Route 53 Hohe TTL Ressourceneintragsätze

Beschreibung

Sucht nach Ressourcendatensätzen, die von einem niedrigeren Wert time-to-live (TTL) profitieren können.

TTL ist die Anzahl der Sekunden, die ein Ressourceneintragsatz von DNS-Auflösern zwischengespeichert wird. Wenn Sie eine lange TTL angeben, brauchen DNS-Auflöser länger, um aktualisierte DNS-Einträge anzufordern, was zu unnötigen Verzögerungen bei der Umleitung des

Datenverkehrs führen kann. Eine lange TTL führt beispielsweise zu einer Verzögerung zwischen dem Zeitpunkt, an dem DNS Failover einen Endpunktausfall feststellt, und dem Zeitpunkt, an dem es mit der Umleitung des Datenverkehrs reagiert.

Von AWS Diensten erstellte gehostete Zonen werden in Ihren Prüfergebnissen nicht angezeigt.

Prüf-ID

`C056F80cR3`

Warnungskriterien

- Gelb: Ein Ressourcendatensatz, dessen Routing-Richtlinie Failover ist, hat eine TTL von mehr als 60 Sekunden.
- Gelb: Ein Ressourcendatensatz mit zugehöriger Zustandsprüfung hat eine TTL von mehr als 60 Sekunden.

Empfohlene Aktion

Geben Sie einen TTL-Wert von 60 Sekunden für die aufgelisteten Ressourcendatensätze ein. Weitere Informationen finden Sie unter Arbeiten mit Ressourcendatensätzen.

Weitere Ressourcen

Erstellen von Amazon-Route-53-Zustandsprüfungen und Konfigurieren des DNS-Failovers

Berichtsspalten

- Status
- Name der gehosteten Zone
- ID der gehosteten Zone
- Name des Ressourcendatensatzes
- Typ des Ressourcendatensatzes
- ID des Ressourcendatensatzes
- TTL

Amazon Route 53-Namenserver-Delegationen

Beschreibung

Prüft auf von Amazon Route 53 gehosteten Zonen, für die Ihr Domain-Registrar oder DNS nicht die richtigen Route 53-Namenserver verwendet.

Wenn Sie eine gehostete Zone erstellen, weist Route 53 einen Delegationssatz von vier Namenservern zu. Die Namen dieser Server lauten ns-###.awsdns-##.com, .net, .org und .co.uk, wobei ### und ## in der Regel für unterschiedliche Nummern stehen. Bevor Route 53 DNS-Anfragen für Ihre Domain weiterleiten kann, müssen Sie die Nameserverkonfiguration Ihres Registrars aktualisieren, um die Nameserver zu entfernen, die der Registrar zugewiesen hat. Anschließend müssen Sie alle vier Nameserver in den Route 53-Delegationssatz aufnehmen. Um eine maximale Verfügbarkeit zu erreichen, müssen Sie alle vier Route 53-Namenserver hinzufügen.

Von AWS Diensten erstellte Hosting-Zonen werden nicht in Ihren Prüfergebnissen angezeigt.

Prüf-ID

`cF171Db240`

Warnungskriterien

Gelb: Eine gehostete Zone, für die die Domainvergabestelle nicht alle vier Route 53-Namenserver im Delegierungssatz verwendet.

Empfohlene Aktion

Fügen Sie Nameserver-Datensätze bei Ihrer Vergabestelle oder mit dem aktuellen DNS-Service hinzu oder aktualisieren Sie sie, damit Ihre Domain alle vier Nameserver in Ihrem Route-53-Delegationssatz enthält. Informationen zu diesen Werten finden Sie unter Das Abrufen der Nameserver für eine öffentliche gehostete Zone. Hinweise zum Hinzufügen oder Aktualisieren von Nameserver-Datensätzen finden Sie unter Verwendung von Amazon Route 53 als DNS-Service für eine Subdomain ohne Migration der übergeordneten Domain.

Weitere Ressourcen

Arbeiten mit gehosteten Zonen

Berichtsspalten

- Name der gehosteten Zone
- ID der gehosteten Zone
- Anzahl der verwendeten Nameserver-Delegationen

Amazon Route 53 Resolver Redundanz der Endpunkt-Verfügbarkeitszonen

Beschreibung

Überprüft, ob in Ihrer Service-Konfiguration aus Redundanzgründen IP-Adressen in mindestens zwei Availability Zones (AZs) angegeben sind. Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Indem Sie IP-Adressen in mehreren Availability Zones in derselben Region angeben, können Sie Ihre Anwendungen vor einem einzelnen Ausfallpunkt schützen.

Prüf-ID

`Chrv231ch1`

Warnungskriterien

- Gelb: IP-Adressen werden nur in einer Availability Zone angegeben
- Grün: IP-Adressen werden in mindestens zwei Availability Zones angegeben

Empfohlene Aktion

Geben Sie zu Redundanzzwecken IP-Adressen in mindestens zwei Availability Zones an.

Weitere Ressourcen

- Wenn Sie benötigen, dass immer mehr als ein Endpunkt der elastic network interface verfügbar ist, empfehlen wir, mindestens eine weitere Netzwerkschnittstelle zu erstellen, als Sie benötigen, um sicherzustellen, dass zusätzliche Kapazitäten für die Handhabung möglicher Überspannungen verfügbar sind. Die zusätzliche Netzwerkschnittstelle stellt auch die Verfügbarkeit während des Servicebetriebs wie Wartung oder Upgrades sicher.
- Hohe Verfügbarkeit für Resolver-Endpunkte

Berichtsspalten

- Status
- Region
- ARN-Ressourcen
- Anzahl der AZs

Amazon S3 Bucket-Protokollierung

Beschreibung

Überprüft die Protokollierungskonfiguration von Amazon Simple Storage Service (Amazon S3)-Buckets.

Wenn die Serverzugriffsprotokollierung aktiviert ist, werden stündlich detaillierte Zugriffsprotokolle an einen von Ihnen gewählten Bucket übermittelt. Ein Zugriffsprotokoll enthält Details zu jeder Anfrage, wie z. B. den Anfragetyp, die in der Anfrage angegebenen Ressourcen sowie die Uhrzeit und das Datum der Bearbeitung der Anfrage. Standardmäßig ist die Bucket-Protokollierung nicht aktiviert. Sie sollten die Protokollierung aktivieren, wenn Sie Sicherheitsprüfungen durchführen oder mehr über Benutzer und Nutzungsmuster erfahren möchten.

Bei der erstmaligen Aktivierung der Protokollierung wird die Konfiguration automatisch validiert. Zukünftige Änderungen können jedoch zu Protokollierungsfehlern führen. Diese Prüfung untersucht explizite Amazon S3-Bucket-Berechtigungen, aber sie untersucht nicht die zugehörigen Bucket-Richtlinien, die die Bucket-Berechtigungen außer Kraft setzen könnten.

Prüf-ID

`BueAdJ7NrP`

Warnungskriterien

- Gelb: Die Serverzugriffsprotokollierung ist für den Bucket nicht aktiviert.
- Gelb: Die Ziel-Bucket-Berechtigungen beinhalten nicht das Root-Konto, daher Trusted Advisor kann es nicht überprüft werden.
- Rot: Der Ziel-Bucket ist nicht vorhanden.
- Rot: Der Ziel-Bucket und der Quell-Bucket haben unterschiedliche Eigentümer.
- Rot: Der Protokollbereitsteller hat keine Schreibberechtigung für den Ziel-Bucket.

Empfohlene Aktion

Aktivieren Sie die Bucket-Protokollierung für die meisten Buckets. Weitere Informationen finden Sie unter Aktivieren der Protokollierung mithilfe der Konsole und Aktivieren der programmgesteuerten Protokollierung.

Wenn die Ziel-Bucket-Berechtigungen das Root-Konto nicht beinhalten und Sie den Logging-Status überprüfen Trusted Advisor möchten, fügen Sie das Root-Konto als Empfänger hinzu. Weitere Informationen finden Sie unter Editing Bucket Permissions (Bearbeiten von Bucket-Berechtigungen).

Wenn der Ziel-Bucket nicht existiert, wählen Sie einen vorhandenen Bucket als Ziel aus oder erstellen Sie einen neuen und wählen Sie ihn aus. Weitere Informationen finden Sie unter Managing Bucket Logging (Verwalten der Bucket-Protokollierung).

Wenn das Ziel und die Quelle unterschiedliche Eigentümer haben, ändern Sie den Ziel-Bucket in einen Bucket mit demselben Eigentümer wie der Quell-Bucket. Weitere Informationen finden Sie unter Managing Bucket Logging (Verwalten der Bucket-Protokollierung).

Wenn der Protokollbereitsteller keine Schreibberechtigung für das Ziel hat (Schreiben nicht aktiviert), gewähren Sie der Protokollbereitstellungsgruppe Upload-/Löschberechtigungen. Weitere Informationen finden Sie unter Editing Bucket Permissions (Bearbeiten von Bucket-Berechtigungen).

Weitere Ressourcen

- Arbeiten mit Buckets
- Server-Zugriffsprotokollierung
- Serverzugriff-Protokollformat
- Löschen von Protokolldateien

Berichtsspalten

- Status
- Region
- Bucket-Name
- Ziel-Name
- Ziel ist vorhanden
- Derselbe Eigentümer
- Schreiben aktiviert
- Grund

Replikation des Amazon-S3-Buckets ist nicht aktiviert

Beschreibung

Überprüft, ob in Ihren Amazon-S3-Buckets Replikationsregeln für regionsübergreifende Replikation, Replikation in derselben Region oder für beides aktiviert sind.

Replikation ist das automatische, asynchrone Kopieren von Objekten zwischen Buckets in derselben oder verschiedenen Regionen. AWS Sie kopiert neu erstellte Objekte und Objektaktualisierungen aus einem Quell-Bucket in einen Ziel-Bucket oder mehrere Ziel-Buckets. Verwenden Sie die Amazon-S3-Bucket-Replikation, um die Resilienz und Konformität Ihrer Anwendungen und Datenspeicher zu verbessern.

Weitere Informationen finden Sie unter Replizieren von Objekten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz119`

Quelle

`AWS Config Managed Rule: s3-bucket-replication-enabled`

Warnungskriterien

Gelb: Die Amazon-S3-Bucket-Replikationsregeln sind nicht für die regionsübergreifende Replikation, die Replikation in derselben Region oder für beides aktiviert.

Empfohlene Aktion

Aktivieren Sie die Amazon-S3-Bucket-Replikationsregeln, um die Resilienz und Konformität Ihrer Anwendungen und Datenspeicher zu verbessern.

Weitere Informationen finden Sie unter Anzeigen Ihrer Backup-Jobs und Wiederherstellungspunkte und Einrichten der Replikation.

Weitere Ressourcen

Anleitungen: Beispiele zum Konfigurieren der Replikation

Berichtsspalten

- Status
- Region

- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon S3 Bucket-Versioning

Beschreibung

Prüft auf Amazon Simple Storage Service-Buckets, bei denen die Versioning nicht aktiviert ist oder die Versionierung ausgesetzt wurde.

Wenn die Versioning aktiviert ist, können Sie sowohl unbeabsichtigte Benutzeraktionen als auch Anwendungsfehler problemlos beheben. Mit Versioning können Sie jede Version eines Objekts, das in einem Bucket gespeichert ist, aufbewahren, abrufen und wiederherstellen. Sie können Lebenszyklusregeln verwenden, um alle Versionen Ihrer Objekte sowie die damit verbundenen Kosten zu verwalten, indem Sie Objekte automatisch in der Speicherklasse Glacier archivieren. Die Regeln können auch so konfiguriert werden, dass Versionen Ihrer Objekte nach einem bestimmten Zeitraum entfernt werden. Sie können auch eine Multi-Faktor-Authentifizierung (MFA) für alle Objektlöschungen oder Konfigurationsänderungen an Ihren Buckets verlangen.

Die Versioning kann nicht mehr deaktiviert werden, nachdem sie aktiviert wurde. Sie kann jedoch ausgesetzt werden, so dass keine neuen Versionen von Objekten erstellt werden können. Die Verwendung der Versioning kann Ihre Kosten für Amazon S3 erhöhen, da Sie für die Speicherung mehrerer Versionen eines Objekts bezahlen.

Prüf-ID

`R365s2Qddf`

Warnungskriterien

- Grün: Versioning ist für den Bucket aktiviert.
- Gelb: Versioning ist für den Bucket aktiviert.
- Gelb: Versionierung ist für den Bucket ausgesetzt.

Empfohlene Aktion

Aktivieren Sie das Bucket-Versioning für die meisten Buckets, um versehentliches Löschen oder Überschreiben zu verhindern. Weitere Informationen finden Sie unter Verwenden des Versioning und Aktivieren des Versioning für Buckets.

Wenn das Bucket-Versioning ausgesetzt ist, sollten Sie es erneut aktivieren. Informationen zum Verwalten von Objekten in einem Bucket mit ausgesetztem Versioning finden Sie unter Arbeiten mit Objekten in einem Bucket mit ausgesetztem Versioning.

Wenn das Versioning aktiviert oder ausgesetzt ist, können Sie Lebenszyklus-Konfigurationsregeln definieren, um bestimmte Objektversionen als abgelaufen zu kennzeichnen oder nicht benötigte Objektversionen dauerhaft zu entfernen. Weitere Informationen hierzu finden Sie im Abschnitt Objektlebenszyklusverwaltung.

MFA Delete erfordert zusätzliche Authentifizierung, wenn der Versioning-Status des Buckets geändert wird oder Versionen eines Objekts gelöscht werden. Der Benutzer muss Anmeldeinformationen und einen Code von einem zugelassenen Authentifizierungsgerät eingeben. Weitere Informationen finden Sie unter MFA Delete (MFA-Löschung).

Weitere Ressourcen

Arbeiten mit Buckets

Berichtsspalten

- Status
- Region
- Bucket-Name
- Versionsverwaltung
- MFA Delete aktiviert

Application Load Balancer, Network Load Balancer und Gateway Load Balancer, die sich nicht über mehrere Availability Zones erstrecken

Beschreibung

Prüft, ob Ihre Load Balancer (Application Load Balancer, Network Load Balancer und Gateway Load Balancer) mit Subnetzen in mehreren Availability Zones konfiguriert sind.

Sie können Ihre gewünschten Mindestverfügbarkeitszonen in den AvailabilityZonesMindestparametern Ihrer AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Availability Zones für Ihren Application Load Balancer, Availability Zones – Network Load Balancer und Erstellen eines Gateway Load Balancers.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz169`

Quelle

`AWS Config Managed Rule: elbv2-multiple-az`

Warnungskriterien

Gelb: Application Load Balancer, Network Load Balancer und Gateway Load Balancer, die mit Subnetzen in weniger als zwei Availability Zones konfiguriert sind.

Empfohlene Aktion

Konfigurieren Sie Ihre Application Load Balancer, Network Load Balancer und Gateway Load Balancer mit Subnetzen in mehreren Availability Zones.

Weitere Ressourcen

Availability Zones für Ihren Application Load Balancer

Availability Zones (Elastic Load Balancing)

Erstellen eines Gateway Load Balancers

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Für Auto Scaling verfügbare IPs in Subnetzen

Beschreibung

Überprüft, ob in den Ziel-Subnetzen noch genügend IPs verfügbar sind. Das wäre hilfreich, wenn die Auto-Scaling-Gruppe ihre maximale Größe erreicht hat und zusätzliche Instances gestartet werden müssen.

Prüf-ID

`Cjxm268ch1`

Warnungskriterien

- Rot: Die maximale Anzahl von Instances und IP-Adressen, die von einer Auto-Scaling-Gruppe erstellt werden könnten, übersteigt die Anzahl der verbleibenden IP-Adressen in den konfigurierten Subnetzen.
- Grün: Es sind ausreichend IP-Adressen für den verbleibenden Umfang verfügbar, der in der Auto-Scaling-Gruppe möglich ist.

Empfohlene Aktion

Erhöhen Sie die Anzahl der verfügbaren IP-Adressen.

Berichtsspalten

- Status
- Region
- ARN-Ressourcen
- Maximale Anzahl an Instances, die erstellt werden können
- Anzahl der verfügbaren Instances

Auto-Scaling-Gruppe Zustandsprüfungen

Beschreibung

Untersucht die Konfiguration der Zustandsprüfung für Auto-Scaling-Gruppen.

Wenn Elastic Load Balancing für eine Auto-Scaling-Gruppe verwendet wird, wird empfohlen, eine Elastic Load Balancing-Zustandsprüfung zu aktivieren. Wenn keine Elastic Load Balancing-Zustandsprüfung verwendet wird, kann Auto-Scaling nur auf den Zustand der Amazon Elastic Compute Cloud (Amazon EC2)-Instance reagieren. Auto-Scaling wirkt sich nicht auf die Anwendung aus, die auf der Instance läuft.

Prüf-ID

CL0G40CD08

Warnungskriterien

- Gelb: Einer Auto-Scaling-Gruppe ist ein Load Balancer zugeordnet, aber die Zustandsprüfung für Elastic-Load-Balancing ist nicht aktiviert.
- Gelb: Einer Auto-Scaling-Gruppe ist kein Load Balancer zugeordnet, aber die Zustandsprüfung für Elastic-Load-Balancing ist aktiviert.

Empfohlene Aktion

Wenn der Auto-Scaling-Gruppe ein Load Balancer zugeordnet ist, die Zustandsprüfung für Elastic Load Balancing jedoch nicht aktiviert ist, finden Sie weitere Informationen unter Hinzufügen von Zustandsprüfungen für Elastic-Load-Balancing zu einer Auto-Scaling-Gruppe.

Wenn die Zustandsprüfung für Elastic-Load-Balancing aktiviert ist, aber der Auto-Scaling-Gruppe kein Load Balancer zugeordnet ist, finden Sie weitere Informationen unter Set Up an Auto-Scaled and Load-Balanced Application (Einrichten einer Auto-Scaling-Anwendung mit Load Balancing).

Weitere Ressourcen

Benutzerhandbuch für Amazon EC2 Auto Scaling

Berichtsspalten

- Status
- Region
- Name der Auto-Scaling-Gruppe
- Load Balancer zugeordnet
- Zustandsprüfung

Auto-Scaling-Gruppe-Ressourcen

Beschreibung

Prüft die Verfügbarkeit von Ressourcen, die mit Startkonfigurationen und Ihren Auto-Scaling-Gruppen verbunden sind.

Auto-Scaling-Gruppen, die auf nicht verfügbare Ressourcen verweisen, können keine neuen Amazon-Elastic-Compute-Cloud(Amazon EC2)-Instances starten. Bei richtiger Konfiguration

bewirkt Auto-Scaling, dass die Anzahl der Amazon-EC2-Instances bei Bedarfsspitzen nahtlos erhöht und bei Bedarfstiefs automatisch verringert wird. Auto-Scaling-Gruppen und Startkonfigurationen, die auf nicht verfügbare Ressourcen verweisen, funktionieren nicht wie vorgesehen.

Prüf-ID

`8CNsSllI5v`

Warnungskriterien

- Rot: Einer Auto-Scaling-Gruppe ist ein gelöschter Load Balancer zugeordnet.
- Rot: Eine Startkonfiguration ist einem gelöschten Amazon Machine Image (AMI) zugeordnet.

Empfohlene Aktion

Wenn der Load Balancer gelöscht wurde, können Sie entweder einen neuen Load Balancer oder eine neue Zielgruppe erstellen und ihn oder sie dann mit der Auto-Scaling-Gruppe verknüpfen. Oder Sie können eine neue Auto-Scaling-Gruppe ohne den Load Balancer erstellen. Informationen zum Erstellen einer neuen Auto-Scaling-Gruppe mit einem neuen Load Balancer finden Sie unter Set Up an Auto-Scaled and Load-Balanced Application (Einrichten einer Auto-Scaling-Anwendung mit Load Balancer). Informationen zum Erstellen einer neuen Auto-Scaling-Gruppe ohne Load Balancer finden Sie unter „Create Auto Scaling Group“ (Erstellen einer Auto-Scaling-Gruppe) in Getting Started With Auto Scaling Using the Console (Erste Schritte mit Auto Scaling mit der Konsole).

Wenn das AMI gelöscht wurde, erstellen Sie eine neue Startvorlage oder Startvorlagenversion mit einem gültigen AMI und ordnen Sie es einer Auto-Scaling-Gruppe zu. Weitere Informationen finden Sie unter „Create Launch Configuration“ (Erstellen einer Startkonfiguration) in Getting Started With Auto Scaling Using the Console (Erste Schritte mit Auto Scaling mit der Konsole).

Weitere Ressourcen

- Fehlerbehebung bei Auto Scaling: Amazon-EC2-AMIs
- Fehlerbehebung bei Auto Scaling: Load-Balancer-Konfiguration
- Benutzerhandbuch für Amazon EC2 Auto Scaling

Berichtsspalten

- Status
- Region
- Name der Auto-Scaling-Gruppe
- Starttyp

- Ressourcentyp
- Ressourcenname

AWS CloudHSM -Cluster, auf denen HSM-Instances in einer einzigen AZ ausgeführt werden

Beschreibung

Überprüft Ihre Cluster, die HSM-Instances in einer einzigen Availability Zone (AZ) ausführen. Diese Prüfung warnt Sie, wenn bei Ihren Clustern das Risiko besteht, dass sie nicht über das neueste Backup verfügen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`hc0dfs7601`

Warnungskriterien

- Gelb: Auf einem CloudHSM-Cluster werden alle HSM-Instances in einer einzigen Availability Zone für mehr als 1 Stunde ausgeführt.
- Grün: Auf einem CloudHSM-Cluster werden alle HSM-Instances in mindestens zwei verschiedenen Availability Zones ausgeführt.

Empfohlene Aktion

Erstellen Sie mindestens eine weitere Instance für den Cluster in einer anderen Availability Zone.

Weitere Ressourcen

Bewährte Verfahren für AWS CloudHSM

Berichtsspalten

- Status

- Region
- Cluster ID
- Anzahl der HSM-Instances
- Zeitpunkt der letzten Aktualisierung

AWS Direct Connect Ausfallsicherheit des Standorts

Beschreibung

Überprüft die Belastbarkeit der für die Verbindung zwischen Ihrem Standort und jedem Direct Connect Gateway oder Virtual Private Gateway AWS Direct Connect verwendeten Geräte.

Diese Prüfung warnt Sie, wenn ein Direct Connect-Gateway oder ein Virtual Private Gateway nicht mit virtuellen Schnittstellen an mindestens zwei verschiedenen Direct Connect-Standorten konfiguriert ist. Mangelnde Ausfallsicherheit kann zu unerwarteten Ausfallzeiten während der Wartung, einem Glasfaserausfall, einem Geräteausfall oder einem kompletten Standortausfall führen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden.

> **Note**
>
> Direct Connect wird mit Transit Gateway unter Verwendung des Direct Connect-Gateways implementiert.

Prüf-ID

`c1dfpnchv2`

Warnungskriterien

Rot: Das Direct Connect-Gateway oder Virtual Private Gateway ist mit einer oder mehreren virtuellen Schnittstellen auf einem einzigen Direct Connect-Gerät konfiguriert.

Gelb: Das Direct Connect-Gateway oder Virtual Private Gateway ist mit virtuellen Schnittstellen für mehrere Direct Connect-Geräte an einem einzigen Direct Connect-Standort konfiguriert.

Grün: Das Direct Connect-Gateway oder Virtual Private Gateway ist mit virtuellen Schnittstellen an zwei oder mehr unterschiedlichen Direct Connect-Standorten konfiguriert.

Empfohlene Aktion

Um die Stabilität von Direct Connect-Standorten zu erhöhen, können Sie das Direct Connect-Gateway oder das Virtual Private Gateway so konfigurieren, dass es Connect zu mindestens zwei unterschiedlichen Direct Connect-Standorten herstellt. Weitere Informationen finden Sie unter AWS Direct Connect Resilienz-Empfehlung.

Weitere Ressourcen

AWS Direct Connect Empfehlungen zur Resilienz

AWS Direct Connect Failover-Test

Berichtsspalten

- Status
- Region
- Zeitpunkt der letzten Aktualisierung
- Status der Resilienz
- Ort
- Verbindungs-ID
- Gateway-ID

AWS Lambda funktioniert, ohne dass eine Warteschlange für unzustellbare Nachrichten konfiguriert ist

Beschreibung

Prüft, ob eine AWS Lambda Funktion mit einer Warteschlange für unzustellbare Briefe konfiguriert ist.

Eine Warteschlange für unzustellbare Nachrichten ist eine Funktion AWS Lambda , mit der Sie fehlgeschlagene Ereignisse erfassen und analysieren können, sodass Sie diese Ereignisse entsprechend behandeln können. Ihr Code kann eine Ausnahme oder eine Zeitüberschreitung

auslösen oder bewirken, dass der Speicher knapp wird, was zu fehlgeschlagenen asynchronen Ausführungen Ihrer Lambda-Funktion führt. In einer Warteschlange für unzustellbare Nachrichten werden Nachrichten von fehlgeschlagenen Aufrufen gespeichert, sodass die Nachrichten verarbeitet und Fehler behoben werden können.

Sie können die Warteschlangenressource für unzustellbare Briefe, die Sie überprüfen möchten, mithilfe des Parameters dlqArns in Ihren Regeln angeben. AWS Config

Weitere Informationen finden Sie unter Warteschlangen für unzustellbare Nachrichten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz182
```

Quelle

```
AWS Config Managed Rule: lambda-dlq-check
```

Warnungskriterien

Gelb: Für die AWS Lambda Funktion wurde keine Warteschlange für unzustellbare Briefe konfiguriert.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre AWS Lambda Funktionen über eine Warteschlange für unzustellbare Briefe verfügen, die so konfiguriert ist, dass die Nachrichtenverarbeitung für alle fehlgeschlagenen asynchronen Aufrufe gesteuert wird.

Weitere Informationen finden Sie unter Warteschlangen für unzustellbare Nachrichten.

Weitere Ressourcen

- Robustes Design für serverlose Anwendung mit AWS-Lambda-Funktion für Warteschlangen für unzustellbare Nachrichten

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Lambda Ziele für Ereignisse bei einem Ausfall

Beschreibung

Überprüft, ob für Lambda-Funktionen in Ihrem Konto ein Ereignisziel bei einem Ausfall oder eine Warteschlange für unzustellbare Nachrichten für asynchrone Aufrufe konfiguriert ist, sodass Datensätze von fehlgeschlagenen Aufrufen zur weiteren Untersuchung oder Verarbeitung an ein Ziel weitergeleitet werden können.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch05`

Warnungskriterien

- Gelb: Für die Funktion ist kein Ereignisziel bei einem Ausfall oder eine Warteschlange für unzustellbare Nachrichten konfiguriert.

Empfohlene Aktion

Richten Sie das Ereignisziel bei einem Ausfall oder eine Warteschlange für unzustellbare Nachrichten für Ihre Lambda-Funktionen ein, um fehlgeschlagene Aufrufe zusammen mit anderen

Details an einen der verfügbaren AWS-Ziel-Services zur weiteren Fehlersuche oder Verarbeitung zu senden.

Weitere Ressourcen

- Asynchroner Aufruf
- AWS Lambda Ziele für Ereignisse bei einem Ausfall

Berichtsspalten

- Status
- Region
- Die Funktion mit der Version, die markiert ist.
- Der Prozentsatz der am aktuellen Tag verworfenen asynchronen Anforderungen
- Asynchrone Anforderungen am aktuellen Tag
- Durchschnittlicher Prozentsatz der täglich verworfenen asynchronen Anforderungen
- Durchschnittliche tägliche asynchrone Anforderungen
- Zeitpunkt der letzten Aktualisierung

AWS Lambda VPC-fähige Funktionen ohne Multi-AZ-Redundanz

Beschreibung

Überprüft die $LATEST-Version von VPC-fähigen Lambda-Funktionen, die anfällig für Dienstunterbrechungen in einer einzelnen Availability Zone sind. Es hat sich bewährt, dass VPC-fähige Funktionen mit mehreren Availability Zones verbunden sind, um eine hohe Verfügbarkeit zu gewährleisten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`L4dfs2Q4C6`

Warnungskriterien

Gelb: Die $LATEST-Version einer VPC-fähigen Lambda-Funktion ist mit Subnetzen in einer einzigen Availability Zone verbunden.

Empfohlene Aktion

Wählen Sie bei der Konfiguration von Funktionen für den Zugriff auf Ihre VPC Subnetze in mehreren Availability Zones aus, um eine hohe Verfügbarkeit sicherzustellen.

Weitere Ressourcen

- Konfigurieren einer Lambda-Funktion für den Zugriff auf Ressourcen in einer VPC
- Resilienz in AWS Lambda

Berichtsspalten

- Status
- Region
- Funktion-ARN
- VPC-ID
- Durchschnittliche tägliche Aufrufe
- Zeitpunkt der letzten Aktualisierung

AWS Resilience Hub Überprüfung der Anwendungskomponenten

Beschreibung

Prüft, ob eine Anwendungskomponente (AppComponent) in Ihrer Anwendung nicht wiederhergestellt werden kann. Wenn ein im Falle einer Unterbrechung AppComponent nicht wiederhergestellt wird, kann es zu unbekanntem Datenverlust und Systemausfällen kommen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden.

Prüf-ID

`RH23stmM04`

Warnungskriterien

Rot: kann AppComponent nicht wiederhergestellt werden.

Empfohlene Aktion

Um sicherzustellen, dass Ihr Gerät wiederherstellbar AppComponent ist, überprüfen und implementieren Sie die Empfehlungen zur Ausfallsicherheit und führen Sie anschließend eine neue Bewertung durch. Weitere Informationen zur Überprüfung der Resilienzempfehlungen finden Sie unter Zusätzliche Ressourcen.

Weitere Ressourcen

Überprüfung der Resilienz-Empfehlungen

AWS Resilience Hub -Konzepte

AWS Resilience Hub Benutzerhandbuch

Berichtsspalten

- Status
- Region
- Anwendungsname
- AppComponent Name
- Zeitpunkt der letzten Aktualisierung

AWS Resilience Hub Richtlinie verletzt

Beschreibung

Sucht in Resilience Hub nach Anwendungen, die das Recovery Time Objective (RTO) und Recovery Point Objective (RPO) nicht erfüllen. Diese Prüfung warnt Sie, wenn Ihre Anwendung die RTO- und RPO-Ziele, die Sie für eine Anwendung in Resilience Hub festgelegt haben, nicht erfüllt.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden automatisch aktualisiert und Aktualisierungsanforderungen sind nicht zulässig. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`RH23stmM02`

Warnungskriterien

- Grün: Die Anwendung hat eine Richtlinie und erfüllt die RTO- und RPO-Ziele.
- Gelb: Die Anwendung wurde noch nicht geprüft.
- Rot: Die Anwendung hat eine Richtlinie, erfüllt aber nicht die RTO- und RPO-Ziele.

Empfohlene Aktion

Melden Sie sich bei der Resilience-Hub-Konsole an und überprüfen Sie die Empfehlungen, damit Ihre Anwendung die RTO- und RPO-Ziele erfüllt.

Weitere Ressourcen

Resilience-Hub-Konzepte

Berichtsspalten

- Status
- Region
- Anwendungsname
- Zeitpunkt der letzten Aktualisierung

AWS Resilience Hub Resilienzwerte

Beschreibung

Prüft, ob Sie eine Bewertung für Ihre Anwendungen in Resilience Hub durchgeführt haben. Diese Prüfung warnt Sie, wenn Ihre Resilienzwerte unter einem bestimmten Wert liegen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden automatisch aktualisiert und Aktualisierungsanforderungen sind nicht zulässig. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`RH23stmM01`

Warnungskriterien

- Grün: Ihre Anwendung hat einen Resilienzwert von 70 oder höher.
- Gelb: Ihre Anwendung hat einen Resilienzwert von 40 bis 69.
- Gelb: Die Anwendung wurde noch nicht geprüft.
- Rot: Ihre Anwendung hat einen Resilienzwert von weniger als 40.

Empfohlene Aktion

Melden Sie sich bei der Resilience-Hub-Konsole an und führen Sie eine Bewertung für Ihre Anwendung durch. Lesen Sie die Empfehlungen zur Verbesserung des Resilienzwertes.

Weitere Ressourcen

Resilience-Hub-Konzepte

Berichtsspalten

- Status
- Region
- Anwendungsname
- Resilienzwert der Anwendung
- Zeitpunkt der letzten Aktualisierung

AWS Resilience Hub Alter der Bewertung

Beschreibung

Prüft, wie lange es her ist, dass Sie das letzte Mal eine Anwendungsbeurteilung durchgeführt haben. Bei dieser Prüfung werden Sie benachrichtigt, wenn Sie seit einer bestimmten Anzahl von Tagen keine Anwendungsbeurteilung durchgeführt haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`RH23stmM03`

Warnungskriterien

- Grün: Ihre Anwendungsbeurteilung wurde in den letzten 30 Tagen durchgeführt.
- Gelb: Ihre Anwendungsbeurteilung wurde in den letzten 30 Tagen nicht durchgeführt.

Empfohlene Aktion

Melden Sie sich bei der Resilience-Hub-Konsole an und führen Sie eine Bewertung für Ihre Anwendung durch.

Weitere Ressourcen

Resilience-Hub-Konzepte

Berichtsspalten

- Status
- Region
- Anwendungsname
- Tage seit der letzten Bewertung
- Laufzeit der letzten Bewertung
- Zeitpunkt der letzten Aktualisierung

AWS Site-to-Site VPN hat mindestens einen Tunnel im Status DOWN

Beschreibung

Überprüft die Anzahl der Tunnel, die für jeden Ihrer AWS Site-to-Site VPN s aktiv sind.

In einem VPN sollten immer zwei Tunnel konfiguriert sein. Dies bietet Redundanz im Falle eines Ausfalls oder einer geplanten Wartung der Geräte am AWS-Endpunkt. Bei einigen Geräten ist jeweils nur ein Tunnel aktiv. Wenn ein VPN keine aktiven Tunnel hat, können trotzdem Gebühren für das VPN anfallen.

Weitere Informationen finden Sie unter Was ist AWS Site-to-Site-VPN?

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz123
```

Quelle

```
AWS Config Managed Rule: vpc-vpn-2-tunnels-up
```

Warnungskriterien

Gelb: Ein Site-to-Site-VPN hat mindestens einen Tunnel im DOWN-Status.

Empfohlene Aktion

Stellen Sie sicher, dass zwei Tunnel für VPN-Verbindungen konfiguriert sind. Und wenn Ihre Hardware dies unterstützt, stellen Sie sicher, dass beide Tunnel aktiv sind. Wenn Sie eine VPN-Verbindung nicht mehr benötigen, löschen Sie sie, um Kosten zu vermeiden.

Weitere Informationen finden Sie unter Ihr Kunden-Gateway-Gerät und in den im AWS-Wissenscenter verfügbaren Inhalten.

Weitere Ressourcen

- AWS Site-to-Site VPN Benutzerhandbuch
- Hinzufügen eines Virtual Private Gateways zu Ihrer VPC

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Well-Architected-Probleme mit hohem Risiko für die Zuverlässigkeit

Beschreibung

Prüft auf Probleme mit hohem Risiko (HRI) für Ihre Workloads hinsichtlich der Zuverlässigkeit. Diese Prüfung basiert auf Ihren AWS-Well Architected-Beurteilungen. Ihre Prüfergebnisse hängen davon ab, ob Sie die Workload-Bewertung mit AWS Well-Architected durchgeführt haben.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`Wxdfp4B1L4`

Warnungskriterien

- Rot: In der Zuverlässigkeitssäule für AWS Well-Architected wurde mindestens ein aktives Problem mit hohem Risiko identifiziert.
- Grün: In der Zuverlässigkeitssäule von AWS Well-Architected wurden keine aktiven Probleme mit hohem Risiko festgestellt.

Empfohlene Aktion

AWS Well-Architected hat bei Ihrer Workload-Evaluierung Probleme mit hohem Risiko erkannt. Diese Probleme bieten Möglichkeiten, Risiken zu reduzieren und Geld zu sparen. Melden Sie sich bei AWS Well-Architected an, um Ihre Antworten zu überprüfen und Maßnahmen zur Lösung der aktiven Probleme zu ergreifen.

Berichtsspalten

- Status
- Region
- Workload-ARN
- Name der Workload
- Name des Reviewers

- Workload-Typ
- Startdatum der Workload
- Datum der letzten Änderung der Workload
- Anzahl der identifizierten HRI für die Zuverlässigkeit
- Anzahl der behobenen HRI für die Zuverlässigkeit
- Anzahl der für die Zuverlässigkeit beantworteten Fragen
- Gesamtzahl der Fragen hinsichtlich der Zuverlässigkeit
- Zeitpunkt der letzten Aktualisierung

Für Classic Load Balancer sind nicht mehrere AZs konfiguriert.

Beschreibung

Prüft, ob der Classic Load Balancer mehrere Availability Zones (AZs) umfasst.

Ein Load Balancer verteilt eingehenden Anwendungsdatenverkehr auf mehrere Amazon-EC2-Instances in mehreren Availability Zones. Der Load Balancer verteilt den Datenverkehr standardmäßig gleichmäßig auf die Availability Zones, die Sie für Ihren Load Balancer aktivieren. Bei einem Ausfall einer Availability Zone leiten Load-Balancer-Knoten Anforderungen automatisch an die fehlerfreien registrierten Instances in einer oder mehreren Availability Zones weiter.

Sie können die Mindestanzahl von Availability Zones mithilfe des AvailabilityZones Parameters min in Ihren Regeln anpassen AWS Config

Weitere Informationen finden Sie unter Was ist Classic Load Balancer?.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz154`

Quelle

```
AWS Config Managed Rule: clb-multiple-az
```

Warnungskriterien

Gelb: Für den Classic Load Balancer ist kein Multi-AZ konfiguriert oder er erfüllt nicht die angegebene Mindestanzahl an AZs.

Empfohlene Aktion

Stellen Sie sicher, dass für Ihre Classic Load Balancer mehrere Availability Zones (AZs) konfiguriert sind. Verteilen Sie Ihren Load Balancer auf mehrere AZs, um sicherzustellen, dass Ihre Anwendung hochverfügbar ist.

Weitere Informationen finden Sie unter Tutorial: Erstellen eines Classic Load Balancer.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

ELB Connection Draining

Beschreibung

Prüft auf Load Balancer, bei denen Connection Draining nicht aktiviert ist.

Wenn Connection Draining nicht aktiviert ist und Sie eine Amazon EC2-Instance von einem Load Balancer abmelden, stellt der Load Balancer das Routing des Datenverkehrs zu dieser Instance ein und schließt die Verbindung. Wenn Connection Draining aktiviert ist, sendet der Load Balancer keine neuen Anfragen mehr an die abgemeldete Instance, hält aber die Verbindung offen, um aktive Anfragen zu bedienen.

Prüf-ID

```
7qGXsKIUw
```

Warnungskriterien

Gelb: Connection Draining ist für einen Load Balancer nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie Connection Draining für den Load Balancer. Weitere Informationen finden Sie unter Connection Draining und Enable or Disable Connection Draining for Your Load Balancer (Aktivieren oder Deaktivieren von Connection Draining für Ihren Load Balancer).

Weitere Ressourcen

Elastic Load Balancing Concepts (Konzepte für Elastic-Load-Balancing)

Berichtsspalten

- Status
- Region
- Load-Balancer-Name
- Grund

Load Balancer Optimization

Beschreibung

Prüft die Load Balancer-Konfiguration.

Um die Fehlertoleranz in Amazon Elastic Compute Cloud (Amazon EC2) bei der Verwendung von Elastic Load Balancing zu erhöhen, empfehlen wir, eine gleiche Anzahl von Instances über mehrere Availability Zones in einer Region zu betreiben. Ein konfigurierter Load Balancer ist kostenpflichtig, so dass es sich auch hier um eine Kostenoptimierungsprüfung handelt.

Prüf-ID

`iqdCTZKCUp`

Warnungskriterien

- Gelb: Ein Load Balancer ist für eine einzelne Availability Zone aktiviert.
- Gelb: Ein Load Balancer ist für eine Availability Zone aktiviert, die keine aktiven Instances hat.
- Gelb: Die Amazon-EC2-Instances, die bei einem Load Balancer registriert sind, sind ungleichmäßig über Availability Zones verteilt. Der Unterschied zwischen der höchsten und niedrigsten Anzahl von Instances in genutzten Availability Zones ist größer als 1 und beträgt mehr als 20 % der höchsten Anzahl).

Empfohlene Aktion

Stellen Sie sicher, dass Ihr Load Balancer auf aktive und fehlerfreie Instances in mindestens zwei Availability Zones verweist. Weitere Informationen finden Sie unter Hinzufügen von Availability Zones.

Wenn Ihr Load Balancer für eine Availability Zone ohne fehlerfreie Instances konfiguriert ist oder wenn Instances in den Availability Zones ungleich verteilt sind, stellen Sie fest, ob alle Availability Zones erforderlich sind. Lassen Sie unnötige Availability Zones weg und stellen Sie sicher, dass die Instances gleichmäßig über die verbleibenden Availability Zones verteilt sind. Weitere Informationen finden Sie unter Entfernen von Availability Zones.

Weitere Ressourcen

- Availability Zones and Regions (Regionen und Availability Zones)
- Managing Load Balancers (Verwalten von Load Balancern)
- Best Practices in Evaluating Elastic Load Balancing (Bewährte Methoden bei der Bewertung von Elastic-Load-Balancing)

Berichtsspalten

- Status
- Region
- Load-Balancer-Name
- Anzahl von Zonen
- Zone-A-Instances
- Zone-B-Instances
- Zone-C-Instances
- Zone-D-Instances
- Zone-E-Instances
- Zone-F-Instances
- Grund

NAT-Gateway-AZ-Unabhängigkeit

Beschreibung

Überprüft, ob Ihre NAT-Gateways mit Availability Zone (AZ)-Unabhängigkeit konfiguriert sind.

Ein NAT-Gateway ermöglicht es Ressourcen in Ihrem privaten Subnetz, mithilfe der IP-Adressen des NAT-Gateways eine sichere Verbindung zu Services außerhalb des Subnetzes herzustellen, und verwirft jeglichen unaufgeforderten eingehenden Datenverkehr. Jedes NAT-Gateway arbeitet innerhalb einer ausgewiesenen Availability Zone (AZ) und ist nur in dieser AZ mit Redundanz aufgebaut. Daher sollten Ihre Ressourcen in einer bestimmten AZ ein NAT-Gateway in derselben AZ verwenden, damit sich ein potenzieller Ausfall eines NAT-Gateways oder seiner AZ nicht auf Ihre Ressourcen in einer anderen AZ auswirkt.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfptbg10`

Warnungskriterien

- Rot: Der Datenverkehr von Ihrem Subnetz in einer AZ wird über ein NATGW in einer anderen AZ weitergeleitet.
- Grün: Der Datenverkehr von Ihrem Subnetz in einer AZ wird über ein NATGW in derselben AZ weitergeleitet.

Empfohlene Aktion

Überprüfen Sie die AZ Ihres Subnetzes und leiten Sie den Datenverkehr über ein NAT-Gateway in derselben AZ weiter.

Wenn es in der AZ kein NATGW gibt, erstellen Sie eines und leiten Sie dann Ihren Subnetz-Datenverkehr durch dieses weiter.

Wenn Sie dieselbe Routing-Tabelle allen Subnetzen in verschiedenen AZs zugeordnet haben, behalten Sie die Zuordnung dieser Routing-Tabelle zu den Subnetzen bei, die sich in derselben AZ wie das NAT-Gateway befinden. Verknüpfen Sie für Subnetze in der anderen AZ eine separate Routing-Tabelle mit einer Route zu einem NAT-Gateway in dieser anderen AZ.

Wir empfehlen, ein Wartungsfenster für Architekturänderungen in Ihrer Amazon VPC auszuwählen.

Weitere Ressourcen

- So erstellen Sie ein NAT-Gateway
- So konfigurieren Sie Routen für verschiedene NAT-Gateway-Anwendungsfälle

Berichtsspalten

- Status
- Region
- NAT-Availability-Zone
- NAT-ID
- Subnetz-Availability-Zone
- Subnetz-ID
- Routing-Tabellen-ID
- NAT-ARN
- Zeitpunkt der letzten Aktualisierung

Network Load Balancer – Zonenübergreifender Lastausgleich

Beschreibung

Prüft, ob zonenübergreifendes Load Balancing in Network Load Balancern aktiviert ist.

Das zonenübergreifende Load Balancing trägt dazu bei, eine gleichmäßige Verteilung des eingehenden Datenverkehrs auf Instances in verschiedenen Availability Zones aufrechtzuerhalten. Dadurch wird verhindert, dass der Load Balancer den gesamten Datenverkehr an Instances in derselben Availability Zone weiterleitet, was zu einer ungleichmäßigen Verteilung des Datenverkehrs und zu einer potenziellen Überlastung führen kann. Die Funktion erhöht auch die Anwendungszuverlässigkeit, weil der Datenverkehr bei einem Ausfall einer einzelnen Availability Zone automatisch an fehlerfreie Instances in anderen Availability Zones weitergeleitet wird.

Weitere Informationen finden Sie unter Zonenübergreifendes Load Balancing.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz105`

Quelle

`AWS Config Managed Rule: nlb-cross-zone-load-balancing-enabled`

Warnungskriterien

- Gelb: Im Network Load Balancer ist kein zonenübergreifendes Load Balancing aktiviert.

Empfohlene Aktion

Stellen Sie sicher, dass zonenübergreifendes Load Balancing in den Network Load Balancern aktiviert ist.

Weitere Ressourcen

Zonenübergreifendes Load Balancing (Network Load Balancer)

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

NLB — Mit dem Internet verbundene Ressource in einem privaten Subnetz

Beschreibung

Überprüft, ob ein mit dem Internet verbundener Network Load Balancer (NLB) mit einem privaten Subnetz konfiguriert ist. Ein mit dem Internet verbundener Network Load Balancer (NLB) muss in öffentlichen Subnetzen konfiguriert sein, um Datenverkehr empfangen zu können. Ein öffentliches Subnetz ist definiert als ein Subnetz, das eine direkte Route zu einem Internet-Gateway hat.

Wenn das Subnetz als privat konfiguriert ist, empfängt die Availability Zone (AZ) keinen Verkehr, was zu Verfügbarkeitsproblemen führen kann.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfpnchv4`

Warnungskriterien

Rot: NLB ist mit einem oder mehreren privaten Subnetzen konfiguriert

Grün: Es ist kein privates Subnetz für NLB mit Internetzugriff konfiguriert

Empfohlene Aktion

Stellen Sie sicher, dass die in einem mit dem Internet verbundenen Load Balancer konfigurierten Subnetze öffentlich sind. Ein öffentliches Subnetz ist definiert als ein Subnetz, das eine direkte Route zu einem Internet-Gateway hat. Verwenden Sie eine der folgenden Optionen:

- Erstellen Sie einen neuen Load Balancer und wählen Sie ein anderes Subnetz mit einer direkten Route zu einem Internet-Gateway aus.
- Ändern Sie das Subnetz, das derzeit mit dem Load Balancer verbunden ist, von privat auf öffentlich. Ändern Sie dazu die Routing-Tabelle und ordnen Sie ein Internet-Gateway zu.

Weitere Ressourcen

- Konfigurieren Sie einen Load Balancer und einen Listener
- Subnetze für Ihre VPC
- Ordnen Sie ein Gateway einer Routentabelle zu

Berichtsspalten

- Status
- Region
- NLB Arn

- NLB-Bezeichnung
- Subnetz-ID
- NLB-Schema
- Typ des Subnetzes
- Zeitpunkt der letzten Aktualisierung

NLB Multi-AZ

Beschreibung

Überprüft, ob Ihre Network Load Balancer so konfiguriert sind, dass sie mehr als eine Availability Zone (AZ) verwenden. Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Konfigurieren Sie Ihren Load Balancer in mehreren AZs in derselben Region, um Ihre Workload-Verfügbarkeit zu verbessern.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch09`

Warnungskriterien

Gelb: NLB befindet sich in einer einzigen AZ.

Grün: NLB hat zwei oder mehr AZs.

Empfohlene Aktion

Stellen Sie sicher, dass Ihr Load Balancer mit mindestens zwei Availability Zones konfiguriert ist.

Weitere Ressourcen

Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Availability Zones
- AWS Gut strukturiert — Stellen Sie den Workload an mehreren Standorten bereit
- Regionen und Availability Zones

Berichtsspalten

- Status
- Region
- Anzahl der AZs
- NLB ARN
- NLB-Name
- Zeitpunkt der letzten Aktualisierung

Nummer von AWS-Regionen in einem Incident Manager-Replikationssatz

Beschreibung

Überprüft, ob die Konfiguration eines Incident Manager-Replikationssatzes mehr als einen verwendet AWS-Region , um regionales Failover und regionale Reaktionen zu unterstützen. Für Vorfälle, die durch CloudWatch Alarme oder EventBridge Ereignisse verursacht werden, erstellt Incident Manager einen Vorfall auf dieselbe Weise AWS-Region wie der Alarm oder die Ereignisregel. Wenn Incident Manager in dieser Region vorübergehend nicht verfügbar ist, versucht das System, einen Vorfall in einer anderen Region im Replikationssatz zu erstellen. Wenn der Replikationssatz nur eine Region umfasst, kann das System keinen Vorfallsdatensatz erstellen, solange Incident Manager nicht verfügbar ist.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
cIdfp1js9r
```

Warnungskriterien

- Grün: Der Replikationssatz enthält mehr als eine Region.
- Gelb: Der Replikationssatz enthält eine Region.

Empfohlene Aktion

Fügen Sie dem Replikationssatz mindestens eine weitere Region hinzu.

Weitere Ressourcen

Weitere Informationen finden Sie unter Cross-region Incident management.

Berichtsspalten

- Status
- Regionsübergreifend
- Replikationssatz
- Zeitpunkt der letzten Aktualisierung

Einzelne AZ-Anwendungsprüfung

Beschreibung

Überprüft Netzwerkmuster dahingehend, ob Ihr ausgehender Netzwerkdatenverkehr über eine einzelne Availability Zone (AZ) geleitet wird.

Eine Availability Zone ist ein eigenständiger Standort, der vor allen Auswirkungen in anderen Zonen geschützt ist. Indem Sie Ihren Service auf mehrere AZs verteilen, begrenzen Sie den Wirkungsradius eines AZ-Ausfalls.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c1dfptbg11
```

Warnungskriterien

- Gelb: Ihre Anwendung kann basierend auf den beobachteten Netzwerkmustern für ausgehende Zugriffe möglicherweise nur in einer AZ bereitgestellt werden. Wenn dies zutrifft und Ihre Anwendung Hochverfügbarkeit erwartet, empfehlen wir Ihnen, Ihre Anwendungsressourcen bereitzustellen und Ihre Netzwerkabläufe so zu implementieren, dass mehrere Availability Zones genutzt werden.

Empfohlene Aktion

Wenn Ihre Anwendung Hochverfügbarkeit erfordert, sollten Sie die Implementierung einer Multi-AZ-Architektur für eine höhere Verfügbarkeit in Betracht ziehen.

Berichtsspalten

- Status
- Region
- VPC-ID
- Zeitpunkt der letzten Aktualisierung

VPC-Schnittstelle, Endpunkt-Netzwerkschnittstellen in mehreren AZs

Beschreibung

Überprüft, ob Ihre AWS PrivateLink VPC-Schnittstellenendpunkte so konfiguriert sind, dass sie mehr als eine Availability Zone (AZ) verwenden. Eine Availability Zone ist ein eigenständiger Standort, der vor Ausfällen in anderen Zonen geschützt ist. Dies unterstützt kostengünstige Netzwerkkonnektivität mit niedriger Latenz zwischen AZs in derselben Region. AWS Wählen Sie Subnetze in mehreren AZs aus, wenn Sie Schnittstellenendpunkte erstellen, um Ihre Anwendungen vor einem einzelnen Ausfallpunkt zu schützen.

> **Note**
>
> Diese Prüfung umfasst derzeit nur Schnittstellen-Endpunkte.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch10`

Warnungskriterien

Gelb: Der VPC-Endpunkt befindet sich in einer einzigen AZ.

Grün: Der VPC-Endpunkt befindet sich in mindestens zwei AZs.

Empfohlene Aktion

Stellen Sie sicher, dass Ihr VPC-Schnittstellenendpunkt mit mindestens zwei Availability Zones konfiguriert ist.

Weitere Ressourcen

Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Greifen Sie über einen VPC-Endpunkt mit einer Schnittstelle auf einen AWS Dienst zu
- Private IP-Adresse der Netzwerkschnittstelle des Endpunkts
- AWS PrivateLink Konzepte
- Regionen und Availability Zones

Berichtsspalten

- Status
- Region
- VPC-Endpunkt-ID
- Ist Multi AZ
- Zeitpunkt der letzten Aktualisierung

VPN-Tunnelredundanz

Beschreibung

Prüft die Anzahl der Tunnel, die für jedes Ihrer VPNs aktiv sind.

In einem VPN sollten immer zwei Tunnel konfiguriert sein. Dies bietet Redundanz im Falle eines Ausfalls oder einer geplanten Wartung der Geräte am AWS Endpunkt. Bei einigen Geräten ist jeweils nur ein Tunnel aktiv. Wenn ein VPN keine aktiven Tunnel hat, können trotzdem Gebühren für das VPN anfallen. Weitere Informationen finden Sie im AWS Client VPN Administratorhandbuch.

Prüf-ID

`S45wrEXrLz`

Warnungskriterien

- Gelb: Ein VPN hat einen aktiven Tunnel (das ist für einige Hardware normal).
- Gelb: Ein VPN hat keine aktiven Tunnel.

Empfohlene Aktion

Stellen Sie sicher, dass zwei Tunnel für Ihre VPN-Verbindung konfiguriert sind und dass beide aktiv sind, wenn Ihre Hardware dies unterstützt. Wenn Sie eine VPN-Verbindung nicht mehr benötigen, können Sie sie löschen, um Kosten zu vermeiden. Weitere Informationen finden Sie unter Ihr Kunden-Gateway oder Löschen einer VPN-Verbindung.

Weitere Ressourcen

- AWS Site-to-Site VPN VPN-Benutzerhandbuch
- Hinzufügen eines Hardware Virtual Private Gateway zu Ihrer VPC

Berichtsspalten

- Status
- Region
- VPN-ID
- VPC
- Virtual Private Gateway
- Kunden-Gateway
- Aktive Tunnel
- Grund

Redundanz der ActiveMQ-Availability-Zone

Beschreibung

Überprüft, ob Amazon MQ-für-ActiveMQ-Broker für Hochverfügbarkeit mit einem aktiven/Standby-Broker in mehreren Availability Zones konfiguriert sind.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1t3k8mqv1`

Warnungskriterien

- Gelb: Ein Amazon-MQ-for-ActiveMQ-Broker ist in einer einzelnen Availability Zone konfiguriert.

  Grün: Ein Amazon-MQ-for-ActiveMQ-Broker ist in mindestens zwei Availability Zones konfiguriert.

Empfohlene Aktion

Erstellen Sie einen neuen Broker mit aktivem/Standby-Bereitstellungsmodus.

Weitere Ressourcen

- Erstellen eines ActiveMQ-Brokers

Berichtsspalten

- Status
- Region
- ActiveMQ-Broker-ID
- Broker-Engine-Typ
- Bereitstellungsmodus
- Zeitpunkt der letzten Aktualisierung

RabbitMQ-Availability-Zone-Redundanz

Beschreibung

Überprüft, ob Amazon-MQ-for-RabbitMQ-Broker für Hochverfügbarkeit mit Cluster-Instances in mehreren Availability Zones konfiguriert sind.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1t3k8mqv2`

Warnungskriterien

- Gelb: Ein Amazon-MQ-for-RabbitMQ-Broker ist in einer einzelnen Availability Zone konfiguriert.

  Grün: Ein Amazon-MQ-for-RabbitMQ-Broker ist in mehreren Availability Zones konfiguriert.

Empfohlene Aktion

Erstellen Sie einen neuen Broker mit dem Cluster-Bereitstellungsmodus.

Weitere Ressourcen

- Erstellen eines RabbitMQ-Brokers

Berichtsspalten

- Status
- Region
- RabbitMQ-Broker-ID
- Broker-Engine-Typ
- Bereitstellungsmodus
- Zeitpunkt der letzten Aktualisierung

Service Limits

Siehe die folgenden Prüfungen für die Kategorie Leistungslimits (auch als Kontingente bekannt).

Alle Überprüfungen in dieser Kategorie haben die folgenden Beschreibungen:

Warnungskriterien

- Gelb: 80 % des Grenzwerts erreicht.
- Rot: 100 % des Grenzwerts erreicht.
- Blau: Trusted Advisor konnte die Auslastung oder Grenzwerte in einer oder mehreren AWS-Regionen nicht abrufen.

Empfohlene Aktion

Wenn Sie davon ausgehen, ein Service-Limit zu überschreiten, fordern Sie eine Erhöhung direkt bei der Konsole -Service Quotas an. Wenn Service Quotas Ihren Service noch nicht unterstützt, können Sie einen offenen Supportfall im Support-Center erstellen.

Berichtsspalten

- Status
- Service
- Region
- Limit-Betrag
- Aktuelle Nutzung

> **Note**
>
> - Die Werte basieren auf einer Snapshots, so dass Ihre aktuelle Nutzung abweichen kann. Es kann bis zu 24 Stunden dauern, bis die Kontingent- und Nutzungsdaten Änderungen widerspiegeln. In Fällen, in denen die Kontingente kürzlich erhöht wurden, kann es vorkommen, dass die Auslastung vorübergehend das Kontingent übersteigt.

Namen prüfen

- Auto Scaling-Gruppen
- Auto-Scaling-Startkonfiguration

- CloudFormation Stapel
- DynamoDB Lesekapazität
- DynamoDB Schreibkapazität
- EBS aktive Snapshots
- EBS kalter HDD (sc1) Volume-Speicher
- EBS universeller SSD (gp2) Volume-Speicher
- EBS universeller SSD (gp3) Volume-Speicher
- EBS magnetischer (Standard)-Volume-Speicher
- EBS bereitgestelltes IOPS (SSD) Volume-Aggregate IOPS
- EBS bereitgestellte IOPS SSD (io1)-Volume-Speicher
- EBS Bereitgestellter IOPS SSD (io2)-Volume-Speicher
- EBS durchsatzoptimierter HDD (st1) Volume-Speicher
- EC2 On-Demand-Instances
- EC2 Reserved Instance Leases
- EC2-Classic Elastic IP-Adressen
- EC2-VPC Elastic IP-Adresse
- ELB Application Load Balancers
- ELB Classic Load Balancers
- ELB Network Load Balancers
- IAM-Gruppe
- IAM-Instance-Profile
- IAM-Richtlinien
- IAM-Rollen
- IAM-Serverzertifikate
- IAM-Benutzer
- Kinesis Shards pro Region
- Nutzung des Lambda-Codespeichers
- RDS-Cluster-Parametergruppen

- RDS-Clusterrollen
- RDS-Cluster
- RDS-DB-Instances
- RDS DB manuelle Snapshots
- RDS-DB-Parametergruppen
- RDS-DB-Sicherheitsgruppe
- RDS-Ereignisabonnements
- RDS Max Auths pro Sicherheitsgruppe
- RDS-Optionsgruppen
- RDS Lese-Replikate pro Master
- RDS Reserved Instances
- RDS Subnetzgruppen
- RDS-Subnetze pro Subnetzgruppe
- RDS-Gesamtspeicherkontingent
- Route 53 gehostete Zonen
- Route 53 Max. Zustandsprüfungen
- Route 53 Wiederverwendbare Delegationssätze
- Route 53-Verkehrsrichtlinien
- Route 53-Verkehrsrichtlinien-Instances
- SES täglich versendetes Kontingent
- VPC
- VPC-Internet-Gateways

Auto Scaling-Gruppen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für Auto-Scaling-Gruppen beträgt.

Prüf-ID

`fW7HH0l7J9`

Weitere Ressourcen

Auto-Scaling-Kontingente

Auto-Scaling-Startkonfiguration

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für Auto-Scaling-Startkonfigurationen beträgt.

Prüf-ID

`aW7HH0l7J9`

Weitere Ressourcen

Auto-Scaling-Kontingente

CloudFormation Stapel

Beschreibung

Prüft, ob die Nutzung mehr als 80% des CloudFormation Stack-Kontingents beträgt.

Prüf-ID

`gW7HH0l7J9`

Weitere Ressourcen

AWS CloudFormation-Kontingente

DynamoDB Lesekapazität

Beschreibung

Prüft auf eine Nutzung, die mehr als 80 % der DynamoDB-Durchsatzgrenze für Lesevorgänge pro AWS-Konto.

Prüf-ID

`6gtQddfEw6`

Weitere Ressourcen

DynamoDB-Kontingente

DynamoDB Schreibkapazität

Beschreibung

Prüft auf eine Nutzung, die mehr als 80 % der DynamoDB-Durchsatzgrenze für Schreibvorgänge pro AWS-Konto.

Prüf-ID

`c5ftjdfkMr`

Weitere Ressourcen

DynamoDB-Kontingente

EBS aktive Snapshots

Beschreibung

Prüft, ob mehr als 80 % des Kontingents für aktive EBS-Snapshots verwendet werden.

Prüf-ID

`eI7KK0l7J9`

Weitere Ressourcen

Limits für Amazon EBS

EBS kalter HDD (sc1) Volume-Speicher

Beschreibung

Prüft, ob mehr als 80 % des EBS kalten HDD (sc1)-Volume-Speicherplatzkontingents genutzt werden.

Prüf-ID

`gH5CC0e3J9`

Weitere Ressourcen

Limits für Amazon EBS

EBS universeller SSD (gp2) Volume-Speicher

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des EBS unversellen SSD (gp2)-Volume-Speicheranteils beträgt.

Prüf-ID

dH7RR0l6J9

Weitere Ressourcen

Limits für Amazon EBS

EBS universeller SSD (gp3) Volume-Speicher

Beschreibung

Prüft,a ob mehr als 80 % des EBS universellen SSD (gp3)-Volume-Speicherplatzkontingents genutzt werden.

Prüf-ID

dH7RR0l6J3

Weitere Ressourcen

Limits für Amazon EBS

EBS magnetischer (Standard)-Volume-Speicher

Beschreibung

Prüft, ob mehr als 80 % des Speicherkontingents des EBS magnetischen (Standard)-Volume genutzt werden.

Prüf-ID

cG7HH0l7J9

Weitere Ressourcen

Limits für Amazon EBS

EBS bereitgestelltes IOPS (SSD) Volume-Aggregate IOPS

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Gesamt-IOPS-des Kontingents des EBS bereitgestellten IOPS (SSD)-Volume beträgt.

Prüf-ID

`tV7YY0l7J9`

Weitere Ressourcen

Limits für Amazon EBS

EBS bereitgestellte IOPS SSD (io1)-Volume-Speicher

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des EBS bereitgestellten IOPS SSD (io1) Volume-Speicherkontingents beträgt.

Prüf-ID

`gI7MM0l7J9`

Weitere Ressourcen

Limits für Amazon EBS

EBS Bereitgestellter IOPS SSD (io2)-Volume-Speicher

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des EBS bereitgestellten IOPS SSD (io2) Volume-Speicherkontingents beträgt.

Prüf-ID

`gI7MM0l7J2`

Weitere Ressourcen

Limits für Amazon EBS

EBS durchsatzoptimierter HDD (st1) Volume-Speicher

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des EBS durchsatzoptimierten HDD (st1) Volume-Speicherkontingents beträgt.

Prüf-ID

`wH7DD0l3J9`

Weitere Ressourcen

Limits für Amazon EBS

EC2 On-Demand-Instances

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für EC2 On-Demand-Instances beträgt.

Prüf-ID

`0Xc6LMYG8P`

Weitere Ressourcen

Amazon-EC2-Kontingente

EC2 Reserved Instance Leases

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der EC2 Reserved Instance Leases beträgt.

Prüf-ID

`iH7PP0l7J9`

Weitere Ressourcen

Amazon-EC2-Kontingente

EC2-Classic Elastic IP-Adressen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für EC2-Classic Elastic IP-Adressen beträgt.

Prüf-ID

`aW9HH0l8J6`

Weitere Ressourcen

Amazon-EC2-Kontingente

EC2-VPC Elastic IP-Adresse

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des EC2-VPC-Kontingents für elastische IP-Adressen beträgt.

Prüf-ID

`lN7RR0l7J9`

Weitere Ressourcen

VPC-Elastic-IP-Kontingente

ELB Application Load Balancers

Beschreibung

Überprüft, ob die Nutzung mehr als 80 % des Kontingents der ELB Application Load Balancer beträgt.

Prüf-ID

`EM8b3yLRTr`

Weitere Ressourcen

- Elastic-Load-Balancing-Kontingente

ELB Classic Load Balancers

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der ELB Classic Load Balancer beträgt.

Prüf-ID

`iK7O00l7J9`

Weitere Ressourcen

- Elastic-Load-Balancing-Kontingente

ELB Network Load Balancers

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der ELB Network Load Balancer beträgt.

Prüf-ID

`8wIqYSt25K`

Weitere Ressourcen

- Elastic-Load-Balancing-Kontingente

IAM-Gruppe

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des IAM-Gruppenkontingents beträgt.

Prüf-ID

`sU7XX0l7J9`

Weitere Ressourcen

- IAM-Kontingente

IAM-Instance-Profile

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der IAM-Instance-Profile beträgt.

Prüf-ID

n07SS0l7J9

Weitere Ressourcen

IAM-Kontingente

IAM-Richtlinien

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der IAM-Richtlinien beträgt.

Prüf-ID

pR7UU0l7J9

Weitere Ressourcen

IAM-Kontingente

IAM-Rollen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des IAM-Rollenkontingents beträgt.

Prüf-ID

oQ7TT0l7J9

Weitere Ressourcen

IAM-Kontingente

IAM-Serverzertifikate

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für IAM-Server-Zertifikate beträgt.

Prüf-ID

`rT7WW0l7J9`

Weitere Ressourcen

IAM-Kontingente

IAM-Benutzer

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des IAM-Benutzerkontingents beträgt.

Prüf-ID

`qS7VV0l7J9`

Weitere Ressourcen

IAM-Kontingente

Kinesis Shards pro Region

Beschreibung

Prüft, ob die Nutzung mehr als 80 % der Kinesis Shards pro Region beträgt.

Prüf-ID

`bW7HH0l7J9`

Weitere Ressourcen

Kinesis-Kontingente

Nutzung des Lambda-Codespeichers

Beschreibung

Prüft, ob die Nutzung des Codespeichers mehr als 80 % des Kontolimits beträgt.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c1dfprch07`

Warnungskriterien

- Gelb: 80 % des Grenzwerts erreicht.

Empfohlene Aktion

Bitte identifizieren Sie ungenutzte Lambda-Funktionen oder -Versionen und entfernen Sie sie, um den Codespeicher für Ihr Konto in der Region freizugeben. Wenn Sie zusätzlichen Speicherplatz benötigen, erstellen Sie bitte im Support-Center einen Supportfall. Wenn Sie davon ausgehen, ein Service-Limit zu überschreiten, fordern Sie eine Erhöhung direkt bei der Konsole -Service Quotas an. Wenn Service Quotas Ihren Service noch nicht unterstützt, können Sie einen offenen Supportfall im Support-Center erstellen.

Weitere Ressourcen

- Nutzung des Lambda-Codespeichers

Berichtsspalten

- Status
- Region
- Die qualifizierte Funktions-ARN für diese Ressource.
- Die Speichernutzung des Funktionscodes MegaBytes mit 2 Dezimalstellen.
- Die Anzahl der Versionen in der Funktion

- Zeitpunkt der letzten Aktualisierung

RDS-Cluster-Parametergruppen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Cluster-Parametergruppenkontingents beträgt.

Prüf-ID

`jtlIMO3qZM`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Clusterrollen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Clusterrollenkontingents beträgt.

Prüf-ID

`7fuccf1Mx7`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Cluster

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Clusterkontingents beträgt.

Prüf-ID

`gjqMBn6pjz`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-DB-Instances

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-DB-Instances-Kontingents beträgt.

Prüf-ID

`XG0aXHpIEt`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS DB manuelle Snapshots

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für RDS-DB manuelle Snapshots beträgt.

Prüf-ID

`dV84wpqRUs`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-DB-Parametergruppen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-DB-Parametergruppenkontingents beträgt.

Prüf-ID

`jEECYg2YVU`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-DB-Sicherheitsgruppe

Beschreibung

Prüft, ob die Nutzung mehr als 80% des RDS-DB-Sicherheitsgruppenkontingents beträgt.

Prüf-ID

`gfZAn3W7wl`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Ereignisabonnements

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Ereignisabonnementkontingents beträgt.

Prüf-ID

`keAhfbH5yb`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS Max Auths pro Sicherheitsgruppe

Beschreibung

Überprüft, ob die Nutzung mehr als 80 % des RDS Max Auths pro Sicherheitsgruppenkontingent beträgt.

Prüf-ID

`dBkuNCvqn5`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Optionsgruppen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Optionsgruppenkontingents beträgt.

Prüf-ID

`3Njm0DJQO9`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS Lese-Replikate pro Master

Beschreibung

Prüft, ob die Nutzung mehr als 80 % der RDS-Lese-Replikate pro Master-Kontingent beträgt.

Prüf-ID

`pYW8UkYz2w`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS Reserved Instances

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS Reserved Instances-Kontingents beträgt.

Prüf-ID

`UUDv0a5r34`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS Subnetzgruppen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Subnetzgruppenkontingents beträgt.

Prüf-ID

`dYWBaXaaMM`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Subnetze pro Subnetzgruppe

Beschreibung

Prüft, ob die Nutzung mehr als 80 % der RDS-Subnetze pro Subnetzgruppe ausmacht.

Prüf-ID

`jEhCtdJK0Y`

Weitere Ressourcen

Amazon-RDS-Kontingente

RDS-Gesamtspeicherkontingent

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des RDS-Gesamtspeicherkontingents beträgt.

Prüf-ID

`P1jhKWEmLa`

Weitere Ressourcen

Amazon-RDS-Kontingente

Route 53 gehostete Zonen

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents für gehostete Route 53-Zonen pro Konto beträgt.

Prüf-ID

`dx3xfcdfMr`

Weitere Ressourcen

Route-53-Kontingente

Route 53 Max. Zustandsprüfungen

Beschreibung

Überprüft, ob die Nutzung mehr als 80 % des Route 53-Zustandsprüfungskontingents pro Konto beträgt.

Prüf-ID

`ru4xfcdfMr`

Weitere Ressourcen

Route-53-Kontingente

Route 53 Wiederverwendbare Delegationssätze

Beschreibung

Prüft, ob die Nutzung mehr als 80 % der wiederverwendbaren Route 53-Delegation beträgt, und legt das Kontingent pro Konto fest.

Prüf-ID

`ty3xfcdfMr`

Weitere Ressourcen

Route-53-Kontingente

Route 53-Verkehrsrichtlinien

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der Route 53-Verkehrsrichtlinien pro Konto beträgt.

Prüf-ID

`dx3xfbjfMr`

Weitere Ressourcen

Route-53-Kontingente

Route 53-Verkehrsrichtlinien-Instances

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der Route 53-Verkehrsrichtlinien-Instances pro Konto beträgt.

Prüf-ID

`dx8afcdfMr`

Weitere Ressourcen

Route-53-Kontingente

SES täglich versendetes Kontingent

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des täglichen Amazon SES-Sendekontingents beträgt.

Prüf-ID

`hJ7NN0l7J9`

Weitere Ressourcen

Amazon-SES-Kontingente

VPC

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des VPC-Kontingents beträgt.

Prüf-ID

`jL7PP0l7J9`

Weitere Ressourcen

VPC-Kontingente

VPC-Internet-Gateways

Beschreibung

Prüft, ob die Nutzung mehr als 80 % des Kontingents der VPC-Internet-Gateways beträgt.

Prüf-ID

`kM7QQ0l7J9`

Weitere Ressourcen

VPC-Kontingente

Operative Exzellenz

Sie können die folgenden Prüfungen für die operative Exzellenz verwenden.

Namen prüfen

- Amazon API Gateway protokolliert keine Ausführungsprotokolle
- Amazon-API-Gateway-REST-APIs ohne aktivierte X-Ray-Ablaufverfolgung
- Amazon CloudFront Access Log konfiguriert
- Amazon CloudWatch Alarm Action ist deaktiviert
- Amazon EC2 EC2-Instance wird nicht verwaltet von AWS Systems Manager
- Amazon-ECR-Repository mit deaktivierter Unveränderlichkeit von Tags
- Amazon-ECS-Cluster mit Container Insights ist deaktiviert
- Amazon-ECS-Aufgabenprotokollierung ist nicht aktiviert

- Amazon OpenSearch Service-Protokollierung CloudWatch nicht konfiguriert
- Amazon RDS-DB-Instances in den Clustern mit heterogenen Parametergruppen
- Amazon RDS Enhanced Monitoring ist ausgeschaltet
- Amazon RDS Performance Insights ist ausgeschaltet
- Der Amazon RDS-Parameter track_counts ist ausgeschaltet
- Amazon-Redshift-Cluster-Auditprotokollierung
- In Amazon S3 sind keine Ereignisbenachrichtigungen aktiviert
- Amazon-SNS-Themen: Nachrichtenzustellungsstatus wird nicht protokolliert
- Amazon VPC ohne Flow-Protokolle
- Application Load Balancer und Classic Load Balancer ohne aktivierte Zugriffsprotokolle
- AWS CloudFormation Stack-Benachrichtigung
- AWS CloudTrail Protokollierung von Datenereignissen für Objekte in einem S3-Bucket
- AWS CodeBuild Protokollierung von Projekten
- AWS CodeDeploy Automatisches Rollback und Monitor aktiviert
- AWS CodeDeploy Lambda verwendet die all-at-once Bereitstellungskonfiguration
- AWS Elastic Beanstalk Enhanced Health Reporting ist nicht konfiguriert
- AWS Elastic Beanstalk mit deaktivierten verwalteten Plattform-Updates
- AWS Fargate Die Plattformversion ist nicht aktuell
- AWS Systems Manager State Manager Association hat den Status „Nichtkonformität“
- CloudTrail Trails sind nicht mit Amazon CloudWatch Logs konfiguriert
- Elastic-Load-Balancing-Löschschutz ist für Load Balancer nicht aktiviert
- Prüfung des Löschschutzes von RDS-DB-Clustern
- RDS-DB-Instance – Prüfung auf automatisches Upgrade für Unterversion

Amazon API Gateway protokolliert keine Ausführungsprotokolle

Beschreibung

Prüft, ob bei Amazon API Gateway CloudWatch Logs auf der gewünschten Protokollierungsebene aktiviert sind.

Aktivieren Sie die CloudWatch Protokollierung für REST-API-Methoden oder WebSocket API-Routen in Amazon API Gateway, um CloudWatch Ausführungsprotokolle für Anfragen, die

von Ihren APIs empfangen wurden, in Logs zu sammeln. Die in den Ausführungsprotokollen enthaltenen Informationen helfen Ihnen dabei, Probleme im Zusammenhang mit Ihrer API zu identifizieren und zu beheben.

Sie können die ID der Protokollierungsebene (ERROR, INFO) im Parameter LoggingLevel in den AWS Config Regeln angeben.

Weitere Informationen zur CloudWatch Anmeldung bei Amazon WebSocket API Gateway finden Sie in der REST-API oder API-Dokumentation.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz125`

Quelle

`AWS Config Managed Rule: api-gw-execution-logging-enabled`

Warnungskriterien

Gelb: Die CloudWatch Protokollierungseinstellung für die Erfassung von Ausführungsprotokollen ist auf der gewünschten Protokollierungsebene für ein Amazon API Gateway nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die CloudWatch Protokollierung für Ausführungsprotokolle für Ihre Amazon API Gateway Gateway-REST-APIs oder WebSocket APIs mit der entsprechenden Protokollierungsebene (ERROR, INFO).

Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls.

Weitere Ressourcen

- CloudWatch Protokollierung für eine REST-API in API Gateway einrichten
- Konfiguration der Protokollierung für eine WebSocket API

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-API-Gateway-REST-APIs ohne aktivierte X-Ray-Ablaufverfolgung

Beschreibung

Prüft, ob die Amazon API Gateway Gateway-REST-APIs AWS X-Ray die Ablaufverfolgung aktiviert haben.

Aktivieren Sie die X-Ray-Ablaufverfolgung für Ihre REST-APIs, damit API Gateway API-Aufrufanforderungen mit Ablaufverfolgungsinformationen testen kann. Auf diese Weise können Sie Anfragen verfolgen und analysieren AWS X-Ray , während sie über Ihre API-Gateway-REST-APIs zu den nachgelagerten Diensten übertragen werden.

Weitere Informationen finden Sie unter Ablaufverfolgung von Benutzeranforderungen an REST-APIs mithilfe von X-Ray.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz126
```

Quelle

```
AWS Config Managed Rule: api-gw-xray-enabled
```

Warnungskriterien

Gelb: Die X-Ray-Ablaufverfolgung ist für eine API-Gateway-REST-API nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die X-Ray-Ablaufverfolgung für Ihre API-Gateway-REST-APIs.

Weitere Informationen finden Sie unter Einrichtung AWS X-Ray mit API Gateway Gateway-REST-APIs.

Weitere Ressourcen

- Ablaufverfolgung von Benutzeranforderungen an REST-APIs mithilfe von X-Ray
- Was ist AWS X-Ray?

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon CloudFront Access Log konfiguriert

Beschreibung

Prüft, ob CloudFront Amazon-Distributionen so konfiguriert sind, dass sie Informationen aus Amazon S3-Serverzugriffsprotokollen erfassen. Die Amazon S3 S3-Serverzugriffsprotokolle enthalten detaillierte Informationen zu jeder eingehenden CloudFront Benutzeranfrage.

Sie können den Namen des Amazon S3 S3-Buckets zum Speichern von Serverzugriffsprotokollen mithilfe des BucketNameS3-Parameters in Ihren AWS Config Regeln anpassen.

Weitere Informationen finden Sie unter Konfigurieren und Verwenden von Standardprotokollen (Zugriffsprotokollen).

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz110`

Quelle

`AWS Config Managed Rule: cloudfront-accesslogs-enabled`

Warnungskriterien

Gelb: Die CloudFront Amazon-Zugriffsprotokollierung ist nicht aktiviert

Empfohlene Aktion

Stellen Sie sicher, dass Sie die CloudFront Zugriffsprotokollierung aktivieren, um detaillierte Informationen zu jeder eingehenden Benutzeranfrage zu CloudFront erfassen.

Sie können Standardprotokolle aktivieren, wenn Sie eine Verteilung erstellen oder aktualisieren.

Weitere Informationen finden Sie unter Werte, die Sie beim Erstellen oder Aktualisieren einer Verteilung angeben.

Weitere Ressourcen

- Werte, die Sie beim Erstellen oder Aktualisieren einer Verteilung angeben
- Konfigurieren und Verwenden von Standardprotokollen (Zugriffsprotokollen)

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon CloudWatch Alarm Action ist deaktiviert

Beschreibung

Überprüft, ob Ihre CloudWatch Amazon-Alarmaktion deaktiviert ist.

Sie können AWS CLI die Aktionsfunktion in Ihrem Alarm aktivieren oder deaktivieren. Oder Sie können die Aktionsfunktion mithilfe des AWS SDK programmgesteuert deaktivieren oder aktivieren. Wenn die Alarmaktionsfunktion ausgeschaltet ist, führt CloudWatch sie in keinem Zustand (OK, INSUFFICIENT_DATA, ALARM) eine definierte Aktion aus.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz109`

Quelle

`AWS Config Managed Rule: cloudwatch-alarm-action-enabled-check`

Warnungskriterien

Gelb: Die CloudWatch Amazon-Alarmaktion ist nicht aktiviert. In keinem Alarmzustand wird eine Aktion ausgeführt.

Empfohlene Aktion

Aktivieren Sie Aktionen in Ihren CloudWatch Alarmen, es sei denn, Sie haben einen triftigen Grund, sie zu deaktivieren, z. B. zu Testzwecken.

Wenn der CloudWatch Alarm nicht mehr benötigt wird, löschen Sie ihn, um unnötige Kosten zu vermeiden.

Weitere Informationen finden Sie unter enable-alarm-actions in der AWS CLI Befehlsreferenz und unter func (*CloudWatch) EnableAlarmActions in der AWS SDK for Go API-Referenz.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon EC2 EC2-Instance wird nicht verwaltet von AWS Systems Manager

Beschreibung

Überprüft, ob die Amazon EC2 EC2-Instances in Ihrem Konto von AWS Systems Manager verwaltet werden.

Systems Manager hilft Ihnen dabei, den aktuellen Status Ihrer Amazon-EC2-Instance und Betriebssystemkonfigurationen zu verstehen und zu kontrollieren. Mit Systems Manager können Sie Softwarekonfigurations- und Bestandsinformationen zu Ihrer Flotte von Instances, einschließlich der darauf installierten Software, erfassen. Auf diese Weise können Sie detaillierte Informationen zu Systemkonfigurationen, Betriebssystem-Patch-Levels, Anwendungskonfigurationen und andere Details zu Ihrer Bereitstellung verfolgen.

Weitere Informationen finden Sie unter Einrichtung von Systems Manager für EC2-Instances.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz145
```

Quelle

```
AWS Config Managed Rule: ec2-instance-managed-by-systems-manager
```

Warnungskriterien

Gelb: Die Amazon-EC2-Instances werden nicht von Systems Manager verwaltet.

Empfohlene Aktion

Konfigurieren Sie Ihre Amazon-EC2-Instance für die Verwaltung durch Systems Manager.

Dieser Scheck kann nicht aus der Ansicht in der Trusted Advisor Konsole ausgeschlossen werden.

Weitere Informationen finden Sie unter Warum wird meine EC2-Instance nicht als verwalteter Knoten angezeigt oder hat den Status „Verbindung getrennt“ in Systems Manager?.

Weitere Ressourcen

Einrichtung von Systems Manager für EC2-Instances

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-ECR-Repository mit deaktivierter Unveränderlichkeit von Tags

Beschreibung

Prüft, ob in einem privaten Amazon-ECR-Repository die Unveränderlichkeit von Image-Tags aktiviert ist.

Aktivieren Sie die Unveränderlichkeit von Image-Tags für ein privates Amazon-ECR-Repository, um zu verhindern, dass Image-Tags überschrieben werden. So können Sie beschreibende Tags als zuverlässigen Mechanismus zur Nachverfolgung und eindeutigen Identifizierung von Images nutzen. Wenn beispielsweise die Unveränderlichkeit von Image-Tags aktiviert ist, können Benutzer ein Image-Tag zuverlässig verwenden, um eine bereitgestellte Image-Version mit dem Build zu korrelieren, der das Image erzeugt hat.

Weitere Informationen finden Sie unter Veränderlichkeit der Image-Tags.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz129`

Quelle

`AWS Config Managed Rule: ecr-private-tag-immutability-enabled`

Warnungskriterien

Gelb: In einem privaten Amazon-ECR-Repository ist die Unveränderlichkeit von Tags nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die Unveränderlichkeit von Image-Tags für Ihre privaten Amazon-ECR-Repositorys.

Weitere Informationen finden Sie unter Veränderlichkeit der Image-Tags.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-ECS-Cluster mit Container Insights ist deaktiviert

Beschreibung

Prüft, ob Amazon CloudWatch Container Insights für Ihre Amazon ECS-Cluster aktiviert ist.

CloudWatch Container Insights sammelt, aggregiert und fasst Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices zusammen. Die Metriken umfassen die Auslastung für Ressourcen wie z B. CPU, Arbeitsspeicher, Datenträger und Netzwerk.

Weitere Informationen finden Sie unter Amazon ECS CloudWatch Container Insights.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz173`

Quelle

`AWS Config Managed Rule: ecs-container-insights-enabled`

Warnungskriterien

Gelb: Für den Amazon-ECS-Cluster sind Container Insights nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie CloudWatch Container Insights auf Ihren Amazon ECS-Clustern.

Weitere Informationen finden Sie unter Verwenden von Container Insights.

Weitere Ressourcen

Einblicke in Amazon ECS CloudWatch Container

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-ECS-Aufgabenprotokollierung ist nicht aktiviert

Beschreibung

Prüft, ob die Protokollkonfiguration für aktive Amazon-ECS-Aufgabendefinitionen festgelegt ist.

Durch die Überprüfung der Protokollkonfiguration in Ihren Amazon-ECS-Aufgabendefinitionen wird sichergestellt, dass die von Containern generierten Protokolle ordnungsgemäß konfiguriert sind und korrekt gespeichert werden. Dies hilft Ihnen dabei, Probleme schneller zu identifizieren und zu beheben, die Leistung zu optimieren und Compliance-Anforderungen zu erfüllen.

Standardmäßig zeigen die erfassten Protokolle die Befehlsausgabe an, die Sie normalerweise in einem interaktiven Terminal sehen, wenn Sie den Container lokal ausführen. Der awslogs-Treiber leitet diese Protokolle von Docker an Amazon Logs weiter. CloudWatch

Weitere Informationen finden Sie unter Verwenden des awslogs-Protokolltreibers.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz175
```

Quelle

```
AWS Config Managed Rule: ecs-task-definition-log-configuration
```

Warnungskriterien

Gelb: Die Amazon-ECS-Aufgabendefinition hat keine Protokollierungskonfiguration.

Empfohlene Aktion

Erwägen Sie, die Konfiguration des Protokolltreibers in der Container-Definition anzugeben, um Protokollinformationen an CloudWatch Logs oder einen anderen Protokollierungstreiber zu senden.

Weitere Informationen finden Sie unter LogConfiguration.

Weitere Ressourcen

Erwägen Sie, die Protokolltreiberkonfiguration in der Container-Definition anzugeben, um Protokollinformationen an CloudWatch Logs oder einen anderen Protokollierungstreiber zu senden.

Weitere Informationen finden Sie unter Beispiel für Aufgabendefinitionen.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon OpenSearch Service-Protokollierung CloudWatch nicht konfiguriert

Beschreibung

Prüft, ob Amazon OpenSearch Service-Domains so konfiguriert sind, dass sie Protokolle an Amazon CloudWatch Logs senden.

Die Überwachung von Protokollen ist entscheidend für die Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung des OpenSearch Service.

Protokolle für langsame Suchen, Protokolle für langsame Indizierung und Fehlerprotokolle sind für die Problembehandlung bei Leistungs- und Stabilitätsproblemen Ihrer Workload nützlich. Diese Protokolle müssen aktiviert sein, um Daten zu erfassen.

Sie können mithilfe des LogTypes-Parameters in Ihren AWS Config Regeln angeben, welche Protokolltypen Sie filtern möchten (Fehler, Suche, Index).

Weitere Informationen finden Sie unter Amazon OpenSearch Service-Domains überwachen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz184`

Quelle

`AWS Config Managed Rule: opensearch-logs-to-cloudwatch`

Warnungskriterien

Gelb: Amazon OpenSearch Service hat keine Protokollierungskonfiguration mit Amazon CloudWatch Logs

Empfohlene Aktion

Konfigurieren Sie OpenSearch Service-Domains so, dass sie CloudWatch Protokolle in Logs veröffentlichen.

Weitere Informationen finden Sie unter Aktivieren der Veröffentlichung von Protokollen (Konsole).

Weitere Ressourcen

- Überwachung von OpenSearch Service-Cluster-Metriken mit Amazon CloudWatch

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon RDS-DB-Instances in den Clustern mit heterogenen Parametergruppen

Beschreibung

Wir empfehlen, dass alle DB-Instances im DB-Cluster dieselbe DB-Parametergruppe verwenden.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt010`

Warnungskriterien

Gelb: DB-Cluster haben DB-Instances mit heterogenen Parametergruppen.

Empfohlene Aktion

Ordnen Sie die DB-Instance der DB-Parametergruppe zu, die der Writer-Instance in Ihrem DB-Cluster zugeordnet ist.

Weitere Ressourcen

Wenn die DB-Instances in Ihrem DB-Cluster unterschiedliche DB-Parametergruppen verwenden, kann es während eines Failovers zu einem inkonsistenten Verhalten oder zu Kompatibilitätsproblemen zwischen den DB-Instances in Ihrem DB-Cluster kommen.

Weitere Informationen finden Sie unter Arbeiten mit Parametergruppen.

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon RDS Enhanced Monitoring ist ausgeschaltet

Beschreibung

Für Ihre Datenbankressourcen ist Enhanced Monitoring nicht aktiviert. Erweiterte Überwachung bietet Echtzeit-Betriebssystemmetriken für die Überwachung und Fehlerbehebung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
>
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt004`

Warnungskriterien

Gelb: Für Amazon RDS-Ressourcen ist Enhanced Monitoring nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die erweiterte Überwachung.

Weitere Ressourcen

Enhanced Monitoring for Amazon RDS bietet zusätzlichen Einblick in den Zustand Ihrer DB-Instances. Wir empfehlen, Enhanced Monitoring zu aktivieren. Wenn die Option Enhanced Monitoring für Ihre DB-Instance aktiviert ist, sammelt sie wichtige Betriebssystemmetriken und Prozessinformationen.

Weitere Informationen finden Sie unter Überwachen von Betriebssystem-Metriken mithilfe von „Erweitere Überwachung“.

Berichtsspalten

- Status
- Region
- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Amazon RDS Performance Insights ist ausgeschaltet

Beschreibung

Amazon RDS Performance Insights überwacht die Auslastung Ihrer DB-Instance, um Sie bei der Analyse und Lösung von Datenbankleistungsproblemen zu unterstützen. Wir empfehlen, Performance Insights zu aktivieren.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt012`

Warnungskriterien

Gelb: Bei Amazon RDS-Ressourcen ist Performance Insights nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie Performance Insights.

Weitere Ressourcen

Performance Insights verwendet eine einfache Datenerfassungsmethode, die die Leistung Ihrer Anwendungen nicht beeinträchtigt. Performance Insights hilft Ihnen dabei, die Datenbanklast schnell einzuschätzen.

Weitere Informationen finden Sie unter Überwachen der DB-Auslastung mit Performance Insights auf Amazon RDS.

Berichtsspalten

- Status
- Region

- Ressource
- Empfohlener Wert
- Name des Motors
- Zeitpunkt der letzten Aktualisierung

Der Amazon RDS-Parameter track_counts ist ausgeschaltet

Beschreibung

Wenn der Parameter track_counts ausgeschaltet ist, sammelt die Datenbank keine Statistiken zur Datenbankaktivität. Autovacuum erfordert, dass diese Statistiken korrekt funktionieren.

Wir empfehlen, den Parameter track_counts auf 1 zu setzen

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

> **Note**
>
> Wenn eine DB-Instance oder ein DB-Cluster gestoppt wird, können Sie sich die Amazon RDS-Empfehlungen innerhalb von 3 bis 5 Tagen ansehen. Trusted Advisor Nach fünf Tagen sind die Empfehlungen nicht mehr verfügbar Trusted Advisor. Um die Empfehlungen anzuzeigen, öffnen Sie die Amazon RDS-Konsole und wählen Sie dann Empfehlungen.
> Wenn Sie eine DB-Instance oder einen DB-Cluster löschen, sind die mit diesen Instances oder Clustern verknüpften Empfehlungen weder in der Amazon RDS-Managementkonsole noch in Trusted Advisor der Amazon RDS-Managementkonsole verfügbar.

Prüf-ID

`c1qf5bt027`

Warnungskriterien

Gelb: Bei DB-Parametergruppen ist der Parameter track_counts ausgeschaltet.

Empfohlene Aktion

Setzen Sie den Parameter track_counts auf 1

Weitere Ressourcen

Wenn der Parameter track_counts ausgeschaltet ist, wird die Erfassung von Statistiken zur Datenbankaktivität deaktiviert. Der Autovacuum-Daemon benötigt die gesammelten Statistiken, um die Tabellen für Autovacuum und Autoanalyze zu identifizieren.

Weitere Informationen finden Sie unter Runtime Statistics for PostgreSQL auf der PostgreSQL-Dokumentationswebsite.

Berichtsspalten

- Status
- Region
- Ressource
- Parameterwert
- Empfohlener Wert
- Zeitpunkt der letzten Aktualisierung

Amazon-Redshift-Cluster-Auditprotokollierung

Beschreibung

Überprüft, ob in Ihren Amazon-Redshift-Clustern die Datenbank-Auditprotokollierung aktiviert ist. Amazon-Redshift-Protokolle stellen Informationen zu Verbindungen und Benutzeraktivitäten in Ihrer Datenbank bereit.

Sie können Ihren gewünschten Amazon S3 S3-Bucket-Namen für die Protokollierung im BucketNames-Parameter Ihrer AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Datenbank-Auditprotokollierung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz134
```

Quelle

```
AWS Config Managed Rule: redshift-audit-logging-enabled
```

Warnungskriterien

Gelb: Bei einem Amazon-Redshift-Cluster ist die Datenbank-Auditprotokollierung deaktiviert

Empfohlene Aktion

Aktivieren Sie die Protokollierung und Überwachung für Ihre Amazon-Redshift-Cluster.

Weitere Informationen finden Sie unter Konfigurieren von Prüfungen über die Konsole.

Weitere Ressourcen

Protokollierung und Überwachung in Amazon Redshift

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

In Amazon S3 sind keine Ereignisbenachrichtigungen aktiviert

Beschreibung

Überprüft, ob Amazon-S3-Ereignisbenachrichtigungen aktiviert oder mit den gewünschten Zielen oder Typen korrekt konfiguriert sind.

Die Amazon-S3-Funktion für Ereignisbenachrichtigungen sendet Benachrichtigungen, wenn bestimmte Ereignisse in Ihren Amazon-S3-Buckets eintreten. Amazon S3 kann Benachrichtigungen an Amazon SQS SQS-Warteschlangen, Amazon SNS SNS-Themen und Funktionen senden. AWS Lambda

Sie können Ihr gewünschtes Ziel und Ihre Ereignistypen mithilfe der Parameter DestinationArn und EventTypes Ihrer Regeln angeben. AWS Config

Weitere Informationen finden Sie unter Amazon-S3-Ereignisbenachrichtigungen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz163
```

Quelle

```
AWS Config Managed Rule: s3-event-notifications-enabled
```

Warnungskriterien

Gelb: In Amazon S3 sind keine Ereignisbenachrichtigungen aktiviert oder nicht mit dem gewünschten Ziel oder den gewünschten Typen konfiguriert.

Empfohlene Aktion

Konfigurieren Sie Amazon-S3-Ereignisbenachrichtigungen für Objekt- und Bucket-Ereignisse.

Weitere Informationen finden Sie unter Aktivieren und Konfigurieren von Ereignis-Benachrichtigungen mit der Amazon-S3-Konsole.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon-SNS-Themen: Nachrichtenzustellungsstatus wird nicht protokolliert

Beschreibung

Prüft, ob für Amazon-SNS-Themen die Protokollierung des Nachrichtenzustellungsstatus aktiviert ist.

Konfigurieren Sie Amazon-SNS-Themen für die Protokollierung des Nachrichtenzustellungsstatus, um bessere betriebliche Einblicke zu erhalten. Durch die Protokollierung der Nachrichtenzustellung wird beispielsweise überprüft, ob eine Nachricht an einen bestimmten Amazon-SNS-Endpunkt gesendet wurde. Und es hilft auch bei der Ermittlung der Antwort, die vom Endpunkt gesendet wurde.

Weitere Informationen finden Sie unter Amazon-SNS-Nachrichtenzustellungsstatus.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz121
```

Quelle

```
AWS Config Managed Rule: sns-topic-message-delivery-notification-enabled
```

Warnungskriterien

Gelb: Die Protokollierung des Nachrichtenzustellungsstatus ist für ein Amazon-SNS-Thema nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die Protokollierung des Nachrichtenzustellungsstatus für Ihre SNS-Themen.

Weitere Informationen finden Sie unter Konfigurieren der Protokollierung des Zustellungsstatus mithilfe der AWS-Managementkonsole.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Amazon VPC ohne Flow-Protokolle

Beschreibung

Prüft, ob Amazon-VPC-Flow-Protokolle für eine Virtual Private Cloud (VPC) erstellt wurden.

Sie können den Verkehrstyp mithilfe des TrafficType-Parameters in Ihren AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC-Flow-Protokollen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz122`

Quelle

`AWS Config Managed Rule: vpc-flow-logs-enabled`

Warnungskriterien

Gelb: VPCs haben keine Amazon-VPC-Flow-Protokolle.

Empfohlene Aktion

Erstellen Sie VPC-Flow-Protokolle für jede Ihrer VPCs.

Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Application Load Balancer und Classic Load Balancer ohne aktivierte Zugriffsprotokolle

Beschreibung

Prüft, ob für Application Load Balancer und Classic Load Balancer die Zugriffsprotokollierung aktiviert ist.

Elastic Load Balancing bietet Zugriffsprotokolle, die detaillierte Informationen zu Anforderungen erfassen, die an Ihren Load Balancer gesendet werden. Jedes Protokoll enthält Informationen wie die Zeit, zu der die Anforderung einging, die Client-IP-Adresse, Latenzen, Anforderungspfade und Serverantworten. Sie können diese Zugriffsprotokolle für die Analyse von Datenverkehrsmustern und zur Problembehebung verwenden.

Zugriffsprotokolle sind ein optionales Feature von Elastic Load Balancing, das standardmäßig deaktiviert ist. Nachdem Sie die Zugriffsprotokolle für Ihren Load Balancer aktiviert haben, erfasst

Elastic Load Balancing die Protokolle und speichert sie in dem von Ihnen angegebenen Amazon-S3-Bucket.

Sie können den Amazon S3 S3-Bucket für das Zugriffsprotokoll, den Sie überprüfen möchten, mithilfe des BucketNamess3-Parameters in Ihren AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Zugriffsprotokolle für Ihre Application Load Balancer oder Zugriffsprotokolle für Ihre Classic Load Balancer.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz167`

Quelle

`AWS Config Managed Rule: elb-logging-enabled`

Warnungskriterien

Gelb: Die Funktion für Zugriffsprotokolle ist für einen Application Load Balancer oder einen Classic Load Balancer nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie die Zugriffsprotokolle für Ihre Application Load Balancer und Classic Load Balancer.

Weitere Informationen finden Sie unter Aktivieren der Zugriffsprotokolle für Ihren Application Load Balancer oder Aktivieren der Zugriffsprotokolle für Ihren Classic Load Balancer.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel

- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CloudFormation Stack-Benachrichtigung

Beschreibung

Überprüft, ob all Ihre AWS CloudFormation Stacks Amazon SNS verwenden, um Benachrichtigungen zu erhalten, wenn ein Ereignis eintritt.

Sie können diese Prüfung so konfigurieren, dass sie mithilfe von Parametern in Ihren AWS Config Regeln nach bestimmten Amazon SNS SNS-Themen-ARNs sucht.

Weitere Informationen finden Sie unter AWS CloudFormation Stack-Optionen einrichten.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz111`

Quelle

`AWS Config Managed Rule: cloudformation-stack-notification-check`

Warnungskriterien

Gelb: Amazon SNS SNS-Ereignisbenachrichtigungen für Ihre AWS CloudFormation Stacks sind nicht aktiviert.

Empfohlene Aktion

Stellen Sie sicher, dass Ihre AWS CloudFormation Stacks Amazon SNS verwenden, um Benachrichtigungen zu erhalten, wenn ein Ereignis eintritt.

Durch die Überwachung von Stack-Ereignissen können Sie schnell auf unbefugte Aktionen reagieren, die Ihre AWS Umgebung verändern könnten.

Weitere Ressourcen

Wie kann ich eine E-Mail-Benachrichtigung erhalten, wenn mein CloudFormation AWS-Stack den Status ROLLBACK_IN_PROGRESS annimmt?

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CloudTrail Protokollierung von Datenereignissen für Objekte in einem S3-Bucket

Beschreibung

Prüft, ob mindestens ein AWS CloudTrail Trail Amazon S3 S3-Datenereignisse für all Ihre Amazon S3 S3-Buckets protokolliert.

Weitere Informationen finden Sie unter Protokollierung von Amazon-S3-API-Aufrufen mit AWS CloudTrail.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz166
```

Quelle

```
AWS Config Managed Rule: cloudtrail-s3-dataevents-enabled
```

Warnungskriterien

Gelb: Die AWS CloudTrail Ereignisprotokollierung für Amazon S3 S3-Buckets ist nicht konfiguriert

Empfohlene Aktion

Aktivieren Sie die CloudTrail Ereignisprotokollierung für Amazon S3 S3-Buckets und -Objekte, um Anfragen für den Zugriff auf Ziel-Buckets zu verfolgen.

Weitere Informationen finden Sie unter Aktivieren der CloudTrail Ereignisprotokollierung für S3-Buckets und -Objekte.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CodeBuild Protokollierung von Projekten

Beschreibung

Prüft, ob die AWS CodeBuild Projektumgebung die Protokollierung verwendet. Bei den Protokollierungsoptionen kann es sich um CloudWatch Protokolle in Amazon Logs oder um in einem bestimmten Amazon S3 S3-Bucket integrierte Protokolle oder beides handeln. Die Aktivierung der Protokollierung in einem CodeBuild Projekt kann mehrere Vorteile bieten, z. B. Debugging und Auditing.

Sie können den Namen des Amazon S3 S3-Buckets oder der CloudWatch Logs-Gruppe zum Speichern der Protokolle angeben, indem Sie den Parameter s3 BucketNames oder cloud WatchGroup Names in Ihren AWS Config Regeln verwenden.

Weitere Informationen finden Sie unter -Überwachung AWS CodeBuild.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz113
```

Quelle

```
AWS Config Managed Rule: codebuild-project-logging-enabled
```

Warnungskriterien

Gelb: Die AWS CodeBuild Projektprotokollierung ist nicht aktiviert.

Empfohlene Aktion

Stellen Sie sicher, dass die Protokollierung in Ihrem AWS CodeBuild Projekt aktiviert ist. Diese Prüfung kann nicht aus der Ansicht in der AWS Trusted Advisor Konsole ausgeschlossen werden.

Weitere Informationen finden Sie unter Anmelden und Überwachen AWS CodeBuild.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CodeDeploy Automatisches Rollback und Monitor aktiviert

Beschreibung

Überprüft, ob die Bereitstellungsgruppe mit automatischem Rollback und automatischer Überwachung der Bereitstellung mit angehängten Alarmen konfiguriert ist. Wenn während einer Bereitstellung etwas schief geht, wird sie automatisch zurückgesetzt und Ihre Anwendung bleibt in einem stabilen Zustand.

Weitere Informationen finden Sie unter Erneute Bereitstellung und Rollback einer Bereitstellung mit. CodeDeploy

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz114`

Quelle

`AWS Config Managed Rule: codedeploy-auto-rollback-monitor-enabled`

Warnungskriterien

Gelb: AWS CodeDeploy Automatisches Bereitstellungs-Rollback und Bereitstellungsüberwachung sind nicht aktiviert.

Empfohlene Aktion

Konfigurieren Sie eine Bereitstellungsgruppe oder Bereitstellung so, dass sie automatisch zurückgesetzt wird, wenn eine Bereitstellung fehlschlägt oder ein definierter Überwachungsschwellenwert erreicht wird.

Konfigurieren Sie den Alarm so, dass während des Bereitstellungsprozesses verschiedene Metriken wie CPU-Auslastung, Speichernutzung oder Netzwerkdatenverkehr überwacht werden. Wenn eine dieser Metriken bestimmte Schwellenwerte überschreitet, werden die Alarme ausgelöst und die Bereitstellung wird gestoppt oder rückgängig gemacht.

Informationen zur Einrichtung automatischer Rollbacks und zur Konfiguration von Alarmen für Ihre Bereitstellungsgruppen finden Sie unter Konfigurieren von erweiterten Optionen für eine Bereitstellungsgruppe.

Weitere Ressourcen

Was ist CodeDeploy?

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS CodeDeploy Lambda verwendet die all-at-once Bereitstellungskonfiguration

Beschreibung

Überprüft, ob die AWS CodeDeploy Bereitstellungsgruppe für die AWS Lambda Rechenplattform die all-at-once Bereitstellungskonfiguration verwendet.

Um das Risiko von Bereitstellungsfehlern Ihrer Lambda-Funktionen in zu verringern CodeDeploy, empfiehlt es sich, die kanarische oder lineare Bereitstellungskonfiguration anstelle der Standardoption zu verwenden, bei der der gesamte Datenverkehr von der ursprünglichen Lambda-Funktion auf die aktualisierte Funktion übertragen wird.

Weitere Informationen finden Sie unter Lambda-Funktionsversionen und Bereitstellungskonfiguration.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz115
```

Quelle

```
AWS Config Managed Rule: codedeploy-lambda-allatonce-traffic-shift-
disabled
```

Warnungskriterien

Gelb: Die AWS CodeDeploy Lambda-Bereitstellung verwendet die all-at-once Bereitstellungskonfiguration, um den gesamten Datenverkehr gleichzeitig auf die aktualisierten Lambda-Funktionen umzuleiten.

Empfohlene Aktion

Verwenden Sie die kanarische oder lineare Bereitstellungskonfiguration der CodeDeploy Bereitstellungsgruppe für die Lambda-Rechenplattform.

Weitere Ressourcen

Bereitstellungskonfiguration

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Elastic Beanstalk Enhanced Health Reporting ist nicht konfiguriert

Beschreibung

Überprüft, ob eine AWS Elastic Beanstalk Umgebung für erweiterte Statusberichte konfiguriert ist.

Die erweiterten Zustandsberichte von Elastic Beanstalk bieten detaillierte Leistungskennzahlen wie CPU-Auslastung, Speichernutzung, Netzwerkdatenverkehr und Informationen zum Zustand der Infrastruktur, wie Anzahl der Instances und Load-Balancer-Status.

Weitere Informationen finden Sie unter Erweiterte Zustandsberichte und -überwachung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die

Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz108`

Quelle

`AWS Config Managed Rule: beanstalk-enhanced-health-reporting-enabled`

Warnungskriterien

Gelb: Die Elastic-Beanstalk-Umgebung ist nicht für erweiterte Zustandsberichte konfiguriert

Empfohlene Aktion

Stellen Sie sicher, dass eine Elastic-Beanstalk-Umgebung für erweiterte Zustandsberichte konfiguriert ist.

Weitere Informationen finden Sie unter Aktivieren der erweiterten Zustandsberichte mit der Elastic-Beanstalk-Konsole.

Weitere Ressourcen

- Aktivieren der erweiterten Elastic-Beanstalk-Zustandsberichte
- Erweiterte Zustandsberichte und -überwachung

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Elastic Beanstalk mit deaktivierten verwalteten Plattform-Updates

Beschreibung

Prüft, ob verwaltete Plattformupdates in Elastic-Beanstalk-Umgebungen und Konfigurationsvorlagen aktiviert sind.

AWS Elastic Beanstalk veröffentlicht regelmäßig Plattform-Updates, um Korrekturen, Softwareupdates und neue Funktionen bereitzustellen. Mit verwalteten Plattformupdates kann Elastic Beanstalk automatisch Plattformupdates für neue Patch- und Unterversionen der Plattform durchführen.

Sie können die gewünschte Aktualisierungsstufe in den UpdateLevelParametern Ihrer AWS Config Regeln angeben.

Weitere Informationen finden Sie unter Aktualisieren der Plattformversion Ihrer Elastic-Beanstalk-Umgebung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz177`

Quelle

`AWS Config Managed Rule: elastic-beanstalk-managed-updates-enabled`

Warnungskriterien

Gelb: AWS Elastic Beanstalk Verwaltete Plattformupdates sind überhaupt nicht konfiguriert, auch nicht auf untergeordneter Ebene oder auf Patch-Ebene.

Empfohlene Aktion

Aktivieren Sie verwaltete Plattformupdates in Ihren Elastic-Beanstalk-Umgebungen oder konfigurieren Sie sie auf Unterversions- oder Update-Ebene.

Weitere Informationen finden Sie unter Verwaltete Plattformupdates.

Weitere Ressourcen

- Aktivieren der erweiterten Elastic-Beanstalk-Zustandsberichte
- Erweiterte Zustandsberichte und -überwachung

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Fargate Die Plattformversion ist nicht aktuell

Beschreibung

Überprüft, ob in Amazon ECS die neueste Plattformversion von AWS Fargate ausgeführt wird. Die Fargate-Plattformversion verweist auf eine bestimmte Laufzeitumgebung für die Fargate-Aufgabeninfrastruktur. Es handelt sich um eine Kombination aus der Kernel-Version und den Container-Laufzeitversionen. Neue Plattformversionen werden veröffentlicht, wenn sich die Laufzeitumgebung weiterentwickelt, weil es beispielsweise Kernel- oder Betriebssystem-Updates, neue Funktionen, Bugfixes oder Sicherheitsupdates gibt.

Weitere Informationen finden Sie unter Fargate-Aufgabenwartung.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz174
```

Quelle

```
AWS Config Managed Rule: ecs-fargate-latest-platform-version
```

Warnungskriterien

Gelb: Amazon ECS wird nicht auf der neuesten Version der Fargate-Plattform ausgeführt.

Empfohlene Aktion

Aktualisieren Sie auf die neueste Fargate-Plattformversion.

Weitere Informationen finden Sie unter Fargate-Aufgabenwartung.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

AWS Systems Manager State Manager Association hat den Status „Nichtkonformität“

Beschreibung

Überprüft, ob der Status der Zuordnungs-Konformität nach der Ausführung der AWS Systems Manager Zuordnung auf der Instanz COMPLIANT oder NON_COMPLIANT lautet.

State Manager, eine Funktion von AWS Systems Manager, ist ein sicherer und skalierbarer Konfigurationsverwaltungsdienst, der den Prozess automatisiert, Ihre verwalteten Knoten und andere AWS Ressourcen in einem von Ihnen definierten Zustand zu halten. Eine State Manager-Zuordnung ist eine Konfiguration, die Sie Ihren AWS Ressourcen zuweisen. Die Konfiguration definiert den Status, den Sie für Ihre Ressourcen beibehalten möchten. Dies hilft Ihnen, das Ziel zu erreichen, beispielsweise das Vermeiden von Konfigurationsabweichungen zwischen Ihren Amazon-EC2-Instances.

Weitere Informationen finden Sie unter AWS Systems Manager State Manager.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz147`

Quelle

`AWS Config Managed Rule: ec2-managedinstance-association-compliance-status-check`

Warnungskriterien

Gelb: Der Status der AWS Systems Manager Zuordnungskonformität ist NON_COMPLIANT.

Empfohlene Aktion

Überprüfen Sie den Status der State-Manager-Zuordnungen und ergreifen Sie dann alle erforderlichen Maßnahmen, um den Status wieder auf COMPLIANT zurückzusetzen.

Weitere Informationen finden Sie unter Info zu State Manager.

Weitere Ressourcen

AWS Systems Manager State Manager

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

CloudTrail Trails sind nicht mit Amazon CloudWatch Logs konfiguriert

Beschreibung

Prüft, ob AWS CloudTrail Trails so konfiguriert sind, dass sie Logs an CloudWatch Logs senden.

Überwachen CloudTrail Sie Protokolldateien mit CloudWatch Protokollen, um eine automatische Reaktion auszulösen, wenn kritische Ereignisse erfasst werden AWS CloudTrail.

Weitere Informationen finden Sie unter Überwachen von CloudTrail Protokolldateien mit CloudWatch Protokollen.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz164`

Quelle

`AWS Config Managed Rule: cloud-trail-cloud-watch-logs-enabled`

Warnungskriterien

Gelb: AWS CloudTrail ist nicht mit der CloudWatch Logs-Integration eingerichtet.

Empfohlene Aktion

Konfigurieren Sie CloudTrail Trails, um Protokollereignisse an CloudWatch Logs zu senden.

Weitere Informationen finden Sie unter CloudWatch Alarme für CloudTrail Ereignisse erstellen: Beispiele.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Elastic-Load-Balancing-Löschschutz ist für Load Balancer nicht aktiviert

Beschreibung

Überprüft, ob der Löschschutz für Ihre Load Balancer aktiviert ist.

Elastic Load Balancing unterstützt den Löschschutz für Ihre Application Load Balancer, Network Load Balancer und Gateway Load Balancer. Aktivieren Sie den Löschschutz, um zu verhindern, dass der Load Balancer versehentlich gelöscht wird. Wenn Sie einen Load Balancer erstellen, ist der Löschschutz standardmäßig deaktiviert. Wenn Ihre Load Balancer Teil einer Produktionsumgebung sind, sollten Sie in Erwägung ziehen, den Löschschutz zu aktivieren.

Zugriffsprotokolle sind ein optionales Feature von Elastic Load Balancing, das standardmäßig deaktiviert ist. Nachdem Sie die Zugriffsprotokolle für Ihren Load Balancer aktiviert haben, erfasst Elastic Load Balancing die Protokolle und speichert sie in dem von Ihnen angegebenen Amazon-S3-Bucket.

Weitere Informationen finden Sie unter Application-Load-Balancer-Löschschutz, Network-Load-Balancer-Löschschutz oder Gateway-Load-Balancer-Löschschutz.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

```
c18d2gz168
```

Quelle

```
AWS Config Managed Rule: elb-deletion-protection-enabled
```

Warnungskriterien

Gelb: Löschschutz ist für einen Load Balancer nicht aktiviert.

Empfohlene Aktion

Aktivieren Sie den Löschschutz für Application Load Balancer, Network Load Balancer und Gateway Load Balancer.

Weitere Informationen finden Sie unter Application-Load-Balancer-Löschschutz, Network-Load-Balancer-Löschschutz oder Gateway-Load-Balancer-Löschschutz.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Prüfung des Löschschutzes von RDS-DB-Clustern

Beschreibung

Überprüft, ob in Ihren Amazon-RDS-DB-Clustern der Löschschutz aktiviert ist.

Wenn Sie für einen DB-Cluster den Löschschutz aktivieren, kann die Datenbank von keinem Benutzer gelöscht werden.

Löschschutz ist für Amazon Aurora und RDS für MySQL, RDS für MariaDB, RDS für Oracle, RDS für PostgreSQL und RDS für SQL Server-Datenbank-Instances in allen Regionen verfügbar. AWS

Weitere Informationen finden Sie unter Löschschutz für Aurora-DB-Cluster.

Prüf-ID

`c18d2gz160`

Quelle

`AWS Config Managed Rule: rds-cluster-deletion-protection-enabled`

Warnungskriterien

Gelb: Sie haben Amazon-RDS-DB-Cluster, bei denen der Löschschutz nicht aktiviert ist.

Empfohlene Aktion

Aktivieren Sie den Löschschutz, wenn Sie einen Amazon RDS-DB-Cluster erstellen.

Sie können nur Cluster löschen, für die der Löschschutz nicht aktiviert ist. Durch das Aktivieren des Löschschutzes wird eine zusätzliche Schutzebene hinzugefügt und Datenverlust durch versehentliches oder unbeabsichtigtes Löschen einer Datenbank-Instance vermieden.

Der Löschschutz trägt auch dazu bei, gesetzliche Anforderungen zu erfüllen und die Geschäftskontinuität zu gewährleisten.

Weitere Informationen finden Sie unter Löschschutz für Aurora-DB-Cluster.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Weitere Ressourcen

Löschschutz für Aurora-DB-Cluster

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

RDS-DB-Instance – Prüfung auf automatisches Upgrade für Unterversion

Beschreibung

Überprüft, ob für Amazon-RDS-DB-Instances automatische Upgrades für Unterversionen konfiguriert sind.

Aktivieren Sie automatische Upgrades von Unterversionen für eine Amazon-RDS-Instance, um sicherzustellen, dass in der Datenbank immer die neueste sichere und stabile Version ausgeführt wird. Upgrades von Unterversionen bieten Sicherheitsupdates, Bugfixes und Leistungsverbesserungen und gewährleisten die Kompatibilität mit bestehenden Anwendungen.

Weitere Informationen finden Sie unter Upgrade der Engine-Version für eine DB-Instance.

> **Note**
>
> Die Ergebnisse dieser Prüfung werden mehrmals täglich automatisch aktualisiert, und Aktualisierungsanfragen sind nicht zulässig. Es kann ein paar Stunden dauern, bis die Änderungen sichtbar werden. Derzeit können Sie keine Ressourcen von dieser Prüfung ausschließen.

Prüf-ID

`c18d2gz155`

Quelle

`AWS Config Managed Rule: rds-automatic-minor-version-upgrade-enabled`

Warnungskriterien

Gelb: Für die RDS-DB-Instance sind keine automatischen Upgrades von Unterversionen aktiviert.

Empfohlene Aktion

Aktivieren Sie automatische Upgrades von Unterversionen, wenn Sie eine Amazon-RDS-DB-Instance erstellen.

Wenn Sie automatische Upgrades von Unterversionen aktivieren, wird die Datenbankversion automatisch aktualisiert, wenn sie eine Unterversion der DB-Engine ausführt, die eine niedrigere Versionsnummer hat als in Manuelles Upgraden der Engine-Version.

Berichtsspalten

- Status
- Region
- Ressource
- AWS Config Regel
- Eingabeparameter
- Zeitpunkt der letzten Aktualisierung

Protokoll ändern für AWS Trusted Advisor

Im folgenden Thema finden Sie die neuesten Änderungen an Trusted Advisor Schecks.

> **Note**
>
> Wenn Sie die Trusted Advisor Konsole oder die AWS Support API verwenden, werden Prüfungen, die entfernt wurden, nicht in den Prüfergebnissen angezeigt. Wenn Sie eine der entfernten Prüfungen verwenden, z. B. die Prüf-ID in einem AWS Support API-Vorgang oder Ihren Code angeben, müssen Sie diese Prüfungen entfernen, um API-Aufruffehler zu vermeiden.

Weitere Informationen über die verfügbaren Prüfungen finden Sie im AWS Trusted Advisor Referenz überprüfen.

5 Schecks wurden entfernt und 1 Scheck hinzugefügt

Trusted Advisor hat am 15. Mai 2024 3 Fehlertoleranzprüfungen, 1 Leistungsprüfung und 1 Sicherheitsprüfung als veraltet markiert:

- Verwendung von IAM
- ELB Zonenübergreifendes Load Balancing
- Überausgelastete Amazon EBS Magnetic Volumes
- Große Anzahl von EC2-Sicherheitsgruppenregeln, die auf eine Instance angewendet werden
- Große Anzahl von Regeln in einer EC2-Sicherheitsgruppe

Trusted Advisor hat am 15. Mai 2024 1 neue Sicherheitsüberprüfung hinzugefügt:

- Amazon S3 S3-Serverzugriffsprotokolle aktiviert

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Die Fehlertoleranzprüfungen wurden entfernt

Trusted Advisor 3 Fault Tolerance Check wurde am 25. April 2024 nicht mehr unterstützt:

- AWS Direct Connect Redundanz der Verbindung
- AWS Direct Connect Standort-Redundanz
- AWS Direct Connect Redundanz virtueller Schnittstellen

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Fehlertoleranzprüfung

Trusted Advisor am 29. Februar 2024 wurde 1 Fehlertoleranzprüfung hinzugefügt:

- NLB — Mit dem Internet verbundene Ressource in einem privaten Subnetz

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Die Fehlertoleranz und die Sicherheitschecks wurden aktualisiert

Trusted Advisor am 28. März 2024 wurde eine neue Fehlertoleranzprüfung hinzugefügt und eine bestehende Fehlertoleranz- und eine Sicherheitsprüfung geändert:

- Prüfung AWS Resilience Hub der Anwendungskomponenten hinzugefügt
- Aktualisierte AWS Lambda VPC-fähige Funktionen ohne Multi-AZ-Redundanz
- Aktualisierte Funktionen AWS Lambda , die veraltete Laufzeiten verwenden

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Fehlertoleranzprüfung

Trusted Advisor am 31. Januar 2024 wurde 1 Fehlertoleranzprüfung hinzugefügt:

- AWS Direct Connect Ausfallsicherheit des Standorts

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Die Fehlertoleranzprüfung wurde aktualisiert

Trusted Advisor 1 Fehlertoleranzprüfung wurde am 08. Januar 2024 geändert:

- Der Amazon RDS-Parameter innodb_flush_log_at_trx_commit ist nicht 1

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Die Sicherheitsüberprüfung wurde aktualisiert

Trusted Advisor 1 Sicherheitscheck wurde am 21. Dezember 2023 geändert:

- AWS Lambda Funktionen, die veraltete Laufzeiten verwenden

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Sicherheits- und Leistungsprüfungen

Trusted Advisor am 20. Dezember 2023 wurden 2 neue Sicherheitschecks und 2 neue Leistungsprüfungen hinzugefügt:

- Amazon EFS-Clients verwenden keine data-in-transit Verschlüsselung
- Amazon Aurora Aurora-DB-Cluster mit unzureichender Bereitstellung für Lese-Workloads
- Amazon RDS-Instance mit unzureichender Systemkapazität
- Ende der Standardunterstützung für Amazon EC2 EC2-Instances mit Ubuntu LTS

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Sicherheitsüberprüfung

Trusted Advisor am 15. Dezember 2023 wurde 1 neue Sicherheitsüberprüfung hinzugefügt:

- Amazon Route 53 stimmt nicht mit CNAME-Datensätzen überein, die direkt auf S3-Buckets verweisen

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Prüfungen zur Fehlertoleranz und Kostenoptimierung

Trusted Advisor am 07. Dezember 2023 wurden 2 neue Fehlertoleranzprüfungen und 1 neue Kostenoptimierungsprüfung hinzugefügt:

- Amazon DocumentDB Single-AZ-Cluster
- Konfiguration zum Abbruch unvollständiger mehrteiliger Uploads in Amazon S3
- Amazon ECS AWS Logs-Treiber im Blockierungsmodus

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Fehlertoleranzprüfungen

Trusted Advisor am 17. November 2023 wurden 3 neue Fehlertoleranzprüfungen hinzugefügt:

- ALB Multi-AZ
- NLB Multi-AZ
- VPC-Schnittstelle, Endpunkt-Netzwerkschnittstellen in mehreren AZs

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue Schecks für Amazon RDS

Trusted Advisor hat am 15. November 2023 37 neue Schecks für Amazon RDS hinzugefügt.

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Neue AWS Trusted Advisor API

AWS Trusted Advisor führt neue APIs ein, mit denen Sie programmgesteuert auf Trusted Advisor Advisor-Best-Practice-Prüfungen, Empfehlungen und priorisierte Empfehlungen zugreifen können. Trusted Advisor APIs ermöglichen Ihnen die programmatische Integration in Trusted Advisor Ihr bevorzugtes Betriebstool, um Ihre Workloads in großem Umfang zu automatisieren und zu optimieren. Die neuen APIs sind für Business-, Enterprise On-Ramp- oder Enterprise Support-Kunden verfügbar und bieten Zugriff auf Trusted Advisor Empfehlungen für Ihr Konto oder alle verknüpften Konten innerhalb eines Zahlerkontos. Enterprise Support-Kunden mit Zugriff auf Verwaltungs- oder delegierte Administratorkonten können zusätzlich programmgesteuert priorisierte Empfehlungen in ihrer gesamten Organisation abrufen.

Die neuen Trusted Advisor APIs werden die drei Funktionen ersetzen, die zuvor über die AWS Support API (SAPI) angeboten wurden. SAPI wird weiterhin Fallstudien und andere Supportinformationen anbieten.

Trusted Advisor APIs sind generell in den Regionen USA Ost (Ohio), USA Ost (Nord-Virginia), USA West (Oregon), Asien-Pazifik (Seoul), Asien-Pazifik (Sydney) und Europa (Irland) verfügbar.

Um mehr zu erfahren, besuchen Sie bitte die AWS Trusted Advisor API-Seite.

Trusted Advisor Entfernung überprüfen

Trusted Advisor hat am 9. November 2023 die folgenden Schecks entfernt.

Name prüfen	Kategorie prüfen	ID prüfen
EBS-Volumes sollten an EC2-Instances angehängt werden	Sicherheit	`Hs4Ma3G119`
Bei S3-Buckets sollte die serverseitige Verschlüsselung aktiviert sein	Sicherheit	`Hs4Ma3G167`
CloudFront Bei Distributionen sollte die Origin-Zugriffside ntität aktiviert sein	Sicherheit	`Hs4Ma3G195`

Integration von AWS Config Schecks in Trusted Advisor

Trusted Advisor 64 neue Schecks hinzugefügt, bereitgestellt von AWS Config am 30. Oktober 2023.

Weitere Informationen hierzu finden Sie unter AWS Trusted Advisor-Prüfungen anzeigen, die von AWS Config unterstützt werden.

Neue Fehlertoleranzprüfungen

Trusted Advisor hat am 12. Oktober 2023 die folgenden Schecks hinzugefügt.

- Amazon RDS ReplicaLag
- Amazon RDS FreeStorageSpace
- Amazon RDS DiskQueueDepth
- Amazon Route 53 Resolver Redundanz der Endpunkt-Verfügbarkeitszone
- Für Auto Scaling verfügbare IPs in Subnetzen
- Amazon-MSK-Broker, die zu viele Partitionen hosten

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Neue Service Limits-Prüfung

Trusted Advisor hat am 17. August 2023 den folgenden Check hinzugefügt.

- Nutzung des Lambda-Codespeichers

Weitere Informationen finden Sie in der Service Limits-Kategorie.

Neue Fehlertoleranzprüfung

Trusted Advisor hat am 3. August 2023 den folgenden Scheck hinzugefügt.

- AWS Lambda Ziele des Ereignisses bei einem Ausfall

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Neue Fehlertoleranzprüfungen und Leistungsprüfungen

Trusted Advisor hat am 1. Juni 2023 die folgenden Prüfungen hinzugefügt.

- Amazon EFS – Keine Mount-Ziel-Redundanz
- Amazon EFS – Optimierung des Durchsatzmodus
- Redundanz der ActiveMQ-Availability-Zone
- RabbitMQ-Availability-Zone-Redundanz

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie und Leistung-Kategorie.

Neue Fehlertoleranzprüfungen

Trusted Advisor hat am 16. Mai 2023 die folgenden Schecks hinzugefügt.

- NAT-Gateway-AZ-Unabhängigkeit
- Einzelne AZ-Anwendungsprüfung

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Neue Fehlertoleranzprüfungen

Trusted Advisor hat am 27. April 2023 die folgenden Schecks hinzugefügt.

- Nummer von AWS-Regionen in einem Incident Manager-Replikationssatz
- AWS Resilience Hub Alter der Bewertung

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Ausweitung der Amazon ECS-Fehlertoleranzprüfungen auf Regionen

Trusted Advisor erweiterte die folgenden Kontrollen am 27. April 2023 auf weitere Regionen. Trusted Advisor Prüfungen für Amazon ECS sind jetzt in allen Regionen verfügbar, in denen Amazon ECS allgemein verfügbar ist.

- Amazon-ECS-Service mit einer einzigen Availability Zone
- Amazon-ECS-Multi-AZ-Platzierungsstrategie

Zu den erweiterten Regionen gehören Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Jakarta), Asien-Pazifik (Melbourne), Europa (Mailand), Europa (Spanien), Europa (Zürich), Naher Osten (Bahrain), Naher Osten (VAE).

Neue Fehlertoleranzprüfungen

Trusted Advisor hat am 30. März 2023 die folgenden Schecks hinzugefügt.

- Amazon-ECS-Service mit einer einzigen Availability Zone
- Amazon-ECS-Multi-AZ-Platzierungsstrategie

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Neue Fehlertoleranzprüfungen

Trusted Advisor hat am 15. Dezember 2022 die folgenden Schecks hinzugefügt.

- AWS CloudHSM Cluster, auf denen HSM-Instanzen in einer einzigen AZ ausgeführt werden
- Amazon ElastiCache Multi-AZ-Cluster
- Amazon-MemoryDB-Multi-AZ-Cluster

Um Ergebnisse Trusted Advisor für Ihre AWS CloudHSM, ElastiCache und MemoryDB-Cluster zu erhalten, müssen Sie Cluster in Ihren Availability Zones haben. Weitere Informationen finden Sie in der folgenden -Dokumentation:

- AWS CloudHSM Benutzerhandbuch
- Amazon MemoryDB für Redis – Entwicklerleitfaden
- Amazon ElastiCache for Redis-Benutzerhandbuch

Trusted Advisor hat die folgenden Prüfinformationen am 15. Dezember 2022 aktualisiert.

- AWS Resilience Hub Richtlinie verletzt — App-Name wurde auf Anwendungsname aktualisiert
- AWS Resilience Hub Resilienzwerte — App-Name und App Resilience Score wurden auf Anwendungsname und Anwendungsbelastbarkeitsbewertung aktualisiert

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Aktualisierungen der Trusted Advisor Integration mit AWS Security Hub

Trusted Advisor hat am 17. November 2022 das folgende Update vorgenommen.

Wenn Sie Security Hub deaktivieren oder AWS Config für einen AWS-Region, werden Ihre Kontrollergebnisse dafür Trusted Advisor jetzt AWS-Region innerhalb von 7-9 Tagen entfernt. Bisher Trusted Advisor betrug der Zeitrahmen für das Entfernen Ihrer Security Hub Hub-Daten 90 Tage.

Weitere Informationen finden Sie in den folgenden Abschnitten im Fehlerbehebung-Thema:

- Ich habe Security Hub AWS Config in einer Region deaktiviert
- Mein Steuerelement ist in Security Hub archiviert, aber ich sehe die Ergebnisse immer noch in Trusted Advisor

Neue Fehlertoleranzprüfungen für AWS Resilience Hub

Trusted Advisor hat am 17. November 2022 die folgenden Prüfungen hinzugefügt.

- AWS Resilience Hub Richtlinie verletzt
- AWS Resilience Hub Resilienzwerte

Sie können diese Prüfungen verwenden, um den aktuellen Stand der Resilienzrichtlinie und den Resilienzwert für Ihre Anwendungen einzusehen. Resilience Hub bietet Ihnen einen zentralen Ort, an dem Sie die Resilienz und Verfügbarkeit Ihrer Anwendungen definieren, verfolgen und verwalten können.

Um Ergebnisse Trusted Advisor für Ihre Resilience Hub-Anwendungen zu erhalten, müssen Sie eine AWS Anwendung bereitstellen und Resilience Hub verwenden, um den Resilienzstatus der Anwendung zu verfolgen. Weitere Informationen finden Sie im AWS Resilience Hub - Benutzerhandbuch.

Um Ergebnisse Trusted Advisor für Ihre Cluster ElastiCache und Ihre MemoryDB-Cluster zu erhalten, müssen Sie Cluster in Ihren Availability Zones haben. Weitere Informationen finden Sie in der folgenden -Dokumentation:

- Amazon MemoryDB für Redis – Entwicklerleitfaden
- Amazon ElastiCache for Redis-Benutzerhandbuch

Weitere Informationen finden Sie in der Fehlertoleranz-Kategorie.

Aktualisieren Sie die Konsole Trusted Advisor

Trusted Advisor hat am 16. November 2022 die folgende Änderung hinzugefügt.

Das Trusted Advisor Dashboard in der Konsole heißt jetzt Trusted Advisor Recommendations. Auf der Trusted Advisor -Empfehlungsseite werden weiterhin die Prüfergebnisse und die verfügbaren Prüfungen für jede Kategorie für Ihre AWS-Konto angezeigt.

Durch diese Namensänderung wird nur die Trusted Advisor Konsole aktualisiert. Sie können die Trusted Advisor Konsole und die Trusted Advisor Operationen in der AWS Support API weiterhin wie gewohnt verwenden.

Weitere Informationen finden Sie unter Erste Schritte mit Trusted Advisor -Empfehlungen.

Neue Überprüfungen für Amazon EC2

Trusted Advisor hat am 1. September 2022 den folgenden Check hinzugefügt.

- Amazon-EC2-Instances mit veraltetem Support für Microsoft Windows Server

Weitere Informationen finden Sie in der Sicherheit-Kategorie.

Security-Hub-Prüfungen wurden Trusted Advisor hinzugefügt

Unterstützt ab 23. Juni 2022 Trusted Advisor nur Security Hub-Steuerelemente, die bis zum 7. April 2022 verfügbar sind. Diese Version unterstützt alle Kontrollen des Sicherheitsstandards AWS Foundational Security Best Practices mit Ausnahme der Kontrollen in der Kategorie: Wiederherstellung > Resilienz. Weitere Informationen finden Sie unter Anzeigen von AWS Security Hub Steuerelemente in AWS Trusted Advisor.

Eine Liste der unterstützten Steuerelemente finden Sie unter AWS Foundational Security Best Practices-Steuerelemente im AWS Security Hub -Benutzerhandbuch.

Es wurden Schecks von hinzugefügt AWS Compute Optimizer

Trusted Advisor hat am 4. Mai 2022 die folgenden Schecks hinzugefügt.

Name prüfen	Kategorie prüfen	ID prüfen
Amazon EBS mit nicht ausgelasteten Volumes	Kostenoptimierung	`COr6dfpM03`
Amazon EBS mit überlasteten Volumes	Leistung	`COr6dfpM04`
AWS Lambda aufgrund der Speichergröße übermäßig bereitgestellte Funktionen	Kostenoptimierung	`COr6dfpM05`
AWS Lambda Funktionen, die aufgrund der Speicherg röße nicht ausreichend zur Verfügung stehen	Leistung	`COr6dfpM06`

Sie müssen sich AWS-Konto für Compute Optimizer entscheiden, damit diese Prüfungen Daten von Ihren Lambda- und Amazon EBS-Ressourcen empfangen können. Weitere Informationen finden Sie unter Melden Sie sich AWS Compute Optimizer für Trusted Advisor Schecks an.

Aktualisierungen der Prüfung zu kompromittierten Zugriffsschlüsseln

Trusted Advisor hat den folgenden Check am 25. April 2022 aktualisiert.

Name prüfen	Kategorie prüfen	ID prüfen
Exposed Access Keys	Sicherheit	`12Fnkpl8Y5`

Trusted Advisor aktualisiert diesen Check jetzt automatisch für Sie. Diese Prüfung kann nicht manuell über die Trusted Advisor Konsole oder die AWS Support API aktualisiert werden. Wenn Ihre Anwendung oder Ihr Code diesen Check für Sie aktualisiert, empfehlen wir Ihnen AWS-Konto, ihn zu aktualisieren, sodass dieser Check nicht mehr aktualisiert wird. Andernfalls wird Ihnen die Fehlermeldung `InvalidParameterValue` angezeigt.

Alle Zugriffsschlüssel, die Sie vor diesem Update ausgeschlossen haben, werden nicht mehr ausgeschlossen und werden als betroffene Ressourcen angezeigt. Sie können Zugriffsschlüssel nicht von Ihren Prüfergebnissen ausschließen. Weitere Informationen finden Sie unter Exposed Access Keys.

> **Note**
>
> Wenn Sie Ihre AWS-Konto nach dem 25. April 2022 erstellt haben, wird in den Prüfergebnissen für exponierte Zugriffstasten zunächst das graue Symbol ( ) angezeigt, auch wenn es sich um unsichtbare Zugriffstasten handelt. Dies bedeutet, dass Trusted Advisor keine Änderungen an der Überprüfung identifiziert hat. Wenn eine gefährdete Ressource Trusted Advisor identifiziert wird, ändert sich der Status in das Symbol für empfohlene Maßnahmen ( ). Nachdem Sie die Ressource repariert oder gelöscht haben, zeigt das Prüfergebnis das Häkchensymbol ( ) an.

Prüfungen für AWS Direct Connect aktualisiert

Trusted Advisor hat die folgenden Prüfungen am 29. März 2022 aktualisiert.

Name prüfen	Kategorie prüfen	ID prüfen
AWS Direct Connect Redundanz der Verbindung	Fehlertoleranz	`0t121N1Ty3`
AWS Direct Connect Standort-Redundanz	Fehlertoleranz	`8M012Ph3U5`
AWS Direct Connect Redundanz virtueller Schnittstellen	Fehlertoleranz	`4g3Nt5M1Th`

- Der Wert für die Spalte Region zeigt jetzt den AWS-Region -Code statt des vollständigen Namens an. Beispielsweise haben Ressourcen in USA Ost (Nord-Virginia) jetzt den Wert `us-east-1`.
- Der Wert für die Spalte Zeitstempel erscheint jetzt im RFC 3339-Format, z. B. `2022-03-30T01:02:27.000Z`.
- Ressourcen, die keine erkannten Probleme haben, werden jetzt in der Prüfungstabelle angezeigt. Neben diesen Ressourcen wird ein Häkchensymbol ( ) angezeigt.

  Bisher wurden in der Tabelle nur Ressourcen aufgeführt, deren Untersuchung Trusted Advisor empfohlen wurde. Neben diesen Ressourcen wird ein Warnungssymbol ( ) angezeigt.

AWS Security Hub Steuerelemente wurden der AWS Trusted Advisor Konsole hinzugefügt

AWS Trusted Advisor hat am 18. Januar 2022 111 Security Hub-Steuerelemente zur Kategorie Sicherheit hinzugefügt.

Sie können Ihre Ergebnisse zu Security Hub-Steuerungen anhand des Sicherheitsstandards „Best Practices“ von AWS Foundational Security einsehen. Diese Integration beinhaltet keine Steuerelemente, die die Kategorie: Recover > Resilienz haben.

Weitere Informationen über dieses Feature finden Sie unter Anzeigen von AWS Security Hub Steuerelemente in AWS Trusted Advisor.

Neue Prüfungen für Amazon EC2 und AWS -Well-Architected

Trusted Advisor hat am 20. Dezember 2021 die folgenden Prüfungen hinzugefügt.

- Konsolidierung von Amazon-EC2-Instances für Microsoft SQL Server
- Amazon-EC2-Instances für Microsoft SQL Server mit übermäßiger Bereitstellung
- Amazon-EC2-Instances mit veraltetem Microsoft SQL Server (Ende des Supports)
- AWS Well-Architected-Probleme mit hohem Risiko für die Kostenoptimierung
- AWS Well-Architected-Probleme mit hohem Risiko für die Leistung
- AWS Well-Architected-Probleme mit hohem Risiko für die Sicherheit
- AWS Well-Architected-Probleme mit hohem Risiko für die Zuverlässigkeit

Weitere Informationen finden Sie unter der AWS Trusted Advisor -Überprüfungsreferenz.

Der Scheckname für Amazon OpenSearch Service wurde aktualisiert

Trusted Advisor hat den Namen für den Amazon OpenSearch Service Reserved Instance Optimization Scheck am 8. September 2021 aktualisiert.

Die Prüfungsempfehlungen, die Kategorie und die ID sind identisch.

Name prüfen	Kategorie prüfen	ID prüfen
Amazon OpenSearch Service Reserved Instance-Optimierung	Kostenoptimierung	`7ujm6yhn5t`

> **Note**
>
> Wenn Sie Trusted Advisor für CloudWatch Amazon-Metriken verwenden, wird der Metrikname für diese Prüfung ebenfalls aktualisiert. Weitere Informationen finden Sie unter Erstellen von Amazon CloudWatch-Alarmen zur Überwachung von AWS Trusted Advisor-Metriken.

Prüfungen für Amazon Elastic Block Store Volume-Speicher hinzugefügt

Trusted Advisor hat am 8. Juni 2021 die folgenden Prüfungen hinzugefügt.

Name prüfen	Kategorie prüfen	ID prüfen
EBS universeller SSD (gp3) Volume-Speicher	Service Limits	dH7RR0l6J3
EBS Bereitgestellter IOPS SSD (io2)-Volume-Speicher	Service Limits	gI7MM0l7J2

Es wurden Schecks für hinzugefügt AWS Lambda

Trusted Advisor hat am 8. März 2021 die folgenden Schecks hinzugefügt.

Name prüfen	Kategorie prüfen	ID prüfen
AWS Lambda Funktionen mit übermäßigen Timeouts	Kostenoptimierung	L4dfs2Q3C3
AWS Lambda Funktionen mit hohen Fehlerraten	Kostenoptimierung	L4dfs2Q3C2
AWS Lambda Funktione n, die veraltete Laufzeiten verwenden	Sicherheit	L4dfs2Q4C5
AWS Lambda VPC-fähige Funktionen ohne Multi-AZ-Redundanz	Fehlertoleranz	L4dfs2Q4C6

Weitere Informationen zur Verwendung dieser Prüfungen mit Lambda finden Sie unter AWS Trusted Advisor Beispielworkflow zur Anzeige von Empfehlungen im AWS Lambda Developer Guide.

Trusted Advisor Entfernung von Schecks

Trusted Advisor hat den folgenden Scheck für den AWS GovCloud (US) Region am 8. März 2021 entfernt.

Name prüfen	Kategorie prüfen	ID prüfen
EC2 elastische IP-Adressen	Service Limits	aW9HH0l8J6

Aktualisierte Prüfungen für Amazon Elastic Block Store

Trusted Advisor hat die Einheit des Amazon EBS-Volumes für die folgenden Prüfungen am 5. März 2021 von Gibibyte (GiB) auf Tebibyte (TiB) aktualisiert.

> **Note**
>
> Wenn Sie Trusted Advisor für CloudWatch Amazon-Metriken verwenden, werden die Metriknamen für diese fünf Prüfungen ebenfalls aktualisiert. Weitere Informationen finden Sie unter Erstellen von Amazon CloudWatch-Alarmen zur Überwachung von AWS Trusted Advisor-Metriken.

Name prüfen	Kategorie prüfen	ID prüfen	Aktualisierte CloudWatch Metrik für ServiceLimit
EBS kalter HDD (sc1) Volume-Speicher	Service Limits	gH5CC0e3J9	EBS kalter HDD (sc1) Volume-Speicher
EBS universeller SSD (gp2) Volume-Sp eicher	Service Limits	dH7RR0l6J9	Universeller SSD (gp2) Volume-Sp eicher (TiB)
EBS magnetischer (Standard)-Volume-Speicher	Service Limits	cG7HH0l7J9	Magnetischer (Standard)-Volume-Speicher TiB)

Name prüfen	Kategorie prüfen	ID prüfen	Aktualisierte CloudWatch Metrik für ServiceLimit
EBS bereitgestellte IOPS SSD (io1)-Volume-Speicher	Service Limits	`gI7MM0l7J9`	Bereitgestellter IOPS (SSD)-Speicher (TiB)
EBS durchsatz optimierter HDD (st1) Volume-Speicher	Service Limits	`wH7DD0l3J9`	Durchsatzoptimierter HDD (st1) Volume-Speicher (TiB)

Trusted Advisor Entfernung überprüfen

> **Note**
>
> Trusted Advisor hat am 18. November 2020 die folgenden Schecks entfernt.

Prüfungen entfernt am 18. November 2020	Kategorie prüfen	ID prüfen
EC2Config-Service für EC2-Windows-Instances	Fehlertoleranz	`V77iOLlBqz`
ENA Treiberversion für EC2 Windows-Instances	Fehlertoleranz	`TyfdMXG69d`
NVMe Treiberversion für EC2 Windows-Instances	Fehlertoleranz	`yHAGQJV9K5`
PV-Treiberversion für EC2 Windows-Instances	Fehlertoleranz	`Wnwm9Il5bG`
EBS aktive Volumes	Service Limits	`fH7LL0l7J9`

Amazon Elastic Block Store hat keine Begrenzung mehr für die Anzahl der Volumes, die Sie bereitstellen können.

Sie können Ihre Amazon EC2-Instances überwachen und überprüfen, ob sie auf dem neuesten Stand sind, indem Sie den AWS Systems Manager Distributor oder andere Tools von Drittanbietern verwenden oder Ihre eigenen Skripte schreiben, um Treiberinformationen für die Windows Management Instrumentation (WMI) zurückzugeben.

Trusted Advisor Entfernung von Schecks

Trusted Advisor hat den folgenden Scheck am 18. Februar 2020 entfernt.

Name prüfen	Kategorie prüfen	ID prüfen
Service Limits	Leistung	`eW7HH0l7J9`

AWS Support App in Slack

Du kannst die AWS Support App verwenden, um deine AWS Supportfälle in Slack zu verwalten. Lade deine Teammitglieder zu Chat-Kanälen ein, antworte auf Fallaktualisierungen und chatte direkt mit Support-Mitarbeitern. Verwende die AWS Support App, um Supportfälle schnell in Slack zu verwalten.

Verwende die AWS Support App, um Folgendes zu tun:

- Erstellen, Aktualisieren, Suchen und Lösen von Support-Fällen in Slack-Kanälen
- Anfügen von Dateien an Support-Fälle
- Anfordern von Kontingenterhöhungen aus Service Quotas
- Freigeben von Details zu Support-Fällen für Ihr Team, ohne den Slack-Kanal zu verlassen
- Starten einer Live-Chat-Sitzung mit Support-Kundendienstmitarbeitern

Wenn Sie einen Supportfall in der AWS Support App erstellen, aktualisieren oder lösen, wird der Fall auch in der aktualisiert AWS Support Center Console. Sie müssen sich nicht in der Support-Center-Konsole anmelden, um Ihre Support-Fälle separat zu verwalten.

Hinweise

- Die Antwortzeiten für Support-Fälle sind dieselben, unabhängig davon, ob Sie den Fall in Slack oder in der Support-Center-Konsole erstellt haben.
- Sie können einen Support-Fall für Konto- und Abrechnungssupport, Erhöhungen des Service-Kontingents und technischen Support erstellen.

Themen

- Nehmen Sie an einer Live-Chat-Sitzung teil mit AWS Support
- Suchen nach Support-Fällen in Slack
- Beheben eines Support-Falls in Slack
- Wiederaufnahme eines Support-Falls in Slack
- Anfordern einer Erhöhung des Service-Kontingents
- Löschen einer Slack-Kanalkonfiguration aus der AWS Support-App
- Löschen einer Slack-Workspace-Konfiguration aus der AWS Support-App
- AWS Support-App in Slack-Befehlen
- Anzeigen von AWS Support-App-Korrespondenzen in der AWS Support Center Console
- Erstellen von AWS Support-App in Slack-Ressourcen mit AWS CloudFormation

Voraussetzungen

Um die AWS Support-App in Slack verwenden zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie haben einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan. Sie finden Ihren Support-Plan unter AWS Support Center Console oder auf der Seite Support-Pläne. Weitere Informationen finden Sie unter AWS Support-Pläne vergleichen.
- Sie haben einen Slack-Workspace und -Kanal für Ihre Organisation. Sie müssen ein Slack-Workspace-Administrator sein oder über die Berechtigung zum Hinzufügen von Apps zu diesem Slack-Workspace verfügen. Weitere Informationen finden Sie im Hilfe-Center von Slack.
- Sie melden sich bei AWS-Konto als beliebiger AWS Identity and Access Management-(IAM)-Benutzer oder -Rolle mit den erforderlichen Berechtigungen an. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf das AWS Support-App-Widget.
- Sie müssen eine IAM-Rolle erstellen, die über die erforderlichen Berechtigungen verfügt, um in Ihrem Auftrag Aktionen durchzuführen. Die AWS Support-App verwendet diese Rolle, um API-Aufrufe an verschiedene Services zu tätigen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support-App.

Themen

- Verwalten des Zugriffs auf das AWS Support-App-Widget

- Verwalten des Zugriffs auf die AWS Support-App

Verwalten des Zugriffs auf das AWS Support-App-Widget

Sie können eine AWS Identity and Access Management (IAM)-Richtlinie anfügen, um einem IAM-Benutzer die Berechtigung zum Konfigurieren des AWS Support-App-Widgets im AWS Support Center Console zu gewähren.

Weitere Informationen zum Hinzufügen einer Richtlinie zu einer IAM-Entität finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) im IAM-Benutzerhandbuch.

> **Note**
>
> Sie können sich auch als Root-Benutzer in Ihrem AWS-Konto anmelden, aber wir raten Ihnen davon ab, dies zu tun. Weitere Informationen über den Zugriff von Root-Benutzern finden Sie unter Schützen Sie Ihre Anmeldeinformationen als Root-Benutzer und verwenden Sie sie nicht für alltägliche Aufgaben im IAM-Benutzerhandbuch.

Beispiel für eine IAM-Richtlinie

Sie können die folgende Richtlinie an eine Entität anfügen, z. B. an einen IAM-Benutzer oder eine Gruppe. Diese Richtlinie ermöglicht es einem Benutzer, einen Slack-Workspace zu autorisieren und Slack-Kanäle in der Support-Center-Konsole zu konfigurieren.

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

Berechtigungen erforderlich für die Verbindung der AWS Support-App mit Slack

Die AWS Support-App enthält „nur mit Berechtigung“-Aktionen, die nicht direkt einer API-Operation entsprechen. Diese Aktionen sind in der Service-Authorization-Referenz mit [nur mit Berechtigung] angegeben.

Die AWS Support-App verwendet die folgenden API-Aktionen, um eine Verbindung zu Slack herzustellen, und listet dann Ihre öffentlichen Slack-Kanäle in der AWS Support Center Console auf:

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

Diese API-Aktionen werden nicht von Ihrem Code aufgerufen. Deshalb sind diese API-Aktionen nicht in der AWS CLI und den AWS SDKs enthalten.

Verwalten des Zugriffs auf die AWS Support-App

Nachdem Sie Berechtigungen für das AWS Support-App-Widget erhalten haben, müssen Sie auch eine AWS Identity and Access Management (IAM)-Rolle erstellen. Diese Rolle führt Aktionen von anderen AWS-Services für Sie aus, wie die AWS Support-API und Service Quotas.

Anschließend fügen Sie dieser Rolle eine IAM-Richtlinie hinzu, damit die Rolle über die erforderlichen Berechtigungen zum Ausführen dieser Aktionen verfügt. Sie wählen diese Rolle aus, wenn Sie Ihre Slack-Kanalkonfiguration in der Support-Center-Konsole erstellen.

Benutzer in Ihrem Slack-Kanal verfügen über dieselben Berechtigungen, die Sie der IAM-Rolle gewähren. Wenn Sie beispielsweise schreibgeschützten Zugriff auf Ihre Support-Fälle festlegen, können Benutzer in Ihrem Slack-Kanal Ihre Support-Fälle anzeigen, aber nicht aktualisieren.

> **Important**
>
> Wenn Sie einen Live-Chat mit Support-Kundendienstmitarbeitern anfordern und einen neuen privaten Kanal als bevorzugten Live-Chat-Kanal auswählen, erstellt die AWS Support-App einen separaten Slack-Kanal. Dieser Slack-Kanal verfügt über dieselben Berechtigungen wie der Kanal, in dem Sie den Fall erstellt oder den Chat initiiert haben.
> Wenn Sie die IAM-Rolle oder die IAM-Richtlinie ändern, gelten Ihre Änderungen für den von Ihnen konfigurierten Slack-Kanal und für alle neuen Live-Chat-Slack-Kanäle, die die AWS Support-App für Sie erstellt.

Befolgen Sie diese Verfahren, um Ihre IAM-Rolle und -Richtlinie zu erstellen.

Themen

Verwenden Sie eine AWS-verwaltete Richtlinie oder erstellen Sie eine vom Kunden verwaltete Richtlinie

Um Ihrer Rolle Berechtigungen zu gewähren, können Sie entweder eine AWS-verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie verwenden.

> **Tip**
>
> Wenn Sie eine Richtlinie nicht manuell erstellen möchten, empfehlen wir stattdessen, dass Sie eine AWS-verwaltete Richtlinie verwenden und diesen Vorgang überspringen. Verwaltete Richtlinien verfügen automatisch über die erforderlichen Berechtigungen für die AWS Support-App. Sie müssen die Richtlinien nicht manuell aktualisieren. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Support Apps in Slack.

Gehen Sie wie folgt vor, um eine vom Kunden verwaltete Richtlinie für Ihre Rolle zu erstellen. Dieses Verfahren verwendet den JSON-Richtlinieneditor in der IAM-Konsole.

So erstellen Sie eine vom Kunden verwaltete Richtlinie für die AWS Support-App

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies.
3. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie den Tab JSON.
5. Geben Sie Ihren JSON ein und ersetzen Sie dann den Standard-JSON im Editor. Sie können die Beispielrichtlinie verwenden.
6. Wählen Sie Next: Markierungen (Weiter: Markierungen).
7. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Richtlinie Metadaten hinzuzufügen.
8. Wählen Sie Weiter: Prüfen aus.
9. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Name (Namen), z. B. *AWSSupportAppRolePolicy*, und eine Description (Beschreibung) (optional) ein.
10. Überprüfen Sie die Seite Summary (Zusammenfassung), um die Berechtigungen anzuzeigen, die die Richtlinie zulässt, und wählen Sie dann Create policy (Richtlinie erstellen) aus.

Diese Richtlinie definiert die Aktionen, die die Rolle ausführen kann. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Beispiel für eine IAM-Richtlinie

Sie können die folgende Beispielrichtlinie Ihrer IAM-Rolle anfügen. Diese Richtlinie lässt der Rolle vollständige Berechtigungen für alle erforderlichen Aktionen für die AWS Support-App zu. Nachdem Sie einen Slack-Kanal mit der Rolle konfiguriert haben, verfügt jeder Benutzer in Ihrem Kanal über die gleichen Berechtigungen.

> **Note**
>
> Eine Liste der AWS-verwalteten Richtlinien finden Sie unter AWS verwaltete Richtlinien für AWS Support Apps in Slack.

Sie können die Richtlinie aktualisieren, um eine Berechtigung aus der AWS Support-App zu entfernen.

```
{
    "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"}
            }
        }
    ]
}
```

Beschreibungen der einzelnen Aktionen finden Sie in den folgenden Themen in der Service-Autorisierungsreferenz:

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support
- Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity and Access Management

Erstellen Sie eine IAM-Rolle

Nachdem Sie die Richtlinie erstellt haben, müssen Sie eine IAM-Rolle erstellen und die Richtlinie dann dieser Rolle anhängen. Sie wählen diese Rolle aus, wenn Sie eine Slack-Kanalkonfiguration in der Support-Center-Konsole erstellen.

So erstellen Sie eine Rolle für die AWS Support-App

1. Melden Sie sich bei der AWS Management Console an und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).
3. Wählen Sie für Select trusted entity (Vertrauenswürdige Entität auswählen) die Option AWS-Service aus.
4. Wählen Sie AWS Support-App aus.
5. Wählen Sie Next: Permissions (Weiter: Berechtigungen) aus.
6. Geben Sie den Richtliniennamen ein. Sie können die AWS-verwaltete Richtlinie oder eine von Ihnen erstellte vom Kunden verwaltete Richtlinie auswählen, z. B. *AWSSupportAppRolePolicy*. Aktivieren Sie dann das Kontrollkästchen neben der Richtlinie.
7. Wählen Sie Next: Markierungen (Weiter: Markierungen).
8. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Rolle Metadaten hinzuzufügen.
9. Wählen Sie Weiter: Prüfen aus.
10. Geben Sie für Role name (Rollenname) einen Namen ein, z. B. *AWSSupportAppRole*.
11. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung für die Rolle ein.
12. Prüfen Sie die Rolle und klicken Sie dann auf Create Role (Rolle erstellen). Sie können diese Rolle jetzt auswählen, wenn Sie einen Slack-Kanal in der Support-Center-Konsole konfigurieren. Siehe Konfigurieren eines Slack-Kanals.

Weitere Informationen finden Sie unter Erstellen einer Rolle für einen AWS-Service im IAM-Benutzerhandbuch.

Fehlerbehebung

Informationen zum Verwalten des Zugriffs auf die AWS Support-App finden Sie in den folgenden Themen.

Inhalt

Ich möchte bestimmte Benutzer in meinem Slack-Kanal von bestimmten Aktionen einschränken

Standardmäßig verfügen Benutzer in Ihrem Slack-Kanal über die gleichen Berechtigungen, die in der IAM-Richtlinie angegeben sind, die Sie der von Ihnen erstellten IAM-Rolle zuordnen. Das bedeutet, dass jeder im Kanal Lese- oder Schreibzugriff auf Ihre Support-Fälle hat, unabhängig davon, ob er über einen AWS-Konto- oder einen IAM-Benutzer verfügt oder nicht.

Wir empfehlen Ihnen, die folgenden bewährten Methoden:

- Konfigurieren von privaten Slack-Kanälen mit der AWS Support-App
- Laden Sie nur Benutzer in Ihren Kanal ein, die Zugriff auf Ihre Support-Fälle benötigen
- Verwenden Sie eine IAM-Richtlinie, die über die minimal erforderlichen Berechtigungen für die AWS Support-App verfügt. Siehe AWS verwaltete Richtlinien für AWS Support Apps in Slack.

Wenn ich einen Slack-Kanal konfiguriere, wird die von mir erstellte IAM-Rolle nicht angezeigt

Wenn Ihre IAM-Rolle nicht in der Liste IAM role for the AWS Support App (IAM-Rolle für die -App angezeigt wird), bedeutet dies, dass die Rolle die AWS Support-App nicht als vertrauenswürdige Entität enthält oder dass die Rolle gelöscht wurde. Sie können die vorhandene Rolle aktualisieren oder eine neue erstellen. Siehe Erstellen Sie eine IAM-Rolle.

Meiner IAM-Rolle fehlt eine Berechtigung

Die IAM-Rolle, die Sie für Ihren Slack-Kanal erstellen, benötigt Berechtigungen, um die von Ihnen gewünschten Aktionen durchzuführen. Wenn Sie beispielweise möchten, dass Ihre Benutzer in Slack Support-Fälle erstellen, muss die Rolle über die `support:CreateCase`-Berechtigung verfügen. Die AWS Support-App übernimmt diese Rolle, um diese Aktionen für Sie durchzuführen.

Wenn Sie von der AWS Support-App eine Fehlermeldung über eine fehlende Berechtigung erhalten, überprüfen Sie, ob die Ihrer Rolle zugeordnete Richtlinie über die erforderliche Berechtigung verfügt.

Lesen Sie das vorhergehende Beispiel für eine IAM-Richtlinie.

Eine Slack-Fehlermeldung besagt, dass meine IAM-Rolle nicht gültig ist

Stellen Sie sicher, dass Sie die richtige Rolle für Ihre Kanalkonfiguration ausgewählt haben.

Überprüfen Sie Ihre Rolle wie folgt

1. Melden Sie sich im AWS Support Center Console auf der Seite https://console.aws.amazon.com/support/app#/config an.
2. Wählen Sie den Kanal, den Sie mit der AWS Support-App konfiguriert haben.
3. Suchen Sie im Abschnitt Permissions (Berechtigungen) nach dem von Ihnen gewählten IAM-Rollennamen.
    - Um die Rolle zu ändern, wählen Sie Edit (Bearbeiten), wählen Sie eine andere Rolle und wählen Sie dann Save (Speichern) aus.
    - Um die Rolle oder die der Rolle zugeordneten Richtlinie zu aktualisieren, melden Sie sich in der IAM-Konsole an.

Die AWS Support-App besagt, dass mir eine IAM-Rolle für Service Quotas fehlt

Sie müssen in Ihrem Konto über die `AWSServiceRoleForServiceQuotas`-Rolle verfügen, um Kontingenterhöhungen aus Service Quotas anzufordern. Wenn Sie eine Fehlermeldung über eine fehlende Ressource erhalten, führen Sie einen der folgenden Schritte aus:

- Zum Anfordern einer Erhöhung des Kontingents können Sie die Konsole Service Quotas verwenden. Nachdem Sie eine erfolgreiche Anfrage gestellt haben, erstellt Service Quotas diese Rolle automatisch für Sie. Anschließend können Sie die AWS Support-App verwenden, um in Slack eine Erhöhung des Kontingents anzufordern. Weitere Informationen finden Sie unter Anfordern einer Kontingenterhöhung.
- Aktualisieren Sie die IAM-Richtlinie, die Ihrer Rolle zugeordnet ist. Dadurch wird der Rolle die Berechtigung für Service Quotas gewährt. Der folgende Abschnitt im Beispiel für eine IAM-Richtlinie ermöglicht es der AWS Support-App, die Rolle Service Quotas für Sie zu erstellen.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
    }
}
```

Wenn Sie die für Ihren Kanal konfigurierte IAM-Rolle löschen, müssen Sie die Rolle manuell erstellen oder die IAM-Richtlinie aktualisieren, damit die AWS Support-App eine Rolle für Sie erstellen kann.

Autorisieren eines Slack-Workspaces

Nachdem Sie Ihren Workspace autorisiert und der AWS Support-App die Zugriffsberechtigung erteilt haben, benötigen Sie eine AWS Identity and Access Management (IAM)-Rolle für Ihr AWS-Konto. Die AWS Support-App verwendet diese Rolle, um API-Operationen von AWS Support und Service Quotas für Sie aufzurufen. Zum Beispiel verwendet die AWS Support-App die Rolle, um die `CreateCase`-Operation zum Erstellen eines Support-Falls für Sie in Slack aufzurufen.

Hinweise

- Der Slack-Kanal übernimmt Berechtigungen von der IAM-Rolle. Das bedeutet, dass jeder Benutzer im Slack-Kanal über dieselben Berechtigungen verfügt, die in der IAM-Richtlinie angegeben sind, die der Rolle zugeordnet ist.

  Wenn Ihre IAM-Richtlinie beispielsweise der Rolle vollständige Lese- und Schreibberechtigungen für Ihre Support-Fälle zulässt, kann jeder in Ihrem Slack-Kanal Ihre Support-Fälle erstellen, aktualisieren und lösen. Wenn Ihre IAM-Richtlinie der Rolle schreibgeschützte Berechtigungen zulässt, haben Benutzer in Ihrem Slack-Kanal nur Leseberechtigungen für Ihre Support-Fälle.
- Wir empfehlen, dass Sie die Slack-Workspaces und -Kanäle hinzufügen, die Sie zum Verwalten Ihrer Support-Operationen benötigen. Wir empfehlen Ihnen, private Kanäle zu konfigurieren und nur erforderliche Benutzer einzuladen.

Sie müssen jeden Slack-Workspace, den Sie für Ihr AWS-Konto verwenden möchten, autorisieren. Wenn Sie über mehrere AWS-Konten verfügen, müssen Sie sich bei jedem Konto anmelden und das folgende Verfahren wiederholen, um den Workspace zu autorisieren. Wenn Ihr Konto zu einer Organisation in AWS Organizations gehört und Sie mehrere Konten autorisieren möchten, fahren Sie mit Autorisieren mehrerer Konten fort.

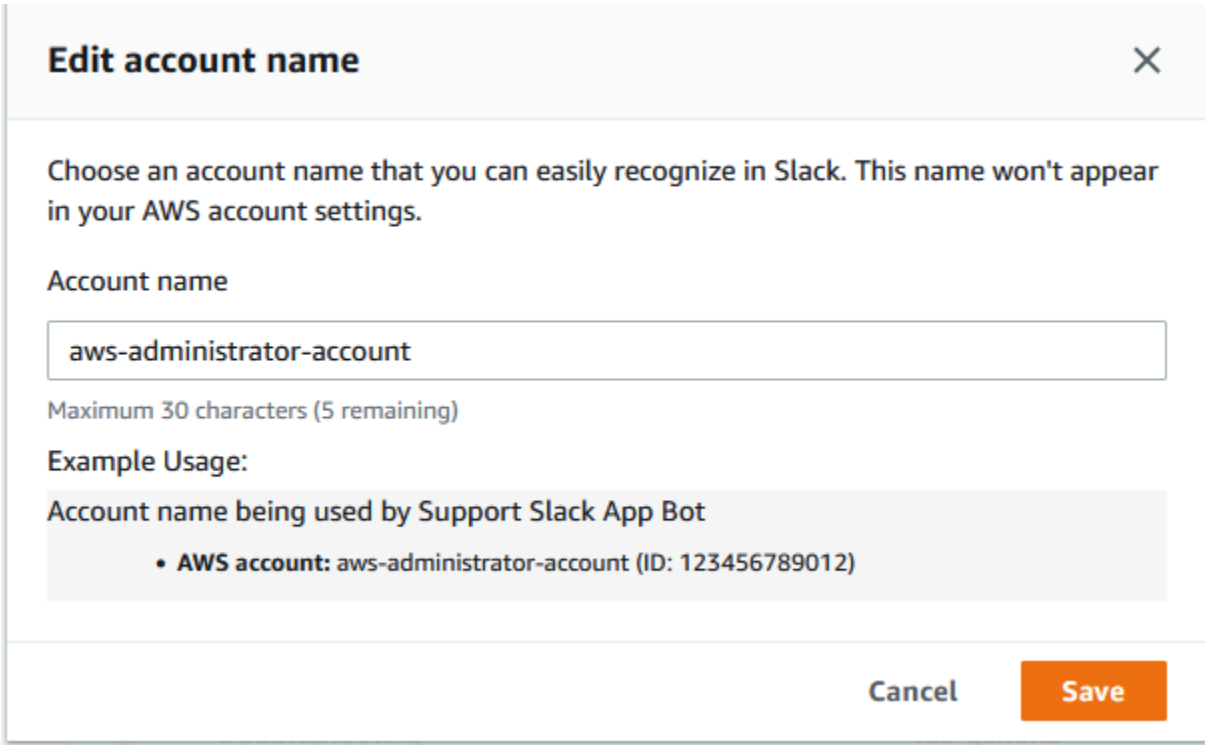
Autorisieren Sie wie folgt den Slack-Workspace für Ihr AWS-Konto

1. Melden Sie sich in der AWS Support Center Console an und wählen Sie Slack configuration (Slack-Konfiguration) aus.
2. Wählen Sie auf der Seite Getting started (Erste Schritte) die Option Authorize workspace (Workspace autorisieren) aus.
3. Wenn Sie noch nicht in Slack angemeldet sind, geben Sie auf der Seite Sign in to your workspace (In Ihrem Workspace anmelden) Ihren Workspace-Namen ein und wählen dann Continue (Weiter).
4. Wählen Sie auf der Seite AWS Support is requesting permission to access the your-workspace-name Slack (fordert die Erlaubnis zum Zugriff auf den Ihr-Workspace-Name-Slack an) die Option Allow (Zulassen) aus.

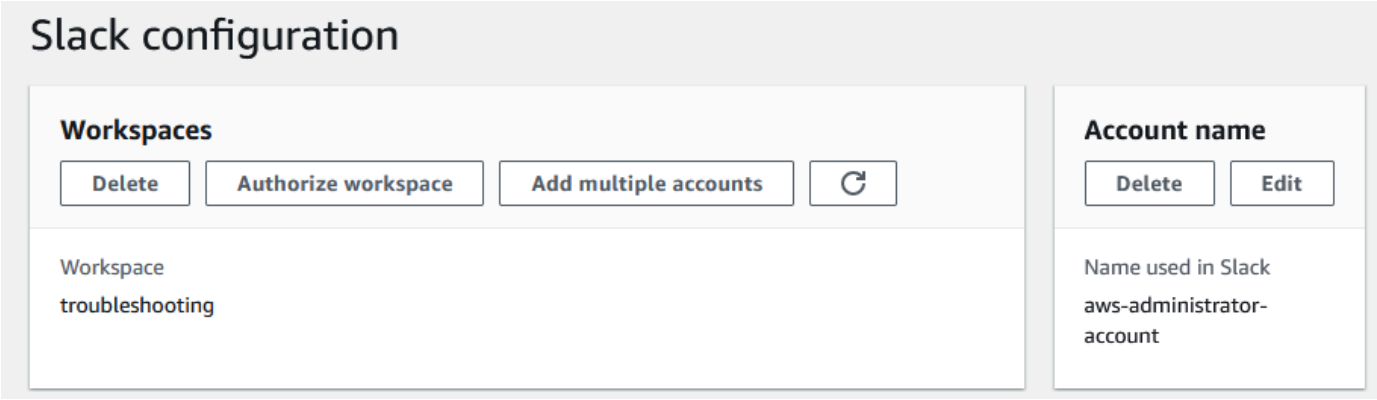
   > **Note**
   >
   > Wenn Sie Slack keinen Zugriff auf Ihren Workspace gewähren können, stellen Sie sicher, dass Sie von Ihrem Slack-Administrator die Berechtigung erhalten, die AWS Support-App zum Workspace hinzuzufügen. Siehe Voraussetzungen.

   Auf der Seite Slack configuration (Slack-Konfiguration) wird Ihr Workspace-Name unter Workspaces angezeigt.
5. (Optional) Um weitere Workspaces hinzuzufügen, wählen Sie Authorize workspace (Workspace autorisieren) und wiederholen Sie die Schritte 3–4. Sie können bis zu fünf Workspaces zu Ihrem Konto hinzufügen.
6. (Optional) Standardmäßig wird Ihre AWS-Konto-ID-Nummer als Kontoname in Ihrem Slack-Kanal angezeigt. Um diesen Wert zu ändern, wählen Sie unter Account name (Kontoname) die Option Edit (Bearbeiten) aus, geben Sie Ihren Kontonamen ein und wählen Sie dann Save (Speichern).

   > **Tip**
   >
   > Verwenden Sie einen Namen, den Sie und Ihr Team leicht erkennen können. Die AWS Support-App verwendet diesen Namen, um Ihr Konto in dem Slack-Kanal zu identifizieren. Sie können diesen Namen jederzeit aktualisieren.



Ihr Workspace und Ihr Kontoname werden auf der Seite Slack configuration (Slack-Konfiguration) angezeigt.



Autorisieren mehrerer Konten

Um mehrere AWS-Konten zur Nutzung von Slack-Workspaces zu autorisieren, können Sie AWS CloudFormation oder Terraform verwenden, um Ihre AWS Support-App-Ressourcen zu erstellen.

Konfigurieren eines Slack-Kanals

Nachdem Sie Ihren Slack-Workspace autorisiert haben, können Sie Ihre Slack-Kanäle für die Verwendung der AWS Support-App konfigurieren.

Der Kanal, in dem Sie die AWS Support-App einladen und hinzufügen, ist der Ort, an dem Sie Fälle erstellen und suchen sowie Fall-Benachrichtigungen erhalten können. In diesem Kanal werden Aktualisierungen von Fällen angezeigt, z. B. neu erstellte oder gelöste Fälle, hinzugefügte Korrespondenzen und gemeinsame Falldetails.

Der Slack-Kanal übernimmt Berechtigungen von der IAM-Rolle. Das bedeutet, dass jeder Benutzer im Slack-Kanal über dieselben Berechtigungen verfügt, die in der IAM-Richtlinie angegeben sind, die der Rolle zugeordnet ist.

Wenn Ihre IAM-Richtlinie beispielsweise der Rolle vollständige Lese- und Schreibberechtigungen für Ihre Support-Fälle zulässt, kann jeder in Ihrem Slack-Kanal Ihre Support-Fälle erstellen, aktualisieren und lösen. Wenn Ihre IAM-Richtlinie der Rolle schreibgeschützte Berechtigungen zulässt, haben Benutzer in Ihrem Slack-Kanal nur Leseberechtigungen für Ihre Support-Fälle.

Sie können bis zu 20 Kanäle für ein Konto hinzufügen. Ein Slack-Kanal kann bis zu 100 AWS-Konten enthalten. Das bedeutet, dass nur 100 Konten denselben Slack-Kanal zur AWS Support-App hinzufügen können. Wir empfehlen Ihnen, nur die Konten hinzuzufügen, die Sie für die Verwaltung von Support-Fällen in Ihrem Unternehmen benötigen. Dadurch kann die Anzahl der Benachrichtigungen, die Sie im Kanal erhalten, reduziert werden, so dass Sie und Ihr Team weniger abgelenkt werden.

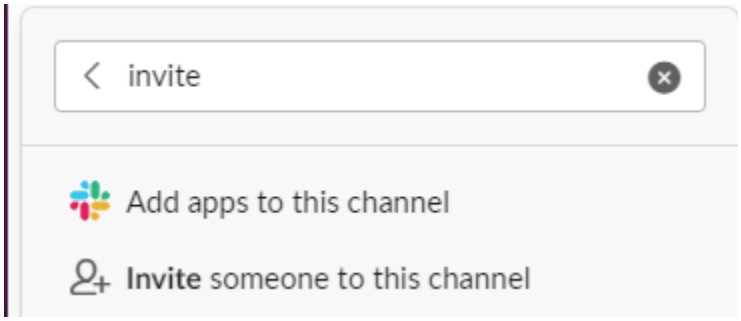
Jedes AWS-Konto muss in der AWS Support-App separat einen Slack-Kanal konfigurieren. Auf diese Weise kann die AWS Support-App auf die Support-Fälle in diesem AWS-Konto zugreifen. Wenn ein anderes AWS-Konto in Ihrer Organisation die AWS Support-App bereits zu diesem Slack-Kanal eingeladen hat, fahren Sie mit Schritt 3 fort.

> **Note**
>
> Sie können Channels konfigurieren, die Teil von Slack Connect sind, und Channels, die mit mehreren Workspaces geteilt werden. Allerdings kann nur der erste Workspace, der den geteilten Channel für ein AWS-Konto konfiguriert hat, die AWS Support-App verwenden. Die AWS Support-App gibt eine Fehlermeldung zurück, wenn Sie versuchen, denselben Slack-Channel für einen anderen Workspace zu konfigurieren.

Konfigurieren Sie einen Slack-Kanal wie folgt

1. Wählen Sie in Ihrer Slack-Anwendung den Slack-Kanal aus, den Sie mit der AWS Support-App verwenden möchten.
2. Führen Sie die folgenden Schritte aus, um die AWS Support-App in Ihren Kanal einzuladen:

   a. Wählen Sie das +-Symbol und geben Sie `invite` ein. Wählen Sie dann, wenn Sie dazu aufgefordert werden, Add apps to this channel (Apps zu diesem Kanal hinzufügen) aus.

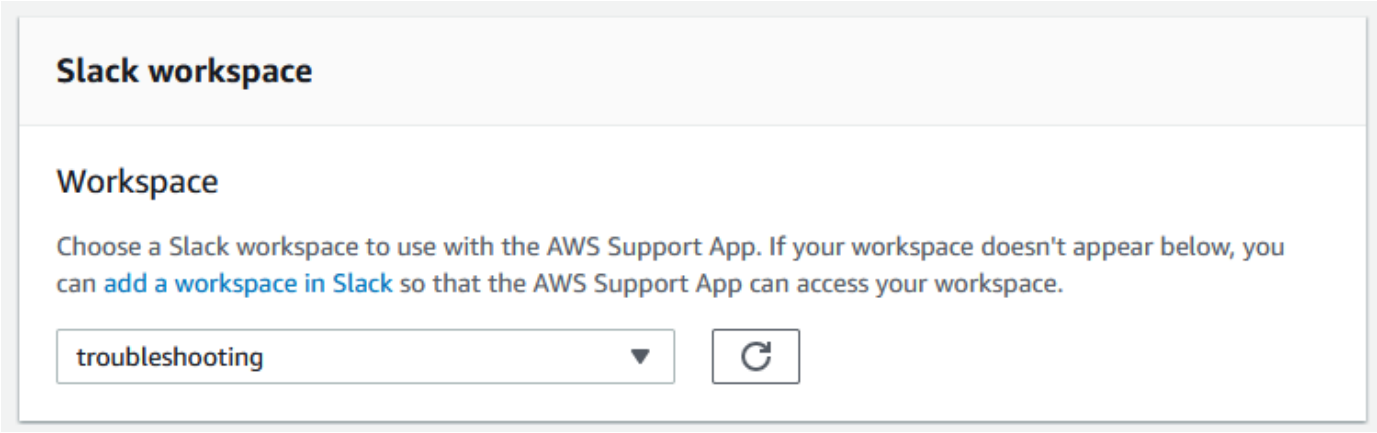
   

   b. Um nach der App zu suchen, geben Sie unter Add apps to channelName (Apps zu ChannelName hinzufügen) AWS Support App ein.

   c. Wählen Sie Add (Hinzufügen) neben der AWS Support App (-App) aus.

3. Melden Sie sich in der Support Center Console (Support-Center-Konsole) an und wählen Sie Slack configuration (Slack-Konfiguration) aus.
4. Wählen Sie Add channel (Kanal hinzufügen) aus.
5. Wählen Sie auf der Seite Add channel (Kanal hinzufügen) unter Workspace den Workspace-Namen aus, den Sie zuvor autorisiert haben. Wenn der Workspace-Name nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol aus.

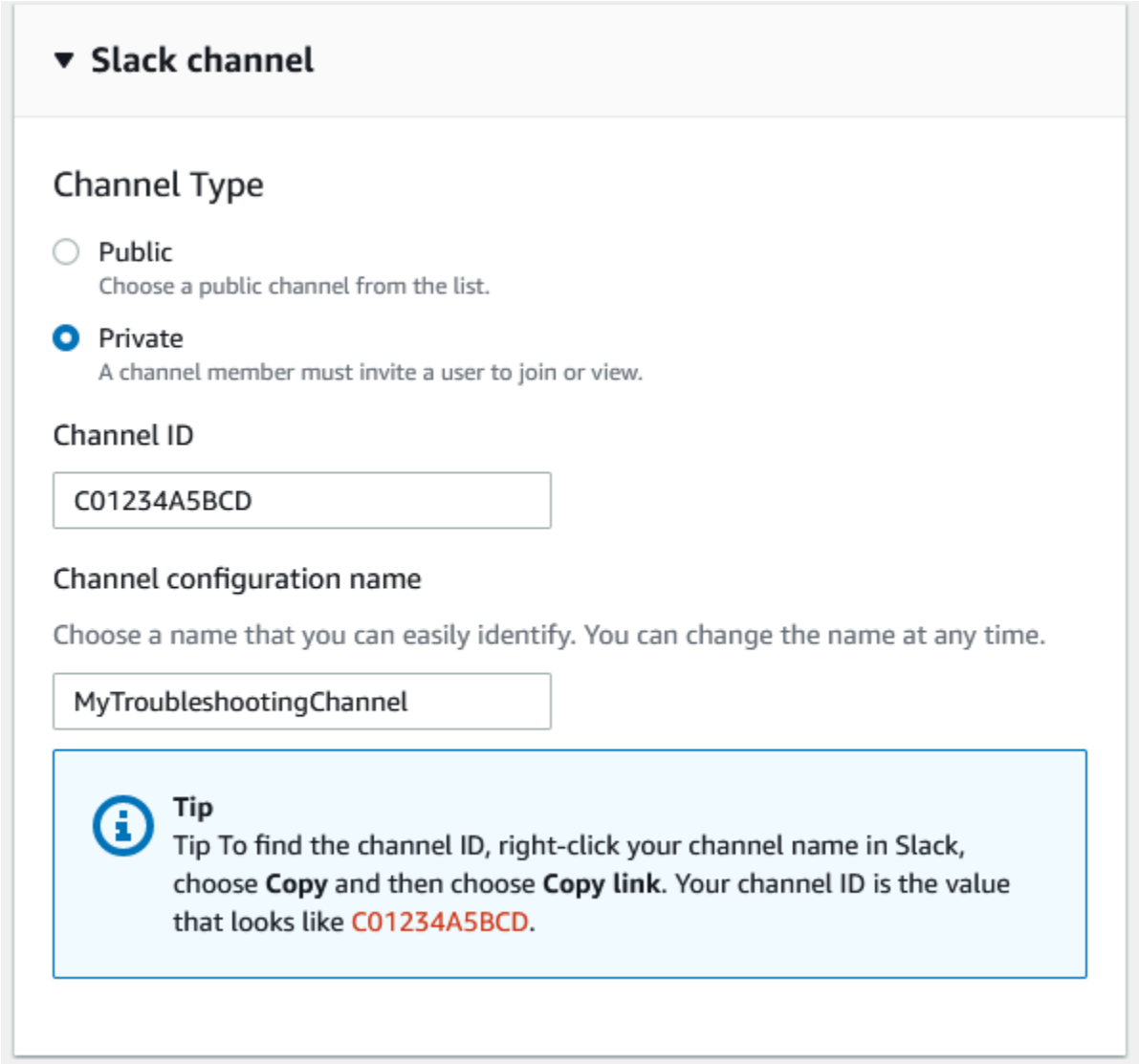


6. Wählen Sie unter Slack channel (Slack-Kanal) als Channel type (Kanaltyp) eine der folgenden Optionen aus:
   - Public (Öffentlich) – Wählen Sie unter Public channel (Öffentlicher Kanal) den Slack-Kanal aus, zu dem Sie die AWS Support-App eingeladen haben (Schritt 2). Wenn Ihr Kanal nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol und versuchen Sie es erneut.
   - Private (Privat) – Geben Sie unter Channel ID (Kanal-ID) die ID oder die URL des Slack-Kanals ein, zu dem Sie die AWS Support-App eingeladen haben.

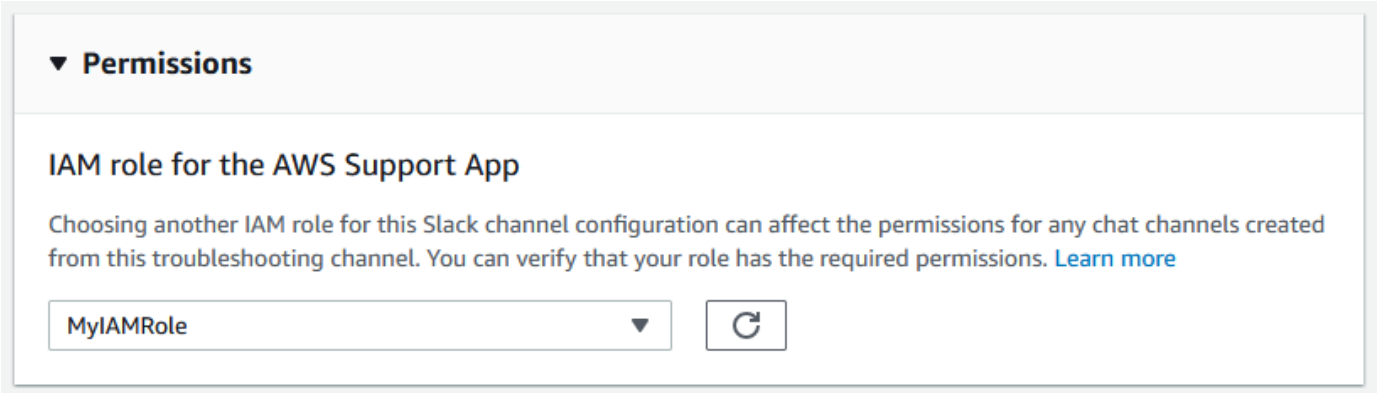
     > **Tip**
     >
     > Um die Kanal-ID zu finden, öffnen Sie das Kontextmenü (Rechtsklick) für den Kanalnamen in Slack und wählen Sie Copy (Kopieren) und dann Copy link (Link kopieren) aus. Ihre Kanal-ID ist der Wert, der wie folgt aussieht: `C01234A5BCD`.

7. Geben Sie unter Channel configuration name (Name der Kanalkonfiguration) einen Namen ein, der Ihre Slack-Kanalkonfiguration für die AWS Support-App leicht identifiziert. Dieser Name ist nur in Ihrem AWS-Konto sichtbar und wird nicht in Slack angezeigt. Sie können Ihre Kanalkonfiguration später umbenennen.

   Ihr Slack-Kanaltyp könnte wie im folgenden Beispiel aussehen.



8. Wählen Sie unter Permissions (Berechtigungen) für die IAM role for the AWS Support App in Slack (IAM-Rolle für die -App in Slack) eine Rolle aus, die Sie für die AWS Support-App erstellt haben. In der Liste werden nur Rollen angezeigt, die die AWS Support-App als vertrauenswürdige Entität enthalten.



> **Note**
>
> Wenn Sie keine Rolle erstellt haben oder Ihre Rolle nicht in der Liste angezeigt wird, finden Sie weitere Informationen unter Verwalten des Zugriffs auf die AWS Support-App.

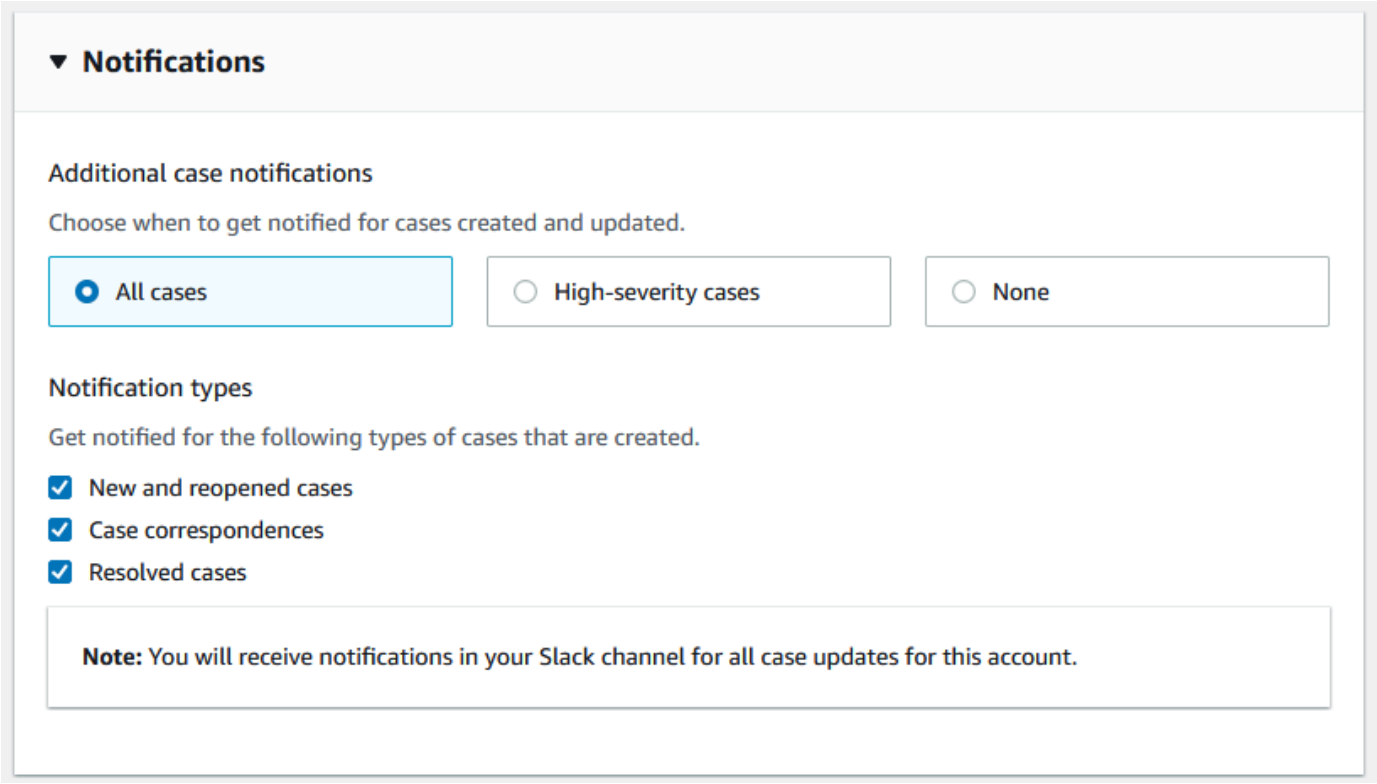
9. Geben Sie unter Notifications (Benachrichtigungen) an, wie Sie über Fälle benachrichtigt werden möchten.

   - All cases (Alle Fälle) – Lassen Sie sich über alle Fall-Aktualisierungen benachrichtigen.
   - High-severity cases (Fälle mit hohem Schweregrad) – Lassen Sie sich nur bei Fällen benachrichtigen, die ein Produktionssystem oder höher betreffen. Weitere Informationen finden Sie unter Auswahl eines Schweregrads.
   - None (Keine) – Lassen Sie sich nicht über Fall-Aktualisierungen benachrichtigen.

10. (Optional) Wenn Sie All cases (Alle Fälle) oder High-severity cases (Fälle mit hohem Schweregrad) auswählen, müssen Sie mindestens eine der folgenden Optionen auswählen:

    - New and reopened cases (Neue und wieder aufgenommene Fälle)
    - Case correspondences (Fall-Korrespondenzen)
    - Resolved cases (Gelöste Fälle)

    Der folgende Kanal erhält Fall-Benachrichtigungen für alle Fall-Aktualisierungen in Slack.



11. Überprüfen Sie Ihre Konfiguration und wählen Sie Add channel (Kanal hinzufügen) aus. Ihr Kanal wird auf der Seite Slack configuration (Slack-Konfiguration) angezeigt.

Aktualisieren Ihrer Slack-Kanalkonfiguration

Nachdem Sie Ihren Slack-Kanal konfiguriert haben, können Sie ihn später aktualisieren, um die IAM-Rolle oder die Fall-Benachrichtigung zu ändern.

Aktualisieren Sie Ihre Slack-Kanalkonfiguration wie folgt

1. Melden Sie sich in der Support Center Console (Support-Center-Konsole) an und wählen Sie Slack configuration (Slack-Konfiguration) aus.
2. Wählen Sie unter Channels (Kanäle) die gewünschte Kanalkonfiguration aus.
3. Auf der Seite ***channelName*** können Sie die folgenden Aufgaben ausführen:
   - Wählen Sie Rename (Umbenennen), um den Namen Ihrer Kanalkonfiguration zu aktualisieren. Dieser Name ist nur in Ihrem AWS-Konto sichtbar und wird nicht in Slack angezeigt.
   - Wählen Sie Delete (Löschen), um die Kanalkonfiguration aus der AWS Support-App zu löschen. Siehe Löschen einer Slack-Kanalkonfiguration aus der AWS Support-App.

- Wählen Sie Open in Slack (In Slack öffnen), um den Slack-Kanal in Ihrem Browser zu öffnen.
- Wählen Sie Edit (Bearbeiten), um die IAM-Rolle oder die Benachrichtigungen zu ändern.

Erstellen von Support-Fällen in einem Slack-Kanal

Nachdem Sie Ihren Slack-Workspace autorisiert und Ihren Slack-Kanal hinzugefügt haben, können Sie einen Support-Fall in Ihrem Slack-Kanal erstellen.

Erstellen Sie einen Support-Fall in Slack wie folgt

1. Geben Sie in Ihrem Slack-Kanal den folgenden Befehl ein:

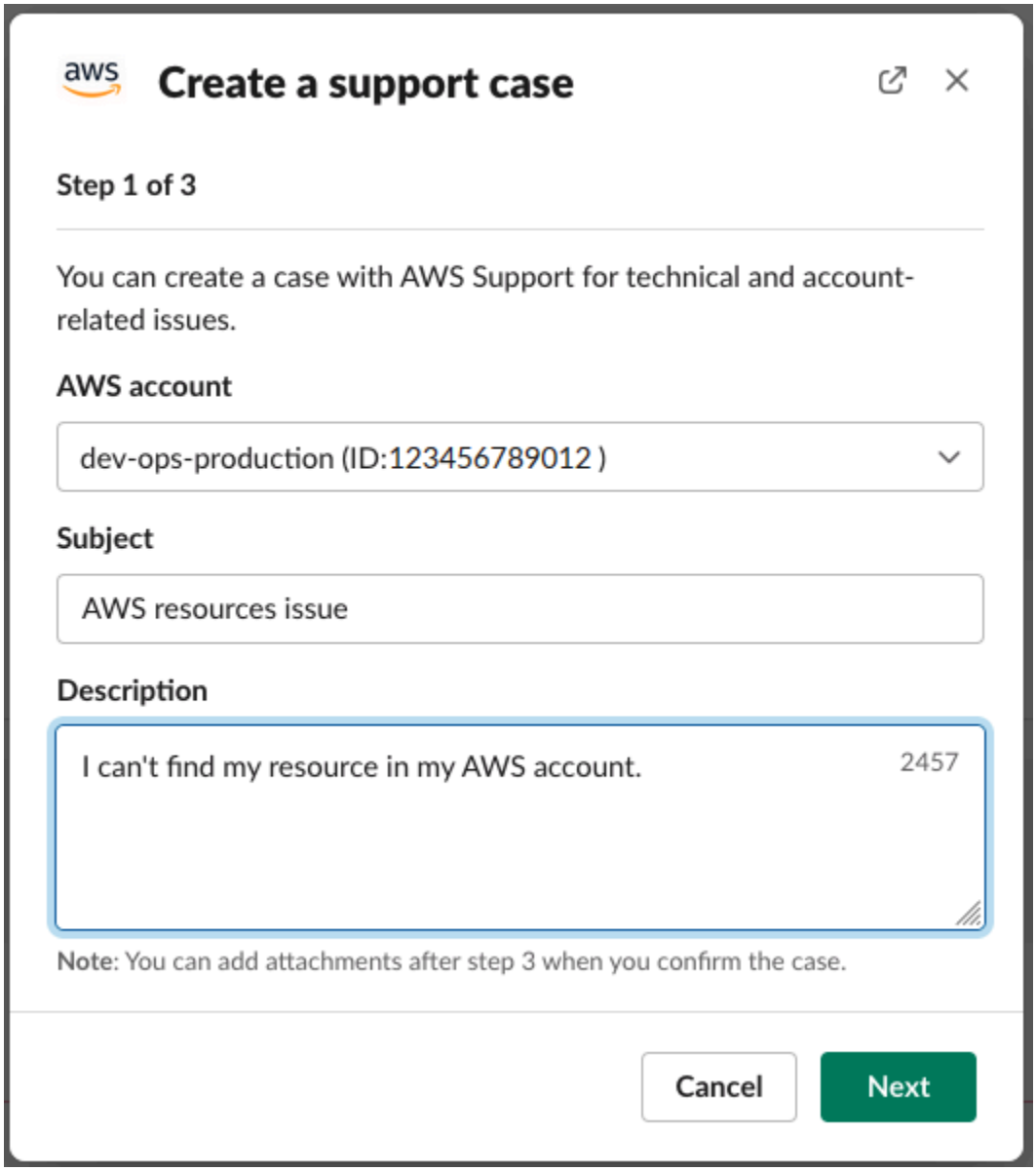
   ```
   /awssupport create
   ```

2. Gehen Sie im Dialogfenster Create a support case (Einen Support-Fall erstellen) wie folgt vor:

   a. Wenn Sie mehr als ein Konto für diesen Slack-Kanal konfiguriert haben, wählen Sie für AWS-Konto die Konto-ID aus. Wenn Sie einen Kontonamen erstellt haben, wird dieser Wert neben der Konto-ID angezeigt. Weitere Informationen finden Sie unter Autorisieren eines Slack-Workspaces.

   b. Geben Sie unter Subject (Betreff) einen Titel für den Support-Fall ein.

   c. Beschreiben Sie unter Description (Beschreibung) den Support-Fall. Geben Sie Details an, z. B. dass Sie AWS-Service verwenden und welche Schritte zur Fehlerbehebung Sie versucht haben.



3. Wählen Sie Next (Weiter).
4. Legen Sie im Dialogfenster Create a support case (Einen Support-Fall erstellen) die folgenden Optionen fest:

   a. Wählen Sie den Issue type (Problemtyp) aus.

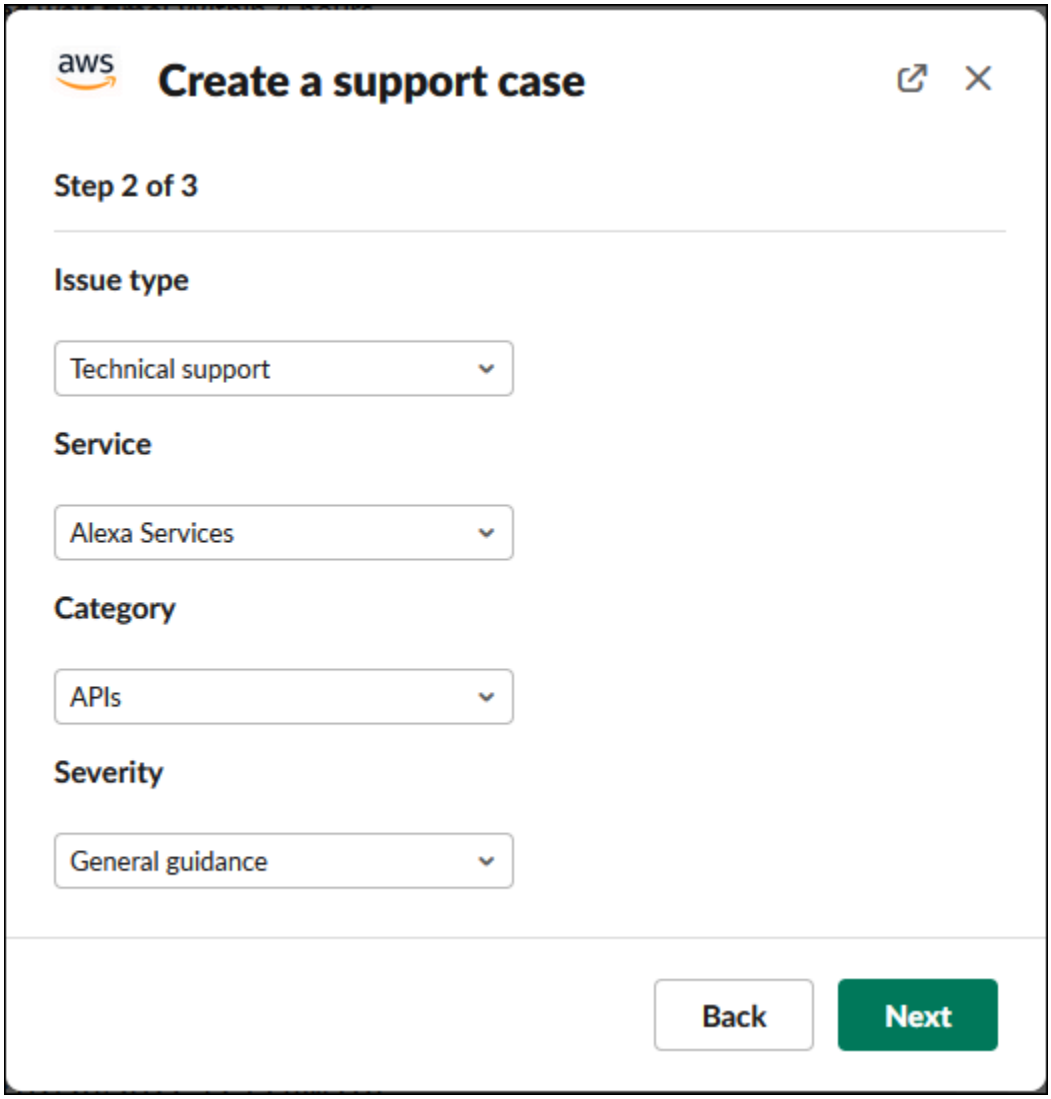
   b. Wählen Sie den Service aus.

   c. Wählen Sie die Category (Kategorie) aus.

   d. Wählen Sie den Severity (Schweregrad) aus.

   e. Überprüfen Sie Ihre Falldetails und wählen Sie Next (Weiter).

      Das folgende Beispiel zeigt einen technischen Support-Fall für Alexa-Services.

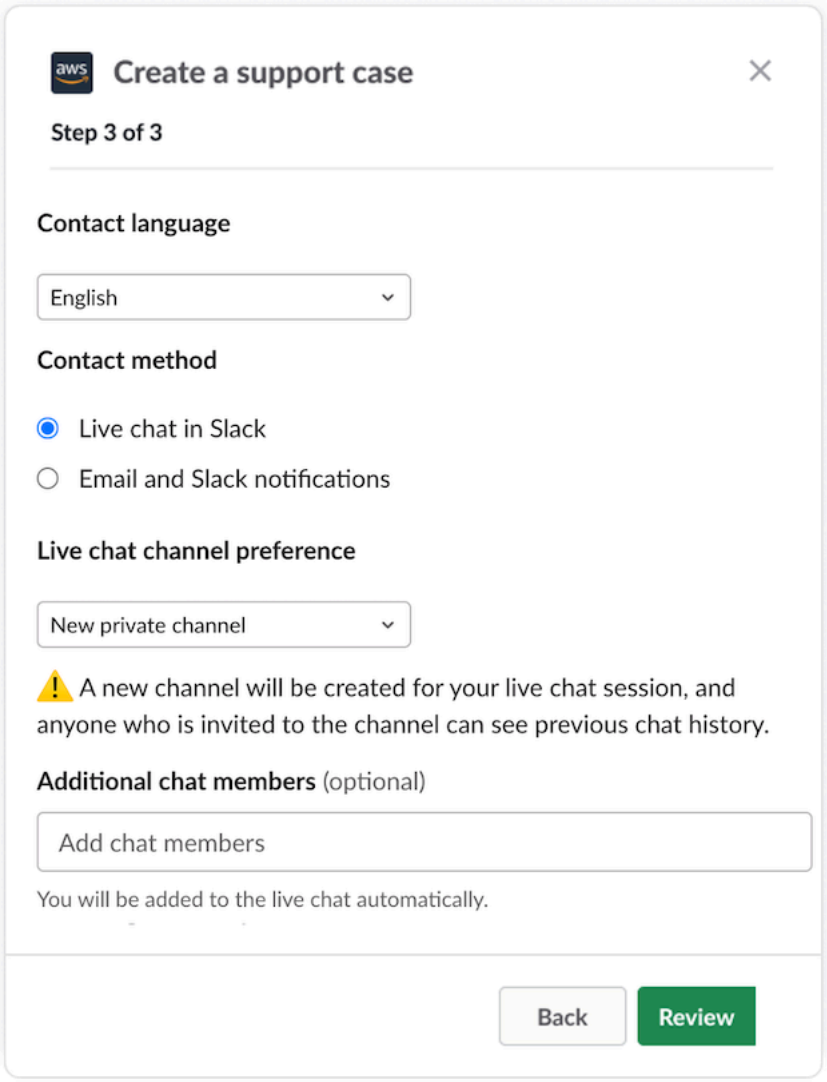


5. Geben Sie unter Contact Language (Kontaktsprache) Ihre für den Support-Fall bevorzugte Sprache an.

> **Note**
>
> Japanischer Sprachsupport ist für den Live-Chat in Slack für Konto- und Rechnungsangelegenheiten nicht verfügbar.

6. Wählen Sie als Contact method (Kontaktmethode) die Option Email and Slack notifications (E-Mail- und Slack-Benachrichtigungen) oder Live chat in Slack (Live-Chat in Slack) aus.

   Das folgende Beispiel zeigt, wie Sie den Live-Chat in Slack auswählen.



a. Wenn Sie den Live-Chat in Slack wählen, wählen Sie Neuer privater Kanal oder Aktueller Kanal als bevorzugten Live-Chat-Kanal. Neuer privater Kanal erstellt einen separaten privaten Kanal für Sie, um mit dem:der AWS Support-Kundendienstmitarbeiter:in zu chatten, und Aktueller Kanal verwendet einen Thread im aktuellen Kanal für Sie, um mit dem:der AWS Support-Kundendienstmitarbeiter:in zu chatten.

b. (Optional) Wenn Sie Live chat in Slack (Live-Chat in Slack) wählen, können Sie die Namen anderer Slack-Mitglieder eingeben. Bei Neuer privater Kanal fügt die AWS Support-App Sie und ausgewählte Mitglieder automatisch zu dem neuen Kanal hinzu. Für den aktuellen Kanal markiert die AWS Support-App automatisch Sie und ausgewählte Mitglieder im Chat-Thread, wenn der:die AWS Support-Kundendienstmitarbeiter:in beitritt.

> **Important**
>
> - Wir empfehlen Ihnen, nur Chat-Mitglieder hinzuzufügen, die Zugriff auf die Details Ihres Supportfalls und den Chatverlauf haben sollen.
> - Wenn Sie eine neue Live-Chat-Sitzung für einen bestehenden Supportfall starten, verwendet die AWS Support-App denselben Chat-Kanal oder Thread, der für einen vorherigen Live-Chat verwendet wurde. Die AWS Support-App verwendet außerdem denselben Live-Chat-Kanal wie zuvor.
> - Die Option Aktueller Kanal ist nur verfügbar, wenn der Chat aus einem privaten Kanal angefordert wird. Wir empfehlen Ihnen, diese Option nur zu verwenden, wenn Sie möchten, dass alle Mitglieder des Kanals Zugriff auf Ihren Chat haben.

7. (Optional) Geben Sie unter Additional contacts to notify (Zusätzliche zu benachrichtigende Kontakte) E-Mail-Adressen ein, die ebenfalls Updates zu diesem Support-Fall erhalten sollen. Sie können bis zu 10 E-Mail-Adressen hinzufügen.
8. Wählen Sie Review (Überprüfen).
9. Überprüfen Sie im Slack-Kanal die Falldetails. Sie haben die folgenden Möglichkeiten:
   - Wählen Sie Edit (Bearbeiten), um die Falldetails zu ändern.
   - Fügen Sie Ihrem Fall eine Datei hinzu. Führen Sie dazu die folgenden Schritte aus:
     a. Wählen Sie Attach file (Datei anhängen), wählen Sie das +-Symbol in Slack und wählen Sie Your computer (Mein Computer) aus.
     b. Navigieren Sie zu Ihrer Datei und wählen Sie sie aus.
     c. Geben Sie im Dialogfeld Upload a file (Datei hochladen) `@awssupport` ein und klicken Sie auf das Symbol Nachricht senden

     .

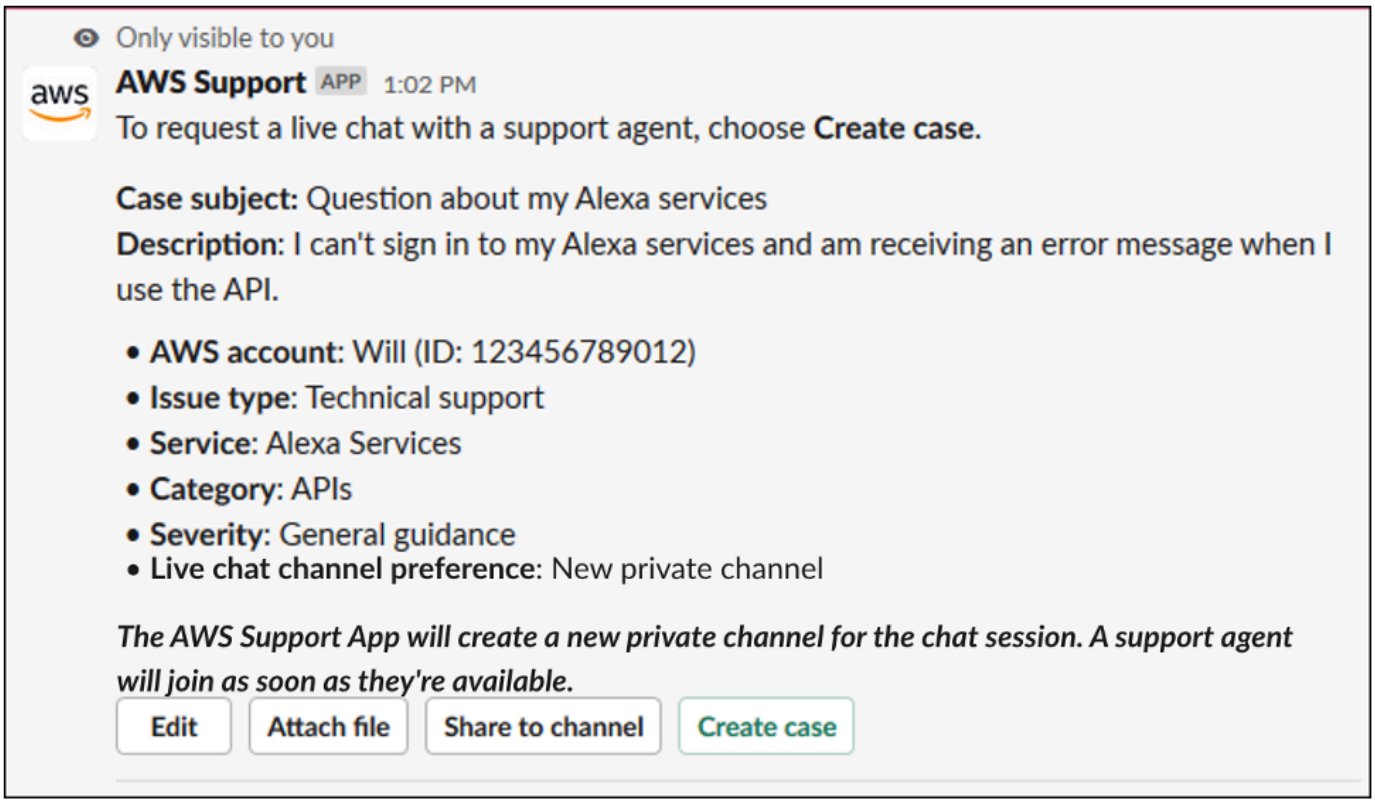
> **Hinweise**
>
> - Sie können bis zu 3 Dateien anfügen. Jede Datei kann bis zu 5 MB groß sein.

- Wenn Sie eine Datei an Ihren Support-Fall anfügen, müssen Sie Ihren Fall innerhalb von 1 Stunde einreichen. Andernfalls müssen Sie die Dateien erneut hinzufügen.

- Wählen Sie Share to channel (An Kanal freigeben), um die Falldetails mit anderen im Slack-Kanal zu teilen. Sie können diese Option verwenden, um die Falldetails für Ihr Team freizugeben, bevor Sie den Fall erstellen.

10. Überprüfen Sie Ihre Falldetails und wählen Sie dann Create case (Fall erstellen) aus.

    Das folgende Beispiel zeigt einen technischen Support-Fall für Alexa-Services.



    Nachdem Sie einen Support-Fall erstellt haben, kann es einige Minuten dauern, bis Ihre Falldetails sichtbar sind.

11. Wenn Ihr Support-Fall aktualisiert wird, können Sie See details (Details anzeigen) auswählen, um Ihre Fall-Informationen anzuzeigen. Sie können dann Folgendes durchführen:

    - Wählen Sie Share to channel (An Kanal freigeben), um die Falldetails mit anderen im Slack-Kanal zu teilen.
    - Wählen Sie Reply (Antworten), um eine Korrespondenz hinzuzufügen.
    - Wählen Sie Resolve case (Fall lösen).

> **Note**
>
> Wenn Sie in Slack keine automatischen Fall-Aktualisierungen gewählt haben, können Sie nach dem Support-Fall suchen, um die Option See details (Details anzeigen) zu finden.

Beantworten von Support-Fällen in Slack

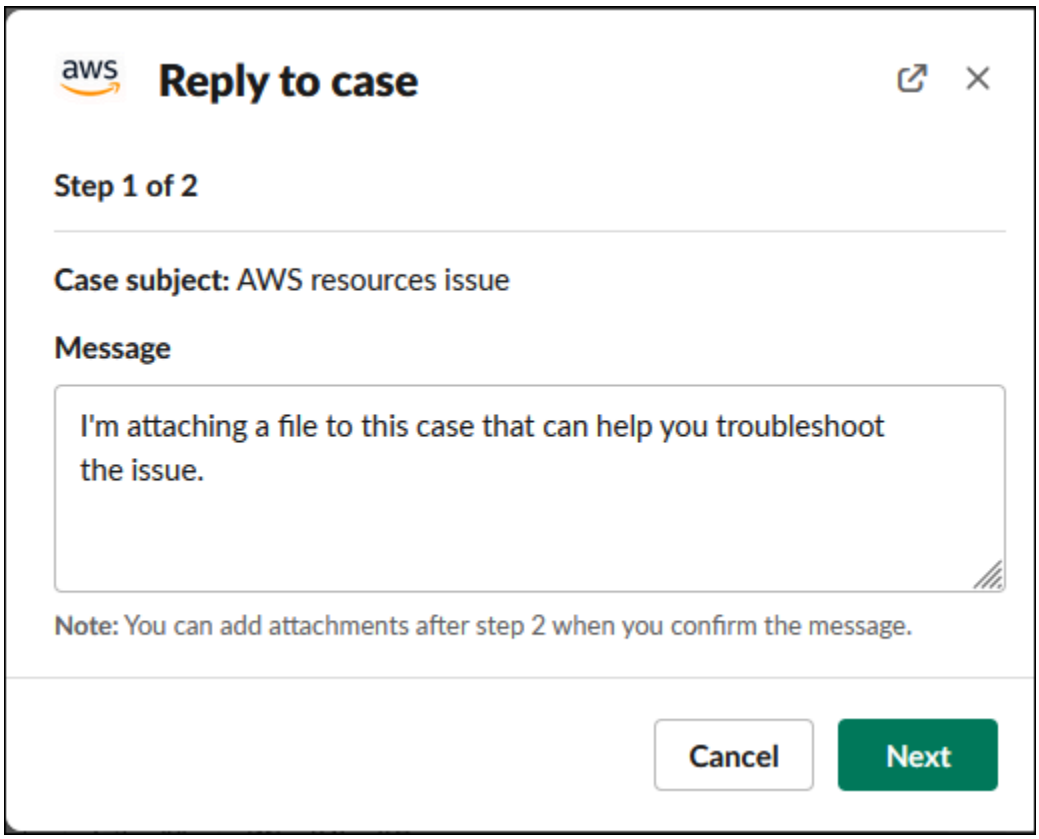
Sie können Aktualisierungen zu Ihrem Fall hinzufügen, z. B. Falldetails und Anhänge, und auf Antworten vom Kundendienstmitarbeiter reagieren.

> **Note**
>
> - Sie können auch die AWS Support Center Console nutzen, um auf Antworten vom Kundendienstmitarbeiter zu reagieren. Weitere Informationen finden Sie unter Aktualisierung, Lösung und Wiederaufnahme Ihres Falls.
> - Sie können keine Korrespondenzen zu Fällen aus von der AWS Support-App erstellten Chat-Kanälen hinzufügen. Live-Chat-Kanäle senden während des Live-Chats nur Nachrichten an Kundendienstmitarbeiter.

Antworten Sie auf einen Support-Fall in Slack wie folgt

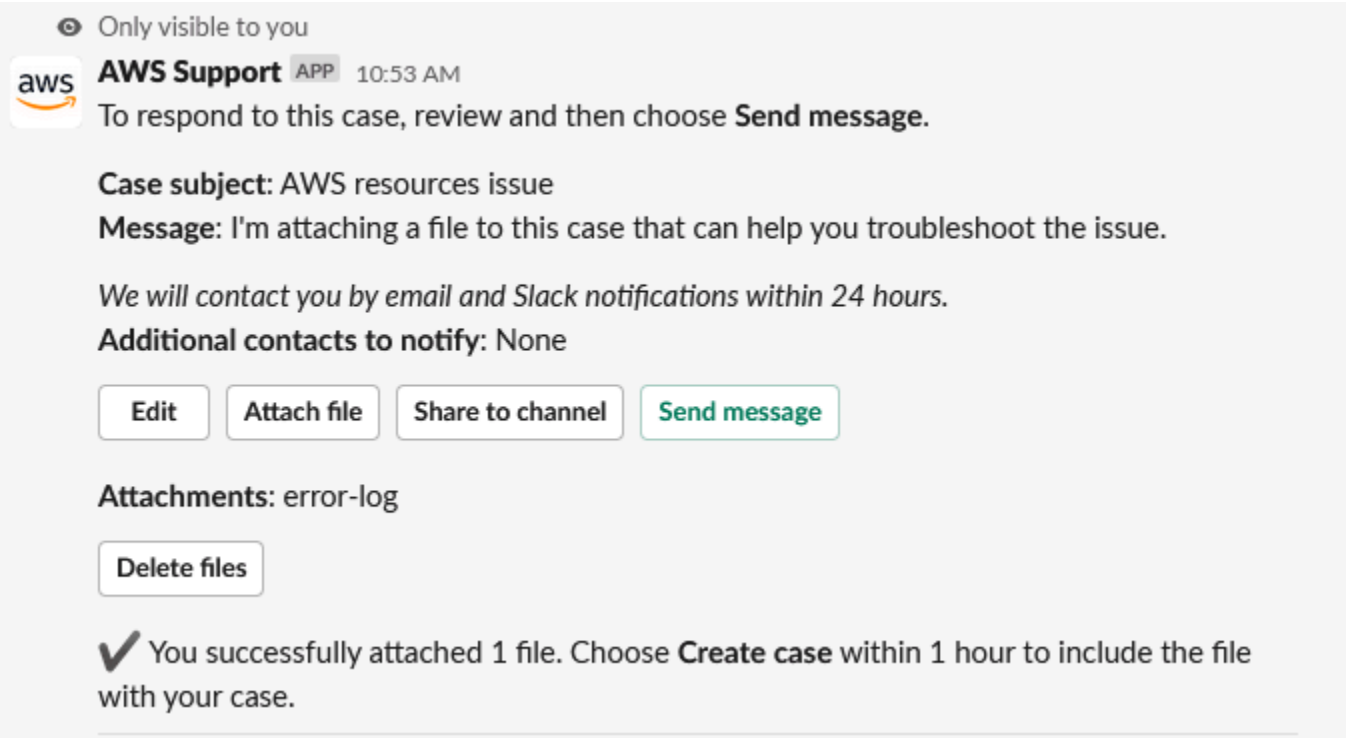
1. Wählen Sie in Ihrem Slack-Kanal den Fall, auf den Sie antworten möchten. Sie können `/awssupport search` eingeben, um Ihren Support-Fall zu finden.
2. Wählen Sie neben dem gewünschten Fall See details (Details anzeigen) aus.
3. Wählen Sie am Ende der Falldetails die Option Reply (Antworten) aus.

4. Geben Sie im Dialogfenster Reply to case (Auf den Fall antworten) eine kurze Beschreibung des Problems in das Feld Message (Nachricht) ein. Wählen Sie anschließend Next (Weiter).



5. Wählen Sie Ihre Kontaktmethode aus. Die verfügbaren Kontaktmethoden hängen von der Art Ihres Falles und Ihrem Support-Plan ab.
6. (Optional) Geben Sie für Additional contacts to notify (Zusätzliche zu benachrichtigende Kontakte) zusätzliche E-Mail-Adressen ein, die Sie über Aktualisierungen zu diesem Support-Fall informieren möchten. Sie können bis zu 10 E-Mail-Adressen hinzufügen.
7. Wählen Sie Review (Überprüfen). Sie können dann wählen, ob Sie Ihre Antwort bearbeiten, Dateien anfügen oder für den Kanal freigeben möchten.
8. Sobald Sie bereit sind zu antworten, wählen Sie Send message (Nachricht senden) aus.
9. (Optional) Um frühere Korrespondenz für Ihren Fall anzuzeigen, wählen Sie Previous correspondence (Frühere Korrespondenz). Um verkürzte Nachrichten anzuzeigen, wählen Sie Show full message (Vollständige Nachricht anzeigen).

Example : Antwort auf einen Fall in Slack



Nehmen Sie an einer Live-Chat-Sitzung teil mit AWS Support

Wenn du einen Live-Chat für deinen Fall anforderst, entscheidest du dich dafür, entweder einen neuen Chat-Kanal oder einen Thread im aktuellen Kanal für dich und den AWS Support Agenten zu verwenden. Verwenden Sie diesen Chat-Kanal oder Thread, um mit dem:der Support-Kundendienstmitarbeiter:in und anderen Personen zu kommunizieren, die Sie zum Live-Chat eingeladen haben.

> **Important**
>
> Jede Person, die einem Kanal mit einem Live-Chat beitritt, kann Details über den spezifischen Supportfall und den Chatverlauf einsehen. Es hat sich bewährt, nur Benutzer hinzuzufügen, die Zugriff auf Ihre Supportfälle benötigen. Jedes Mitglied eines Chat-Kanals oder Threads kann auch an einem aktiven Chat teilnehmen.

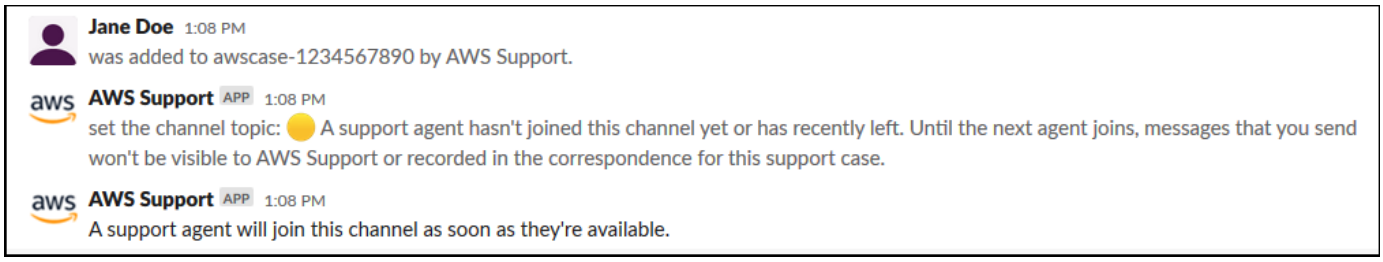
> **Note**
>
> Live-Chat-Kanäle und -Threads erhalten auch Benachrichtigungen, wenn dem Fall außerhalb der Live-Chat-Sitzung eine Korrespondenz hinzugefügt wird. Dies geschieht vor, während und nach einer Chat-Sitzung, sodass Sie einen Chat-Kanal oder einen Chat-Thread verwenden können, um alle Aktualisierungen für einen Fall zu überwachen. Wenn Sie sich für einen neuen Chat-Kanal entschieden haben, verwenden Sie den Konfigurationskanal, zu dem Sie die AWS Support App eingeladen haben, um auf diese Korrespondenzen zu antworten.

Um an einer Live-Chat-Sitzung AWS Support in einem neuen Kanal teilzunehmen

1. Navigiere in der Slack-Anwendung zu dem Channel, den die AWS Support App für dich erstellt. Der Kanalname enthält Ihre Support-Fall-ID, z. B. *awscase-1234567890*.

   > **Note**
   >
   > Die AWS Support App fügt dem Live-Chat-Kanal eine angeheftete Nachricht hinzu, die Details zu deinem Support-Fall enthält. Über die angeheftete Nachricht können Sie den Chat beenden oder den Fall lösen. Sie finden alle angehefteten Nachrichten in diesem Kanal unter dem Kanalnamen.

2. Wenn der Support-Kundendienstmitarbeiter dem Kanal beitritt, können Sie über Ihren Support-Fall chatten. Bis ein Support-Mitarbeiter dem Kanal beitritt, sieht der Agent keine Nachrichten in diesem Chat und die Nachrichten erscheinen auch nicht in Ihrer Fallkorrespondenz.

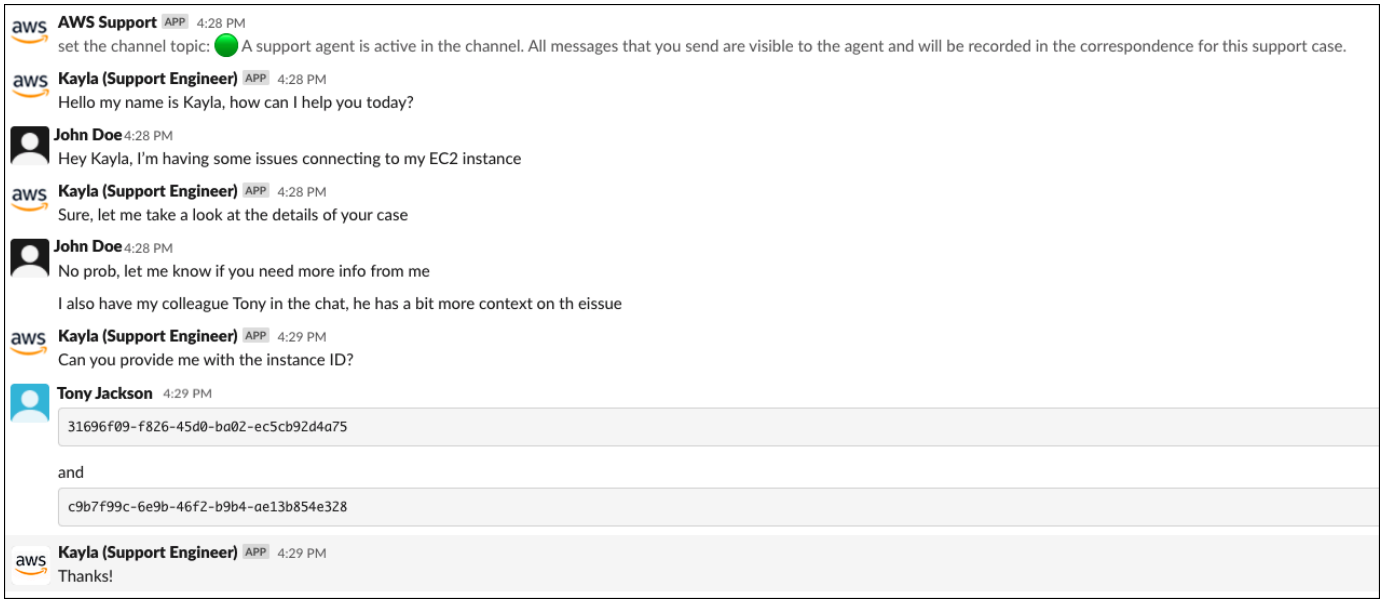
3. (Optional) Fügen Sie dem Chat-Kanal weitere Mitglieder hinzu. Chat-Kanäle sind standardmäßig privat.
4. Nachdem der Support-Kundendienstmitarbeiter dem Chat beigetreten ist, ist der Chat-Kanal aktiv und die AWS Support -App zeichnet den Chat auf.

Sie können mit dem Kundendienstmitarbeiter über Ihren Support-Fall chatten und beliebige Dateianhänge in den Kanal hochladen. Die AWS Support App speichert Ihre Dateien und das Chat-Protokoll automatisch in Ihrer Fallkorrespondenz.

> **Note**
>
> Wenn du mit einem Support-Mitarbeiter chattest, beachte die folgenden Unterschiede in Slack für die AWS Support App:
>
> - Support-Kundendienstmitarbeiter können freigegebene Nachrichten oder Threads nicht anzeigen. Um Text aus einer Nachricht oder einem Thread freizugeben, geben Sie den Text als neue Nachricht ein.
> - Wenn Sie eine Nachricht bearbeiten oder löschen, sieht der Kundendienstmitarbeiter weiterhin die ursprüngliche Nachricht. Sie müssen Ihre neue Nachricht erneut eingeben, um die Überarbeitung anzuzeigen.

Example : Live-Chat-Sitzung

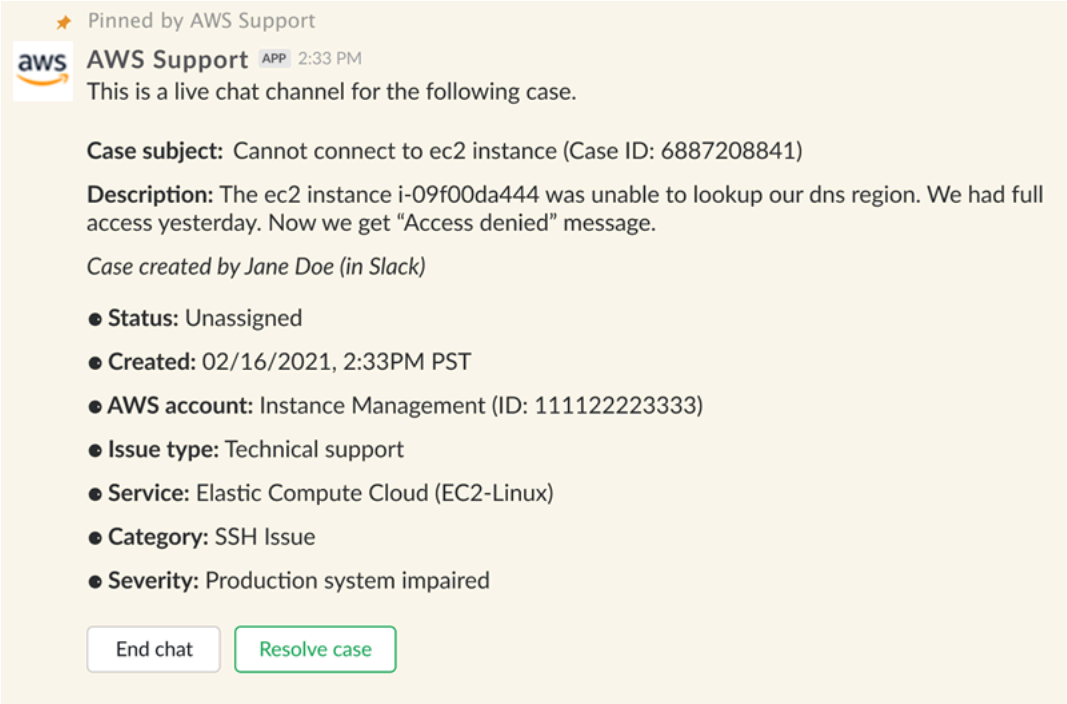
Im Folgenden finden Sie ein Beispiel für eine Live-Chat-Sitzung mit einem Support-Kundendienstmitarbeiter zur Behebung eines Verbindungsproblems für zwei Amazon Elastic Compute Cloud (Amazon EC2)-Instances.



5. (Optional) Um den Live-Chat zu beenden, wählen Sie End chat (Chat beenden) aus. Der Support-Mitarbeiter verlässt den Channel und die AWS Support App beendet die Aufzeichnung des Live-Chats. Den Chatverlauf finden Sie im Anhang der Fall-Korrespondenz für diesen Support-Fall.
6. Wenn das Problem behoben ist, können Sie über die angehefteten Nachricht Resolve case (Fall lösen) auswählen oder `/awssupport resolve` eingeben.

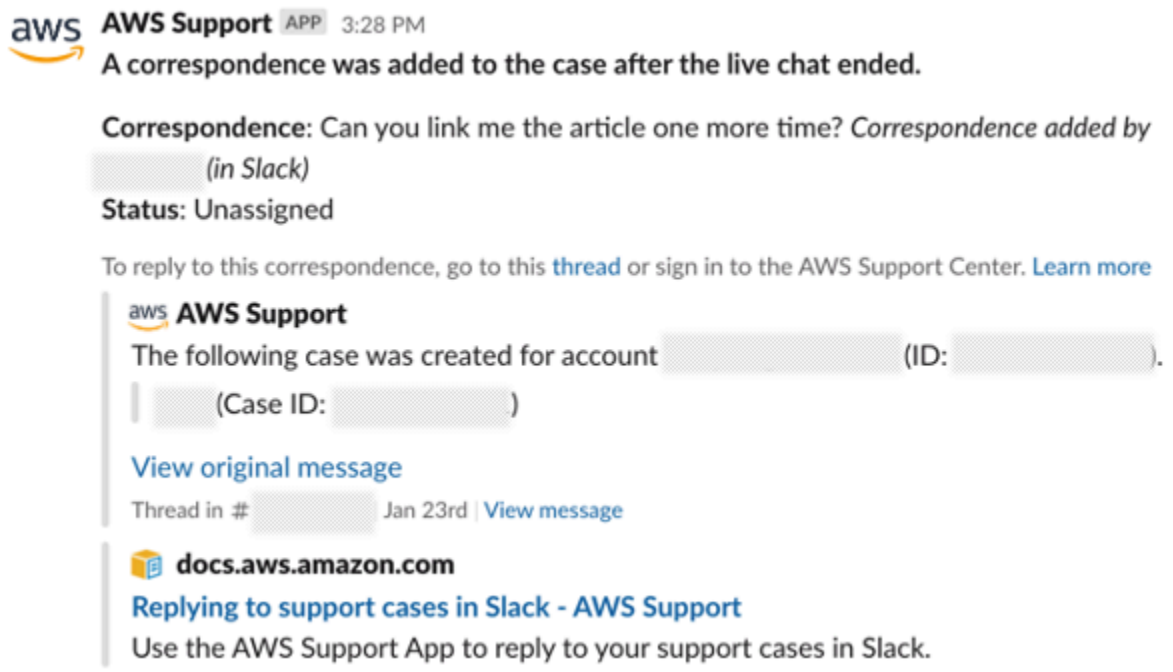
   Example : Beenden eines Live-Chats

   Die folgende angeheftete Nachricht zeigt die Falldetails zu einer Amazon-EC2-Instance. Sie können die angehefteten Nachrichten unter dem Namen des Slack-Kanals finden.



   Example : Korrespondenzbenachrichtigung im Chat-Kanal

   Im Folgenden finden Sie ein Beispiel für einen Live-Chat-Kanal, der eine Benachrichtigung erhält, wenn der andere Mitarbeiter nach dem Ende des Chats eine Aktualisierung hinzufügt.

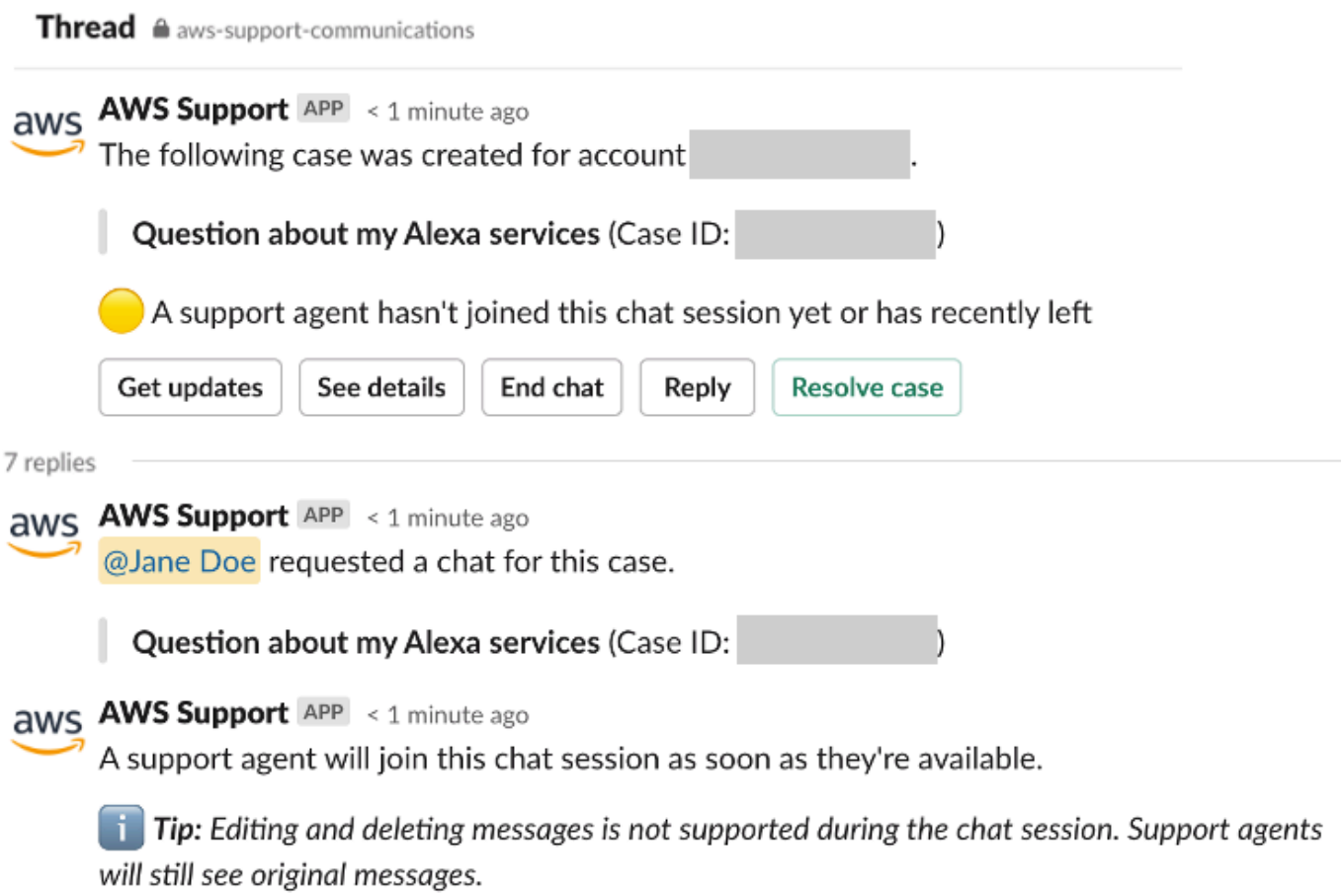


Die Benachrichtigung gibt den Chat-Status („requested“ (angefordert), „in Progress“ (in Bearbeitung) oder „ended“ (beendet)) an und ob die Korrespondenz von einem Kundendienstmitarbeiter oder einem anderen Mitarbeiter hinzugefügt wurde. Die Support-App wird außerdem versuchen, einen Link zum ursprünglichen Slack-Thread oder Kanal herzustellen, in dem dieser Chat angefordert wurde. Sie können über diesen Kanal oder einen anderen Kanal, der Zugriff auf diesen Fall hat, auf diesen Fall antworten.

Um an einer Live-Chat-Sitzung AWS Support im aktuellen Kanal teilzunehmen

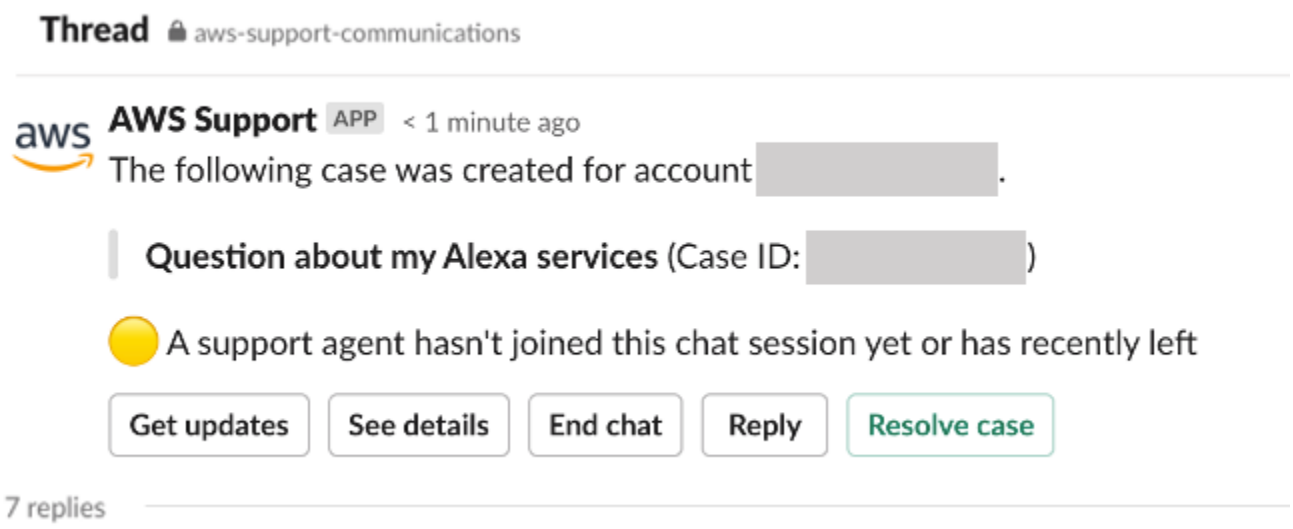
1. Navigiere in der Slack-Anwendung zu dem Thread im aktuellen Channel, den die AWS Support App für den Chat verwendet. In den meisten Fällen handelt es sich dabei um den Thread, der bei der Ersterstellung des Falles begonnen wurde.
2. Wenn der:die Support-Kundendienstmitarbeiter:in dem Thread beitritt, können Sie über Ihren Supportfall chatten. Solange kein:e Support-Kundendienstmitarbeiter:in dem Thread beitritt, sieht der:die Kundendienstmitarbeiter:in die Nachrichten in diesem Thread nicht, und die Nachrichten erscheinen nicht in Ihrer Fallkorrespondenz, wenn der Chat endet.

> **Note**
>
> Nachrichten, die außerhalb des Chat-Threads an diesen Kanal gesendet werden, werden von niemandem gesehen AWS Support, auch nicht, wenn ein Chat aktiv ist.



3. (Optional) Markieren Sie andere Mitglieder des Kanals, um sie über den Chat-Thread zu informieren.
4. Nachdem der Support-Mitarbeiter dem Chat beigetreten ist, ist der Chat-Thread aktiv und die AWS Support App zeichnet den Chat auf. Ähnlich wie beim neuen Chat-Kanal können Sie mit dem:der Kundendienstmitarbeiter:in über Ihren Supportfall chatten und Dateianhänge in den Thread hochladen. Die AWS Support App speichert Ihre Dateien und das Chat-Protokoll automatisch in Ihrer Fallkorrespondenz.

5. (Optional) Um den Live-Chat zu beenden, wählen Sie in der Anfangsnachricht für diesen Thread „Chat beenden“ aus. Der Support-Mitarbeiter verlässt den Thread und die AWS Support App beendet die Aufzeichnung des Live-Chats. Den Chatverlauf finden Sie im Anhang der Fall-Korrespondenz für diesen Support-Fall.
6. Wenn das Problem behoben ist, können Sie in der Anfangsnachricht zu diesem Thread die Option „Fall lösen“ wählen.



Suchen nach Support-Fällen in Slack

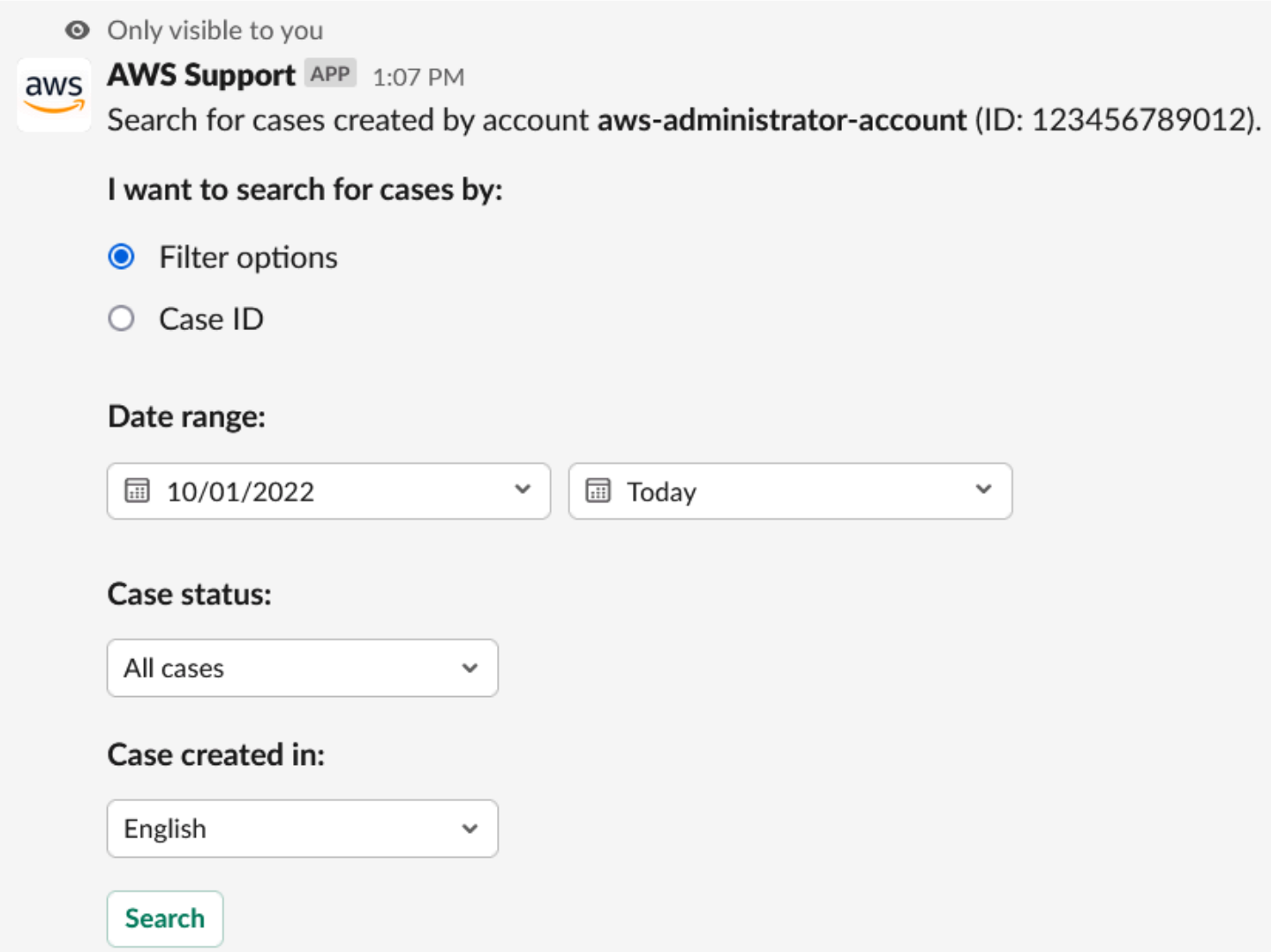
Von Ihrem Slack-Kanal aus können Sie nach Support-Fällen von Ihrem AWS-Konto und von anderen Konten suchen, die denselben Kanal und Workspace konfiguriert haben. Wenn beispielsweise Ihr Konto (123456789012) und das Konto Ihres Kollegen (111122223333) denselben Workspace und dieselben Kanäle in AWS Support Center Console konfiguriert haben, können Sie die AWS Support-App verwenden, um die Supportfälle des jeweils anderen zu suchen.

Sie können die folgenden Optionen verwenden, um Ihre Suchergebnisse zu filtern:

- Konto-ID
- Fall-ID
- Fallstatus
- Kontaktsprache
- Datumsbereich

Example : Nach Fällen in Slack suchen

Das folgende Beispiel zeigt, wie Sie anhand der Filteroptionen nach einem einzelnen Konto suchen, indem Sie den Zeitraum, den Fallstatus und die Kontaktsprache angeben.



So suchen Sie nach einem Support-Fall in Slack

1. Geben Sie im Slack-Kanal den folgenden Befehl ein:

   ```
   /awssupport search
   ```

2. Wählen Sie für die Option Ich möchte nach Fällen suchen nach: eine der folgenden Möglichkeiten aus:

   A. Filteroptionen – Sie können Fälle mit den folgenden Optionen filtern:

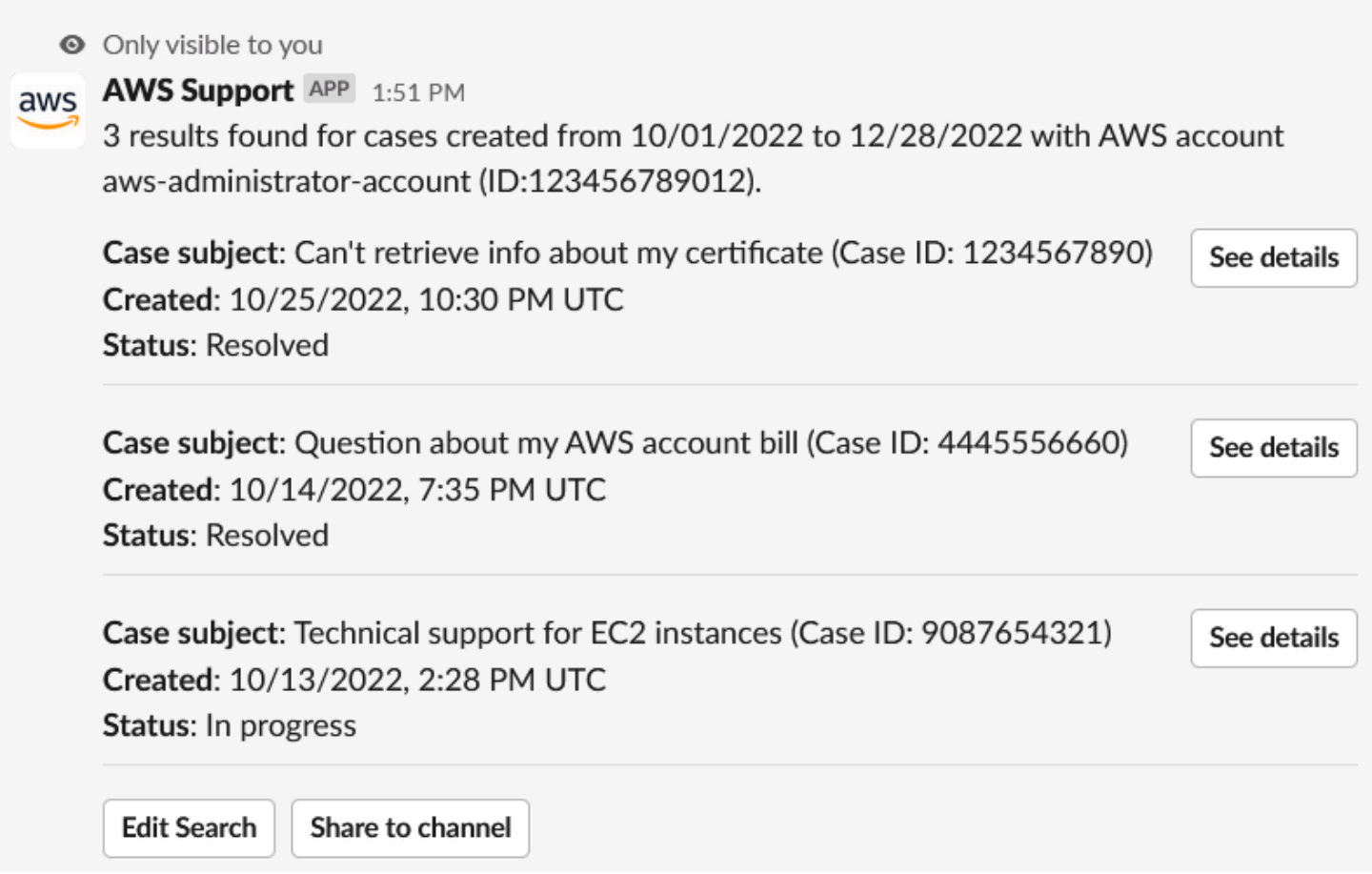
- AWS-Konto – Diese Liste wird nur angezeigt, wenn Sie mehrere Konten in dem Channel haben.
- Zeitraum – Das Datum, an dem der Fall erstellt wurde.
- Fallstatus – Der aktuelle Fallstatus, z. B. Alle offenen Fälle oder Gelöst.
- Fall wurde erstellt in – Die Kontaktsprache für den Fall.

B. Fall-ID – Geben Sie die Fall-ID ein. Sie können jeweils nur eine Fall-ID gleichzeitig eingeben. Wenn Sie mehrere Konten in diesem Kanal haben, wählen Sie AWS-Konto aus, um nach dem Fall zu suchen.

3. Wählen Sie Search (Suchen) aus. Ihre Suchergebnisse werden in Slack angezeigt.

Verwenden Sie Ihre Suchergebnisse

Das folgende Beispiel gibt drei gelöste Support-Fälle von einem AWS-Konto zurück.



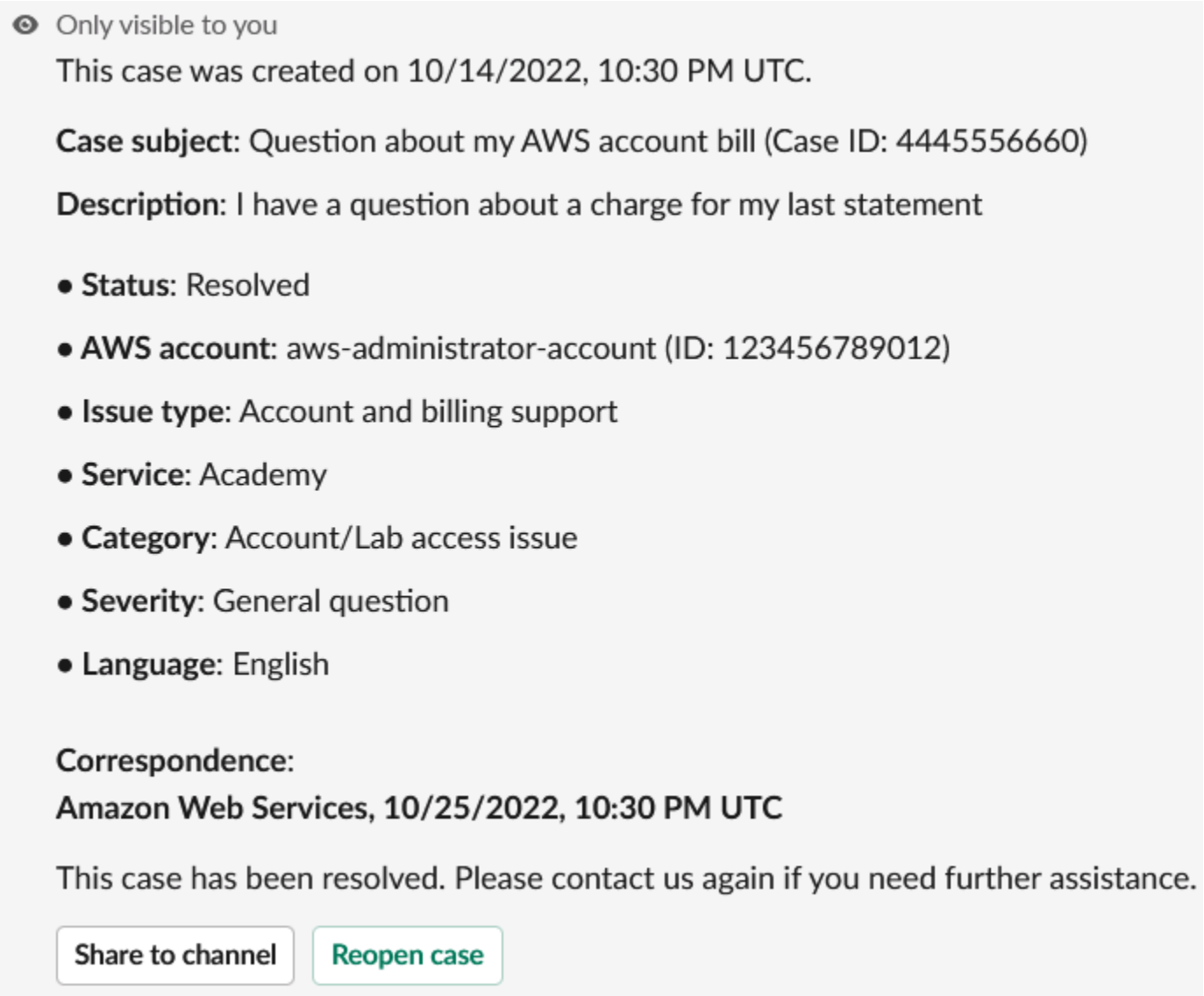
Nachdem Sie Ihre Suchergebnisse erhalten haben, haben Sie folgende Optionen:

Um Sie Ihre Suchergebnisse zu verwenden

1. Wählen Sie Edit Search (Suche bearbeiten), um Ihre vorherigen Filteroptionen oder die Fall-ID zu ändern.
2. Wählen Sie Share to channel (An Kanal freigeben), um die Suchergebnisse für den Kanal freizugeben.
3. Wählen Sie See details (Details anzeigen) aus, um mehr Informationen zu einem Fall zu erhalten. Sie können Show full message (Vollständige Nachricht anzeigen) auswählen, um den Rest der aktuellsten Korrespondenz anzuzeigen.
4. Wenn Sie anhand von Filteroptionen gesucht haben, können in den Suchergebnissen mehrere Fälle zurückgegeben werden. Wählen Sie Next 5 results (Nächste 5 Ergebnisse) oder previous 5 results (Vorherige 5 Ergebnisse), um die nächsten oder die vorherigen 5 Fälle anzuzeigen.

Example : Gelöster Support-Fall

Das folgende Beispiel zeigt einen gelösten Support-Fall für ein Konto- und Abrechnungsproblem, nachdem Sie Details anzeigen ausgewählt haben.



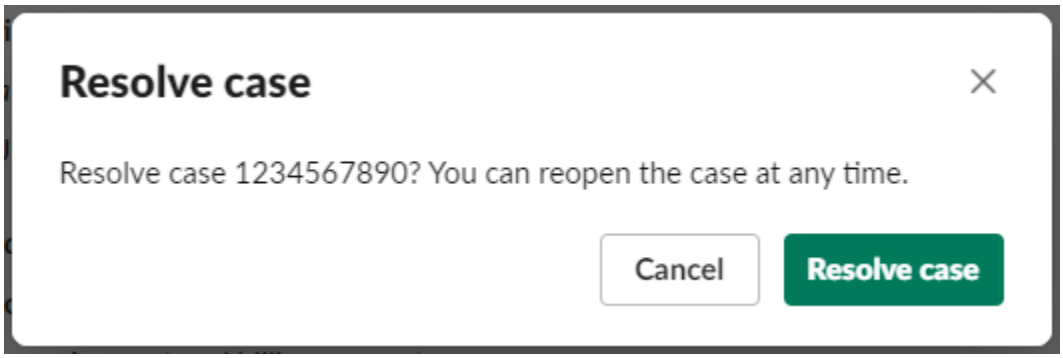
Beheben eines Support-Falls in Slack

Wenn Sie Ihren Support-Fall nicht mehr benötigen oder Sie das Problem behoben haben, können Sie einen Support-Fall direkt in Slack lösen. Dies löst auch den Fall in AWS Support Center Console. Nachdem Sie einen Fall behoben haben, können Sie den Fall später wieder aufnehmen.

Lösen Sie einen Support-Fall in Slack wie folgt

1. Navigieren Sie in Ihrem Slack-Kanal zum Support-Fall. Siehe Suchen nach Support-Fällen in Slack.
2. Wählen Sie See details (Details anzeigen) für den Fall.
3. Wählen Sie Resolve case (Fall lösen).

4. Wählen Sie im Dialogfeld Resolve case (Fall lösen) die Option Resolve case (Fall lösen) aus. Sie können einen Fall im Slack-Kanal oder über die Support-Center-Konsole wieder aufnehmen.

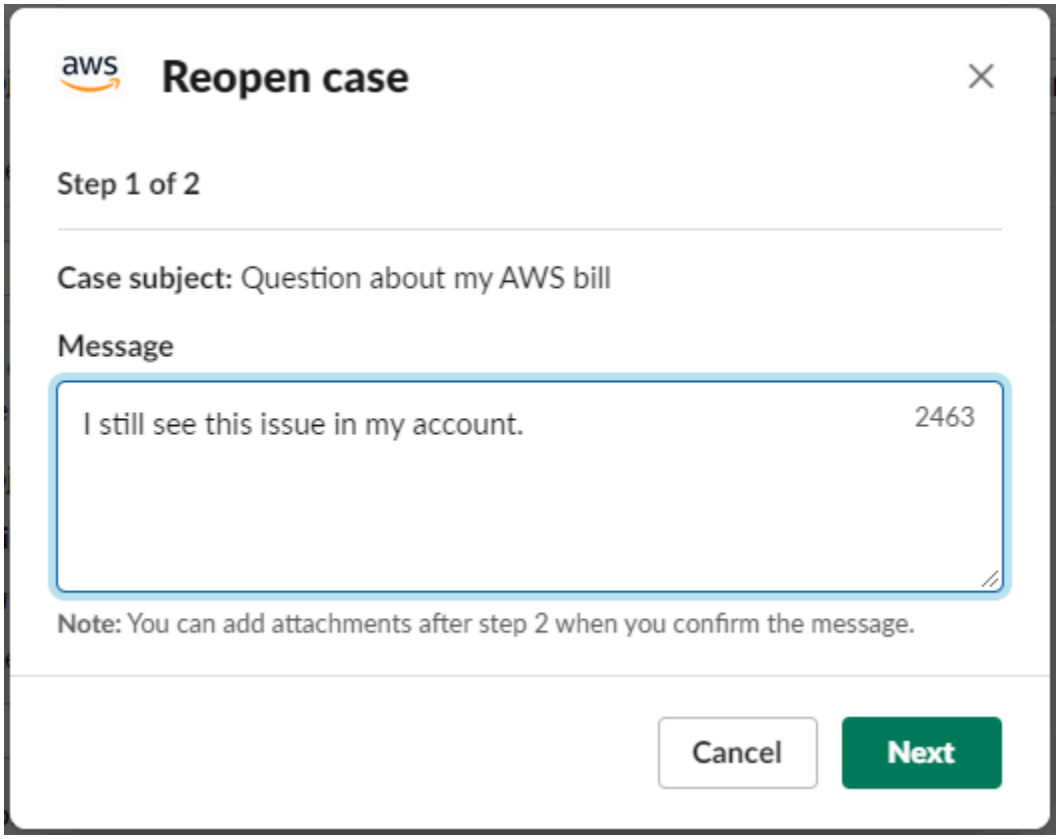


Wiederaufnahme eines Support-Falls in Slack

Nachdem Sie einen Support-Fall gelöst haben, können Sie den Fall in Slack wieder aufnehmen.

Nehmen Sie einen Support-Fall in Slack wieder auf wie folgt

1. Suchen Sie den Support-Fall, um ihn in Slack wieder aufzunehmen. Siehe Suchen nach Support-Fällen in Slack.
2. Wählen Sie See details (Details anzeigen) aus.
3. Wählen Sie Reopen case (Fall wieder öffnen).
4. Geben Sie im Dialogfeld Reopen case (Fall wieder aufnehmen) eine kurze Beschreibung des Problems in das Feld Message (Nachricht) ein.
5. Wählen Sie Next (Weiter).



6. (Optional) Geben Sie weitere Kontakte ein.
7. Wählen Sie Review (Überprüfen).
8. Überprüfen Sie Ihre Falldetails und wählen Sie dann Send message (Nachricht senden) aus. Ihr Fall wird wieder aufgenommen. Wenn Sie einen neuen Live-Chat mit einem:einer Support-Kundendienstmitarbeiter:in angefordert haben, verwendet Slack denselben Chat-Kanal oder Thread wie den, der für einen vorherigen Live-Chat verwendet wurde. Wenn Sie einen Live-Chat in einem neuen Kanal angefordert haben und noch keinen hatten, wird ein neuer Chat-Kanal geöffnet. Wenn Sie einen Live-Chat im aktuellen Kanal angefordert haben und bisher noch keinen hatten, wird ein Thread im aktuellen Kanal verwendet.

Anfordern einer Erhöhung des Service-Kontingents

Sie können über Ihren Slack-Kanal eine Erhöhung des Service-Kontingents für Ihr Konto anfordern.

Fordern Sie eine Erhöhung des Service-Kontingents an wie folgt

1. Geben Sie im Slack-Kanal den folgenden Befehl ein:

   ```
   /awssupport quota
   ```

2. Geben Sie im Dialogfeld Increase service quota (Servicekontingent erhöhen) die folgenden Informationen ein:

   a. Wählen Sie das Symbol AWS-Konto.

   b. Wählen Sie das Symbol AWS-Region.

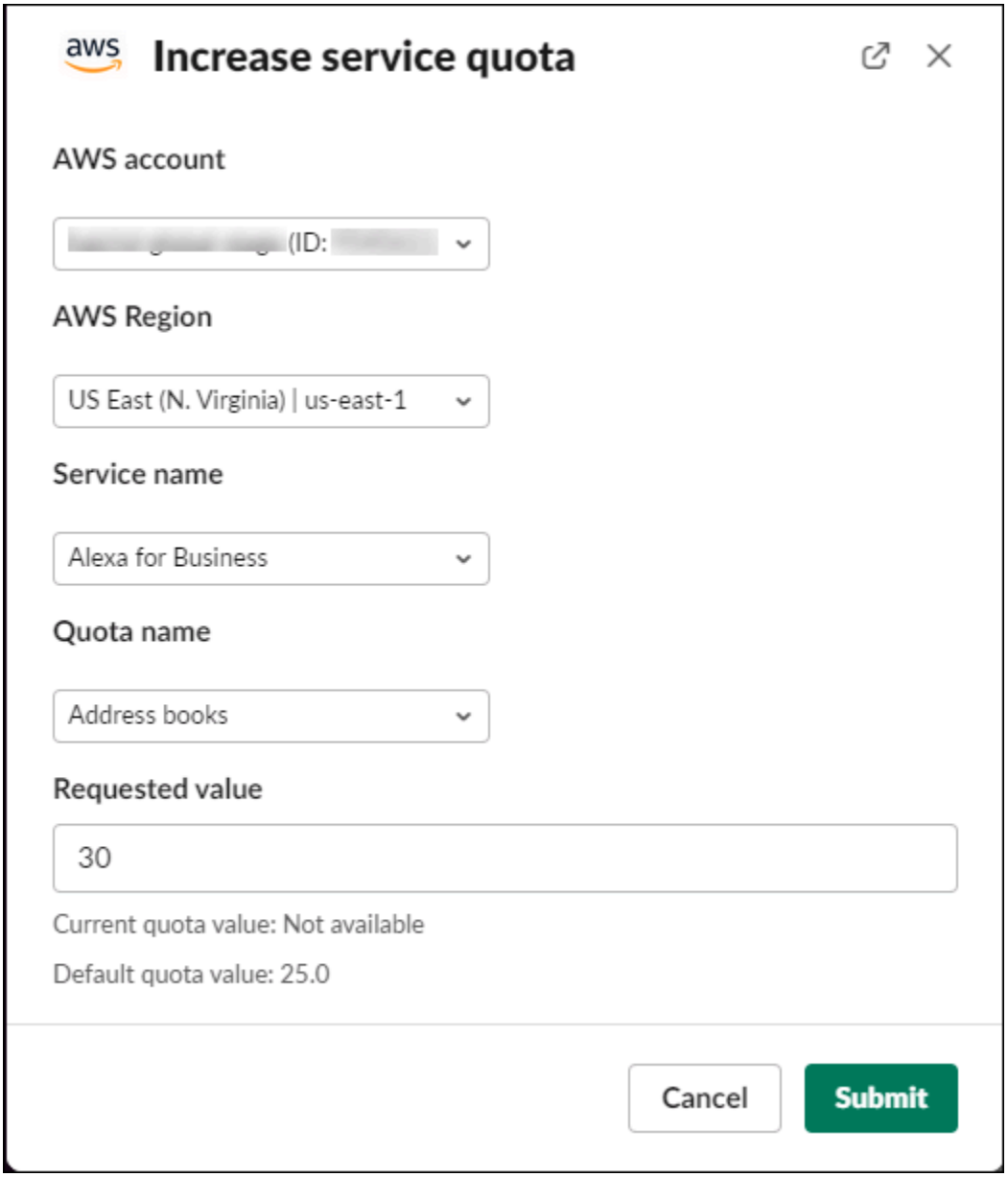
   c. Wählen Sie den Service name (Servicenamen) aus.

   d. Wählen Sie den Quota name (Kontingentnamen) aus.

   e. Geben Sie den Requested value (angeforderten Wer) für die Kontingenterhöhung ein. Sie müssen einen Wert eingeben, der größer als das Standardkontingent ist.

3. Wählen Sie Submit (Absenden) aus.

Example : Kontingenterhöhung für Alexa for Business



Sie können Ihre Anforderungen auch über die Service-Quotas-Konsole anzeigen. Weitere Informationen finden Sie unter Beantragen einer Quota-Erhöhung im Service-Quotas-Benutzerhandbuch.

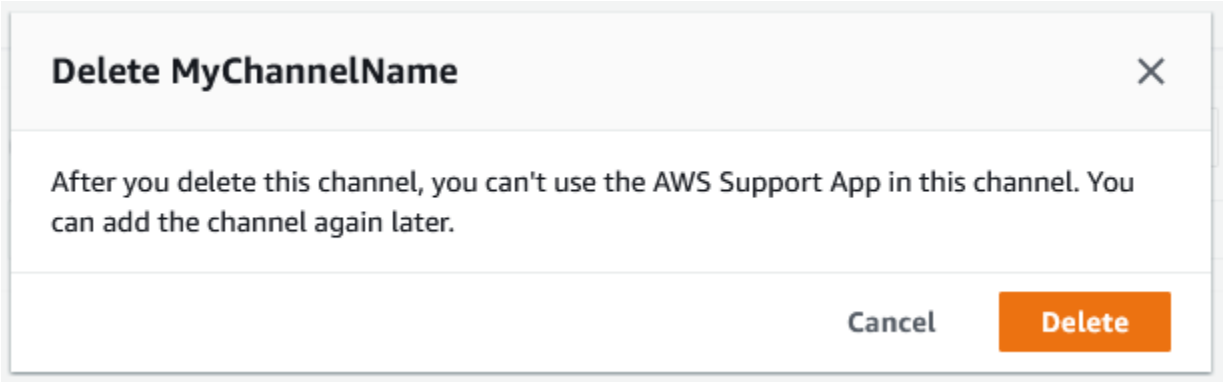
Löschen einer Slack-Kanalkonfiguration aus der AWS Support-App

Sie können eine Kanalkonfiguration aus der AWS Support-App löschen, wenn Sie sie nicht benötigen. Diese Aktion entfernt nur den Kanal aus der AWS Support-App und der AWS Support Center Console. Ihr Kanal wird nicht aus Slack gelöscht.

Sie können bis zu 20 Kanäle für Ihr AWS-Konto hinzufügen. Wenn Sie dieses Kontingent bereits erreicht haben, müssen Sie einen Kanal löschen, bevor Sie einen weiteren hinzufügen können.

Löschen Sie eine Slack-Kanalkonfiguration wie folgt

1. Melden Sie sich in der Support Center Console (Support-Center-Konsole) an und wählen Sie Slack configuration (Slack-Konfiguration) aus.
2. Wählen Sie auf der Seite Slack configuration (Slack-Konfiguration) unter Channels (Kanäle) den Namen des Kanals aus und wählen Sie dann Delete (Löschen).
3. Wählen Sie im Dialogfeld Delete channel name (Kanalname löschen) die Option Delete (Löschen) aus. Sie können diesen Kanal später wieder zur AWS Support-App hinzufügen.



Löschen einer Slack-Workspace-Konfiguration aus der AWS Support-App

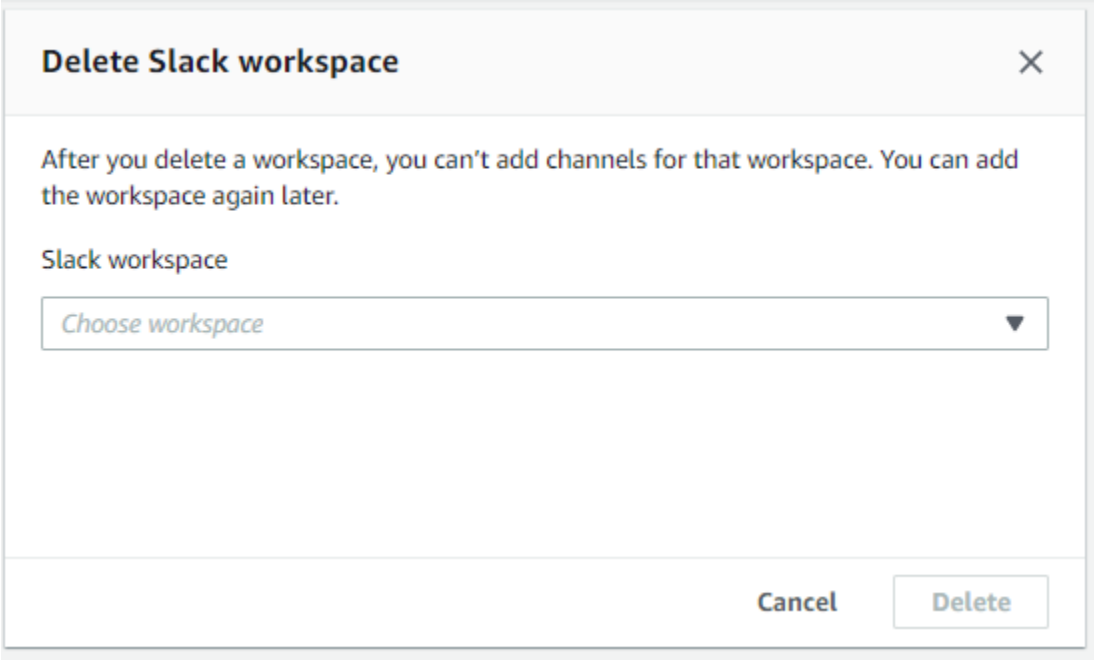
Sie können eine Workspace-Konfiguration aus der AWS Support-App löschen, wenn Sie sie nicht benötigen. Diese Aktion entfernt nur den Workspace aus der AWS Support-App und der AWS Support Center Console. Ihr Workspace wird nicht aus Slack gelöscht.

Sie können bis zu 5 Workspaces für Ihr AWS-Konto hinzufügen. Wenn Sie dieses Kontingent bereits erreicht haben, müssen Sie einen Slack-Workspace löschen, bevor Sie einen weiteren hinzufügen können.

> **Note**
>
> Wenn Sie Kanäle aus diesem Workspace zur AWS Support-App hinzugefügt haben, müssen Sie diese Kanäle zuerst löschen, bevor Sie den Workspace löschen können. Siehe Löschen einer Slack-Kanalkonfiguration aus der AWS Support-App.

Löschen Sie eine Slack-Workspace-Konfiguration wie folgt

1. Melden Sie sich in der AWS Support Center Console an und wählen Sie Slack configuration (Slack-Konfiguration) aus.
2. Wählen Sie auf der Seite Slack configuration (Slack-Konfiguration) unter Slack workspaces (Slack-Workspaces) die Option Delete a workspace (Einen Workspace löschen) aus.
3. Wählen Sie im Dialogfeld Delete Slack workspace (Slack-Workspace löschen) den Namen des Slack-Workspaces und wählen Sie dann Delete (Löschen). Sie können den Workspace später wieder zu Ihrem AWS-Konto hinzufügen.



AWS Support-App in Slack-Befehlen

Befehle für den Slack-Kanal

Sie können die folgenden Befehle in dem Slack-Kanal eingeben, in dem Sie die AWS Support-App eingeladen haben. Dieser Slack-Kanalname wird auch als konfigurierter Kanal in der AWS Support Center Console angezeigt.

`/awssupport create` oder `/awssupport create-case`

Erstellen Sie einen Support-Fall.

`/awssupport search` oder `/awssupport search-case`

Suchen Sie nach Fällen. Sie können nach Support-Fällen für das AWS-Konten suchen, das die AWS Support-App für denselben Slack-Kanal konfiguriert hat.

`/awssupport quota` oder `/awssupport service-quota-increase`

Fordern Sie eine Erhöhung des Service-Kontingents an.

Befehle des Live-Chat-Kanals

Sie können die folgenden Befehle im Live-Chat-Kanal eingeben. Dies ist der Kanal, den die AWS Support-App für Sie erstellt, wenn Sie einen neuen Kanal für Ihren Chat mit dem AWS Support wählen. Chat-Kanäle enthalten Ihre Support-Fall-ID, z. B. *awscase-1234567890*.

> **Note**
>
> Die folgenden Befehle sind nicht verfügbar, wenn ein Thread im aktuellen Kanal für einen Live-Chat verwendet wird. Verwenden Sie stattdessen die Schaltflächen, die an die ursprüngliche Thread-Nachricht angehängt sind, um einen Chat zu beenden, eine:n neue:n Kundendienstmitarbeiter:in einzuladen oder den Fall zu lösen.

`/awssupport endchat`

Entfernen Sie den Support-Kundendienstmitarbeiter und beenden Sie die Live-Chat-Sitzung.

`/awssupport invite`

Laden Sie einen neuen Support-Kundendienstmitarbeiter zu diesem Kanal ein.

`/awssupport resolve`

Lösen Sie diesen Support-Fall.

Anzeigen von AWS Support-App-Korrespondenzen in der AWS Support Center Console

Wenn Sie Support-Fälle für Ihr Konto im Slack-Kanal erstellen, aktualisieren oder lösen, können Sie sich auch in der Support-Center-Konsole anmelden, um Ihre Fälle anzuzeigen. Sie können die Fall-Korrespondenz anzeigen, um festzustellen, ob der Fall im Slack-Kanal aktualisiert wurde, den

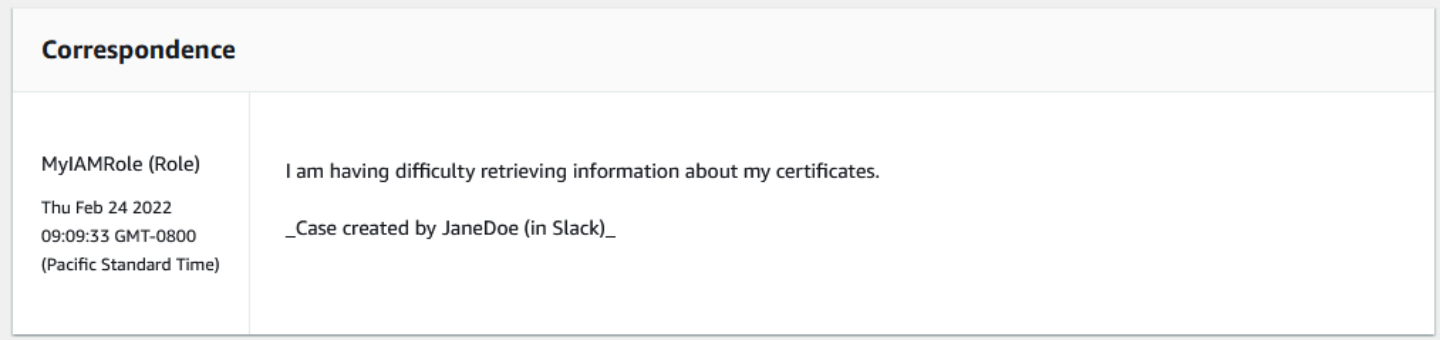
Chatverlauf mit einem Support-Kundendienstmitarbeiter anzeigen und alle Anhänge finden, die Sie aus Slack hochgeladen haben.

Zeigen Sie Fall-Korrespondenzen aus Slack an wie folgt

1. Melden Sie sich in der AWS Support Center Console für Ihr Konto an.
2. Wählen Sie Ihren Support-Fall.
3. In der Correspondence (Korrespondenz) können Sie sehen, ob der Fall über den Slack-Kanal erstellt und aktualisiert wurde.

Example : Support-Fall

Auf dem folgenden Screenshot hat Jane Doe einen Support-Fall in Slack wieder aufgenommen. Diese Korrespondenz wird für den Support-Fall in der Support-Center-Konsole angezeigt.



Erstellen von AWS Support-App in Slack-Ressourcen mit AWS CloudFormation

Die AWS Support-App in Slack ist mit AWS CloudFormation integriert, einem Service, der Sie bei der Modellierung und Einrichtung Ihrer AWS-Ressourcen unterstützt, so dass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle gewünschten AWS-Ressourcen beschreibt (z. B. Ihren AccountAlias und Ihre SlackChannelConfiguration), und AWS CloudFormation stellt diese Ressourcen bereit und konfiguriert sie für Sie.

Wenn Sie AWS CloudFormation verwenden, können Sie Ihre Vorlage wiederverwenden, um Ihre AWS Support-App-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten-Konten und -Regionen immer wieder bereitstellen.

AWS Support-App und AWS CloudFormation-Vorlagen

Um Ressourcen für die AWS Support-App und die damit verbundenen Services bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

AWS Support-App unterstützt die Erstellung Ihrer AccountAlias und SlackChannelConfiguration in AWS CloudFormation. Weitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für die AccountAlias- und SlackChannelConfiguration-Ressourcen, finden Sie in der Referenz zum AWS Support-App-Ressourcentyp im AWS CloudFormation-Benutzerhandbuch.

Erstellen Sie Slack-Konfigurationsressourcen für Ihr Unternehmen

Sie können CloudFormation-Vorlagen verwenden, um die Ressourcen zu erstellen, die Sie für die AWS Support-App benötigen. Wenn Sie das Verwaltungskonto für Ihre Organisation sind, können Sie die Vorlagen verwenden, um diese Ressourcen für Ihre Mitgliedskonten in AWS Organizations zu erstellen.

Sie können beispielsweise eine Vorlage verwenden, um dieselbe Slack-Workspace-Konfiguration für alle Konten in der Organisation zu erstellen, aber dann separate Vorlagen verwenden, um verschiedene Slack-Kanalkonfigurationen für bestimmte AWS-Konten oder organisatorische Einheiten (OUs) zu erstellen. Sie können auch eine Vorlage verwenden, um eine Slack-Workspace-Konfiguration zu erstellen, sodass Mitgliedskonten dann die Slack-Kanäle konfigurieren können, die sie für ihr AWS-Konten haben möchten.

Sie können wählen, ob CloudFormation-Vorlagen verwendet werden sollen oder nicht. Wenn Sie keine CloudFormation-Vorlagen verwenden, können Sie stattdessen die folgenden manuellen Schritte ausführen:

- Erstellen Sie die AWS Support-App-Ressourcen in der AWS Support Center Console.
- Erstellen Sie einen Support-Fall mit AWS Support, um mehrere Konten zu autorisieren, die AWS Support-App zu verwenden.
- Sie können den API-Vorgang RegisterSlackWorkspaceForOrganization verwenden, um einen Slack-Workspace für Ihr Konto zu registrieren. Der CloudFormation-Stack ruft diese API-Operation für Sie auf.

Gehen Sie wie folgt vor, um die CloudFormation-Vorlage in Ihre Organisation hochzuladen. Sie können die Beispielvorlagen von der Referenzseite AWS Support-App-Ressourcentyp verwenden.

Die Vorlagen weisen CloudFormation an, die folgenden Ressourcen zu erstellen:

- Löschen einer Slack-Kanalkonfiguration
- Löschen einer Slack-Workspace-Konfiguration
- Eine IAM-Rolle mit dem `AWSSupportSlackAppCFNRole`-Namen. Die AWSSupportAppFullAccess AWS-verwaltete Richtlinie ist angefügt.

Inhalt

Aktualisieren Sie Ihre CloudFormation-Vorlagen für Slack

Verwenden Sie zunächst die folgenden Vorlagen, um Ihren Stack zu erstellen. Sie müssen die Vorlagen durch gültige Werte für Ihren Slack-Workspace und -Kanal ersetzen.

> **Note**
>
> Wir empfehlen nicht, die Vorlage zu verwenden, um eine AccountAlias-Ressource für Ihr Unternehmen zu erstellen. Die AccountAlias-Ressource identifiziert eindeutig AWS-Konto in der AWS Support-App. Ihre Mitgliedskonten können einen Kontonamen in der Support Center Console eingeben. Weitere Informationen finden Sie unter Autorisieren eines Slack-Workspaces.

So aktualisieren Sie Ihre CloudFormation-Vorlagen für Slack

1. Wenn Sie das Verwaltungskonto für eine Organisation sind, müssen Sie manuell einen Slack-Workspace für Ihr Konto autorisieren, bevor Ihre Mitgliedskonten die Ressourcen mithilfe von CloudFormation erstellen können. Falls dies noch nicht geschehen ist, finden Sie weitere Informationen unter Autorisieren eines Slack-Workspaces.
2. Kopieren Sie von der Referenzseite AWS Support-App-Ressourcentyp die JSON- oder YAML-Vorlage für die gewünschte Ressource.

3. Fügen Sie die Vorlage in einem Texteditor in eine neue Datei ein.
4. Geben Sie in der Vorlage die gewünschten Parameter an. Ersetzen Sie mindestens die Werte für die folgenden Felder:

   - `TeamId` mit Ihrer Slack-Workspace-ID
   - `ChannelId` mit der Slack-Kanal-ID
   - `ChannelName` mit einem Namen zur Identifizierung der Slack-Kanalkonfiguration

   > **Tip**
   >
   > Um die Workspace- und Channel-IDs zu finden, öffnen Sie Ihren Slack-Channel in einem Browser. In der URL ist Ihre Workspace-ID die erste Kennung und die Channel-ID ist die zweite. Beispielsweise ist in https://app.slack.com/client/T012ABCDEFG/C01234A5BCD T012ABCDEFG die Workspace-ID und C01234A5BCD die Channel-ID.

5. Speichern Sie die Datei entweder als JSON- oder YAML.

Stack für das Verwaltungskonto erstellen

Als Nächstes müssen Sie einen Stack für das Verwaltungskonto in der Organisation erstellen. Dieser Schritt ruft den RegisterSlackWorkspaceForOrganization-API-Vorgang für Sie auf und autorisiert den Workspace mit Slack.

> **Note**
>
> Wir empfehlen, dass Sie die Slack-Workspace-Konfigurationsvorlage hochladen, die Sie im vorherigen Verfahren für das Verwaltungskonto aktualisiert haben. Sie müssen die Slack-Kanal-Konfigurationsvorlage nicht hochladen, es sei denn, Sie konfigurieren das Verwaltungskonto auch für die Verwendung der AWS Support-App.

So erstellen Sie einen Stack für das Verwaltungskonto

1. Melden Sie sich bei der AWS Management Console als das Verwaltungskonto Ihrer Organisation an.
2. Öffnen Sie die AWS CloudFormation-Konsole unter https://console.aws.amazon.com/cloudformation.

3. Wenn Sie es noch nicht getan haben, wählen Sie in der Regionsauswahl eine der folgenden AWS-Regionen:

   - Europe (Frankfurt)
   - Europa (Irland)
   - Europe (London)
   - USA Ost (Nord-Virginia)
   - USA Ost (Ohio)
   - USA West (Oregon)
   - Asien-Pazifik (Singapur)
   - Asien-Pazifik (Tokio)
   - Canada (Central)

4. Gehen Sie folgendermaßen vor, um einen Stack zu erstellen. Weitere Informationen finden Sie unter Erstellen eines Stacks in der AWS CloudFormation-Konsole.

   Nachdem der Stack erfolgreich erstellt von CloudFormation wurde, können Sie dieselbe Vorlage verwenden, um ein Stack-Set für Ihre Organisation zu erstellen.

Erstellen eines Stack-Sets für Ihr Unternehmen

Verwenden Sie als Nächstes dieselbe Vorlage für die Slack-Workspace-Konfiguration, um ein Stack-Set mit `service-managed`-Berechtigungen zu erstellen. Sie können Stack-Sets verwenden, um den Stack für Ihre gesamte Organisation zu erstellen, oder die gewünschten Organisationseinheiten angeben. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets.

Dieses Verfahren ruft auch den RegisterSlackWorkspaceForOrganization-API-Vorgang für Sie auf. Dieser API-Vorgang autorisiert den Workspace mit Slack für die Mitgliederkonten.

Um ein Stack-Set für Ihr Unternehmen zu erstellen

1. Melden Sie sich bei der AWS Management Console als das Verwaltungskonto Ihrer Organisation an.
2. Öffnen Sie die AWS CloudFormation-Konsole unter https://console.aws.amazon.com/cloudformation.
3. Wenn Sie es noch nicht getan haben, wählen Sie in der Regionsauswahl dieselbe AWS-Region aus, die Sie im vorherigen Verfahren verwendet haben.

4. Wählen Sie im Navigationsbereich StackSets aus.
5. Wählen Sie Create StackSet.
6. Behalten Sie auf der Seite Vorlage auswählen die Standardoptionen für die folgenden Optionen bei:

   - Für Permissions (Berechtigungen) behalten Sie die Option Service-managed permissions (Serviceverwaltete Berechtigungen).
   - Für Prerequisite – Prepare template (Voraussetzung – Vorlage vorbereiten) behalten Sie die Option Template is ready (Vorlage ist bereit).
7. Unter Specify template (Vorlage festlegen), wählen Sie Upload a template file (Vorlagendatei hochladen) aus und wählen Sie dann Choose file (Datei wählen).
8. Wählen Sie die Datei aus und wählen Sie Weiter.
9. Geben Sie auf der Seite Specify StackSet details (Stack-Set-Details angeben) einen Stack-Namen ein, z. B. **`support-app-slack-workspace`**, geben Sie eine Beschreibung ein und wählen Sie dann Weiter.
10. Behalten Sie auf der Seite Configure StackSet options (StackSet-Optionen konfigurieren) die Standardoptionen bei, und wählen Sie dann Weiter.
11. Behalten Sie auf der Seite Bereitstellungsoptionen festlegen für Stacks zum Stack-Set hinzufügen die Standardoption Neue Stacks bereitstellen bei.
12. Wählen Sie für Bereitstellungsziele aus, ob Sie den Stack für die gesamte Organisation oder für bestimmte OUs erstellen möchten. Wenn Sie eine OU wählen, geben Sie die OU-ID ein.
13. Geben Sie für Regionen angeben nur eine der folgenden AWS-Regionen ein:

    - Europe (Frankfurt)
    - Europa (Irland)
    - Europe (London)
    - USA Ost (Nord-Virginia)
    - USA Ost (Ohio)
    - USA West (Oregon)
    - Asien-Pazifik (Singapur)
    - Asien-Pazifik (Tokio)
    - Canada (Central)

Hinweise:

- Um Ihren Workflow zu optimieren, empfehlen wir Ihnen, dasselbe AWS-Region zu verwenden, das Sie in Schritt 3 ausgewählt haben.
- Wenn Sie mehrere AWS-Region auswählen, kann dies zu Konflikten bei der Erstellung Ihres Stacks führen.

14. Geben Sie für Bereitstellungsoptionen bzw. für Fehlertoleranz – optional die Anzahl der Konten ein, bei denen die Stacks fehlschlagen können, bevor der Vorgang von CloudFormation beendet wird. Wir empfehlen, dass Sie die Anzahl der Konten, die Sie hinzufügen möchten, minus eins eingeben. Wenn Ihre angegebene OU beispielsweise 10 Mitgliedskonten hat, geben Sie 9 ein. Das bedeutet, dass selbst wenn der Vorgang bei CloudFormation neunmal fehlschlägt, mindestens ein Konto erfolgreich ist.
15. Wählen Sie Next (Weiter).
16. Überprüfen Sie auf der Seite Review (Überprüfen) Ihre Optionen und wählen Sie anschließend Submit (Einsenden) aus. Sie können den Status Ihres Stack auf der Registerkarte Stack-Instances überprüfen.
17. (Optional) Wiederholen Sie diesen Vorgang, um eine Vorlage für eine Slack-Kanalkonfiguration hochzuladen. Die Beispielvorlage erstellt auch die IAM-Rolle und fügt eine von AWS verwaltete Richtlinie hinzu. Diese Rolle verfügt über die erforderlichen Berechtigungen, um für Sie auf andere Services zuzugreifen. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support-App.

    Wenn Sie kein Stack-Set für die Slack-Kanalkonfiguration erstellen, können Ihre Mitgliedskonten den Slack-Kanal manuell konfigurieren. Weitere Informationen finden Sie unter Konfigurieren eines Slack-Kanals.

Nachdem CloudFormation die Stacks erstellt hat, kann sich jedes Mitgliedskonto bei der Support Center Console anmelden und seine konfigurierten Slack-Workspaces und -Kanäle vorfinden. Sie können dann die AWS Support-App für ihr AWS-Konto verwenden. Siehe Erstellen von Support-Fällen in einem Slack-Kanal.

> **Tip**
>
> Wenn Sie eine neue Vorlage hochladen müssen, empfehlen wir Ihnen, dieselbe AWS-Region zu verwenden, die Sie zuvor angegeben haben.

Weitere Informationen zu CloudFormation

Weitere Informationen zu CloudFormation finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

AWS Support-App-Ressourcen mithilfe von Terraform erstellen

Sie können Terraform auch verwenden, um die AWS Support-App-Ressourcen für Ihr AWS-Konto zu erstellen. Terraform ist ein Infrastructure-as-Code-Tool, das Sie für Ihre Cloud-Anwendungen verwenden können. Sie können Terraform verwenden, um AWS Support-App-Ressourcen zu erstellen, anstatt einen CloudFormation-Stack für ein Konto bereitzustellen.

Nachdem Sie Terraform installiert haben, können Sie die gewünschten AWS Support-App-Ressourcen angeben. Terraform ruft die RegisterSlackWorkspaceForOrganization API-Operation auf, um einen Slack-Workspace für Sie zu registrieren, und erstellt Ihre Ressourcen. Sie können sich dann bei der Support Center Console anmelden und dort Ihre konfigurierten Slack-Workspaces und Kanäle vorfinden.

> **Hinweise**
>
> - Wenn Sie das Verwaltungskonto für eine Organisation sind, müssen Sie manuell einen Slack-Workspace für Ihr Konto autorisieren, bevor Ihre Mitgliedskonten die Ressourcen mithilfe von Terraform erstellen können. Falls dies noch nicht geschehen ist, finden Sie weitere Informationen unter Autorisieren eines Slack-Workspaces.
> - Im Gegensatz zu CloudFormation-Stack-Sets können Sie Terraform nicht verwenden, um die AWS Support-App-Ressourcen für eine OU in Ihrer Organisation zu erstellen.

- Den Ereignisverlauf für diese Updates von Terraform finden Sie auch unter AWS CloudTrail. Die `eventSource` für diese Ereignisse werden `cloudcontrolapi.amazonaws.com` und `supportapp.amazonaws.com` sein. Weitere Informationen finden Sie unter Protokollieren der AWS Support-App in Slack-API-Aufrufen mit AWS CloudTrail.

Weitere Informationen

Weitere Informationen zu Terraform finden Sie in den folgenden Themen.

- Terraform-Installation
- Terraform-Tutorial: Infrastruktur erstellen für AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

Sicherheit in AWS Support

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS und . Weitere Informationen zu den Compliance-Programmen, für die gelten AWS Support, finden Sie unter AWS Services nach Compliance-Programm .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Support. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Support , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere Amazon Web Services nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Support Ressourcen unterstützen.

Themen

Datenschutz in AWS Support

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Support. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Support oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Sicherheit für Ihre Fälle AWS Support

Wenn Sie einen Support-Fall erstellen, sind Sie der Eigentümer der Informationen, die Sie in Ihrem Support-Fall angeben. AWS greift ohne Ihre Zustimmung nicht auf Ihre AWS-Konto Daten zu. AWS gibt Ihre Daten nicht an Dritte weiter.

Wenn Sie einen Support-Fall erstellen, beachten Sie Folgendes:

- AWS Support verwendet die in der `AWSServiceRoleForSupport` serviceverknüpften Rolle definierten Berechtigungen, um andere anzurufen AWS-Services , die Kundenprobleme für Sie beheben. Weitere Informationen finden Sie unter Verwenden von dienstbezogenen Rollen für AWS Support und unter AWS verwaltete Richtlinien:. AWSSupportServiceRolePolicy
- Sie können API-Aufrufe anzeigen AWS Support , die in Ihrem AWS-Konto aufgetreten sind. Beispielsweise können Sie Protokollinformationen anzeigen, wenn jemand in Ihrem Konto einen Support-Fall erstellt oder löst. Weitere Informationen finden Sie unter Protokollieren von AWS Support API-Aufrufen mit AWS CloudTrail.
- Sie können die AWS Support API verwenden, um die `DescribeCases` API aufzurufen. Diese API stellt Support-Fall-Informationen bereit, wie z. B. die Fall-ID, das Erstellungs- und Lösungsdatum sowie die Korrespondenz mit dem Support-Kundendienstmitarbeiter. Sie können die Falldetails bis zu 12 Monate nach der Erstellung des Falles einsehen. Weitere Informationen finden Sie DescribeCasesin der AWS Support API-Referenz.
- Ihre Support-Fälle folgen der Konformitätsvalidierung für AWS Support.
- Wenn Sie einen Support-Fall erstellen, erhält AWS er keinen Zugriff auf Ihr Konto. Bei Bedarf verwenden Support-Kundendienstmitarbeiter ein Tool zur Bildschirmfreigabe, um Ihren Bildschirm aus der Ferne anzuzeigen und Probleme zu identifizieren und zu beheben. Dieses Tool ist nur zur Ansicht verfügbar. AWS Support kann während der Bildschirmfreigabesitzung nicht für Sie handeln. Sie müssen Ihre Zustimmung geben, um einen Bildschirm für einen Support-Kundendienstmitarbeiter freizugeben. Weitere Informationen finden Sie unter AWS Support – Häufig gestellte Fragen.
- Sie können Ihren AWS Support Tarif ändern, um die Hilfe zu erhalten, die Sie für Ihr Konto benötigen. Weitere Informationen finden Sie unter AWS Support Tarife vergleichen und AWS Support Abo ändern.

Identitäts- und Zugriffsmanagement für AWS Support

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Ressourcen zu verwenden. AWS Support IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Support

Dienstbenutzer — Wenn Sie den AWS Support Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Support Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung bei AWS Support Identität und Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Support haben.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die AWS Support Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AWS Support. Es ist Ihre Aufgabe, zu bestimmen, auf welche AWS Support Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM nutzen kann AWS Support, finden Sie unterWie AWS Support funktioniert mit IAM.

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Support verfassen können. Beispiele für AWS Support identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. AWS Support Beispiele für identitätsbasierte Richtlinien

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center - Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS Konto (Root-Benutzer)

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb von Ihnen AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen

bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann

dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon EC2 ausgeführte Anwendungen — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien.

Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS Support funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf zu verwalten AWS Support, sollten Sie wissen, mit welchen IAM-Funktionen Sie verwenden können. AWS SupportEinen allgemeinen Überblick darüber, wie AWS Support und andere AWS Dienste mit IAM funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Informationen zur Verwaltung des Zugriffs für die AWS Support Verwendung von IAM finden Sie unter Zugriff verwalten für. AWS Support

Themen

- Identitätsbasierte AWS Support -Richtlinien
- AWS Support IAM-Rollen

Identitätsbasierte AWS Support -Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. AWS Support unterstützt bestimmte Aktionen. Informationen zu den Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen,

die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Support verwendet:`support:`. Um einem Benutzer beispielsweise die Berechtigung zum Ausführen einer Amazon-EC2-Instance mit der Amazon-EC2-`RunInstances`-API-Operation zu erteilen, fügen Sie die Aktion `ec2:RunInstances` in seine Richtlinie ein. Richtlinienanweisungen müssen ein `Action`- oder `NotAction`-Element enthalten. AWS Support definiert seinen eigenen Satz an Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "ec2:Describe*"
```

Eine Liste der AWS Support Aktionen finden Sie AWS Support im IAM-Benutzerhandbuch unter Definierte Aktionen von.

Beispiele

Beispiele für AWS Support identitätsbasierte Richtlinien finden Sie unter. AWS Support Beispiele für identitätsbasierte Richtlinien

AWS Support IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS Konto, die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit AWS Support

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder GetFederationToken aufrufen.

AWS Support unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

AWS Support unterstützt dienstbezogene Rollen. Einzelheiten zum Erstellen oder Verwalten von AWS Support dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für AWS Support

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

AWS Support unterstützt Servicerollen.

AWS Support Beispiele für identitätsbasierte Richtlinien

IAM-Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von AWS Support -Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der AWS Support -Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien sind sehr leistungsfähig. Sie bestimmen, ob jemand AWS Support Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien — Um AWS Support schnell mit der Nutzung zu beginnen, sollten Sie AWS verwaltete Richtlinien verwenden, um Ihren Mitarbeitern die erforderlichen Berechtigungen zu erteilen. Diese Richtlinien sind bereits in Ihrem Konto verfügbar und werden von AWS. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erste Schritte zur Nutzung von Berechtigungen mit AWS verwalteten Richtlinien.
- Gewähren Sie die geringstmöglichen Berechtigungen – Gewähren Sie beim Erstellen benutzerdefinierter Richtlinien nur die Berechtigungen, die zum Ausführen einer Aufgabe erforderlich sind. Beginnen Sie mit einem Mindestsatz von Berechtigungen und gewähren Sie zusätzliche Berechtigungen wie erforderlich. Dies ist sicherer, als mit Berechtigungen zu beginnen, die zu weit gefasst sind, und dann später zu versuchen, sie zu begrenzen. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.
- Aktivieren Sie für sensible Vorgänge MFA – Fordern Sie von IAM-Benutzern die Verwendung von Multi-Factor Authentication (MFA), um zusätzliche Sicherheit beim Zugriff auf sensible Ressourcen oder API-Operationen zu bieten. Weitere Informationen finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.
- Verwenden Sie Richtlinienbedingungen, um zusätzliche Sicherheit zu bieten – Definieren Sie die Bedingungen, unter denen Ihre identitätsbasierten Richtlinien den Zugriff auf eine Ressource zulassen, soweit praktikabel. Beispielsweise können Sie Bedingungen schreiben, die eine Reihe von zulässigen IP-Adressen festlegen, von denen eine Anforderung stammen muss. Sie können auch Bedingungen schreiben, die Anforderungen nur innerhalb eines bestimmten Datums- oder

Zeitbereichs zulassen oder die Verwendung von SSL oder MFA fordern. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Verwenden der AWS Support -Konsole

Um auf die AWS Support Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Informationen zu den AWS Support Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Benutzer oder -Rollen) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten die AWS Support Konsole weiterhin verwenden können, fügen Sie den Entitäten außerdem die folgende AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die Sie ausführen möchten.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen

AWS Support und AWS Trusted Advisor verwenden Sie AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine eindeutige IAM-Rolle, die direkt mit und verknüpft ist. AWS Support Trusted Advisor In jedem Fall ist die serviceverknüpfte Rolle eine vordefinierte Rolle. Diese Rolle umfasst alle Berechtigungen, AWS Support die Trusted Advisor erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen. In den folgenden Themen wird erklärt, was mit Diensten verknüpfte Rollen bewirken und wie Sie mit ihnen in AWS Support und Trusted Advisor arbeiten.

Themen

- Verwenden von serviceverknüpften Rollen für AWS Support
- Verwenden von serviceverknüpften Rollen für Trusted Advisor

Verwenden von serviceverknüpften Rollen für AWS Support

AWS Support Tools sammeln mithilfe von API-Aufrufen Informationen über Ihre AWS Ressourcen, um Kundenservice und technischen Support bereitzustellen. Um die Transparenz und

Überprüfbarkeit von Supportaktivitäten zu erhöhen, AWS Support verwendet eine AWS Identity and Access Management (IAM) -Servicefunktion.

Bei der `AWSServiceRoleForSupport` serviceverknüpften Rolle handelt es sich um eine einzigartige IAM-Rolle, die direkt mit verknüpft ist. AWS Support Diese dienstbezogene Rolle ist vordefiniert und umfasst die Berechtigungen, die AWS Support erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen.

Die serviceverknüpfte Rolle `AWSServiceRoleForSupport` vertraut dem Service `support.amazonaws.com`, sodass dieser die Rolle annehmen kann.

Um diese Dienste bereitzustellen, gewähren die vordefinierten Berechtigungen der Rolle AWS Support Zugriff auf Ressourcenmetadaten, nicht auf Kundendaten. Nur AWS Support Tools können diese Rolle übernehmen, die in Ihrem AWS Konto existiert.

Wir schwärzen Felder, die Kundendaten enthalten. Beispielsweise sind die `Output` Felder `Input` und in der GetExecutionHistorie für den AWS Step Functions API-Aufruf für Sie nicht sichtbar AWS Support. Wir benutzen AWS KMS keys , um sensible Felder zu verschlüsseln. Diese Felder sind in der API-Antwort geschwärzt und für AWS Support Agenten nicht sichtbar.

> **Note**
>
> AWS Trusted Advisor verwendet eine separate, mit dem IAM-Dienst verknüpfte Rolle, um auf AWS Ressourcen für Ihr Konto zuzugreifen und Empfehlungen und Prüfungen zu bewährten Methoden zu geben. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Trusted Advisor.

Durch die `AWSServiceRoleForSupport` serviceverknüpfte Rolle sind alle AWS Support API-Aufrufe für Kunden sichtbar. AWS CloudTrail Dies hilft bei den Überwachungs- und Prüfanforderungen, da auf diese Weise transparent nachvollzogen werden kann, welche Aktionen in AWS Support Ihrem Namen ausgeführt werden. Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Berechtigungen von serviceverknüpften Rollen für AWS Support

Diese Rolle verwendet die `AWSSupportServiceRolePolicy` AWS verwaltete Richtlinie. Diese verwaltete Richtlinie ist mit der Rolle verknüpft und gibt der Rolle die Berechtigung, Aktionen in Ihrem Namen durchzuführen.

Diese Aktionen könnten Folgendes umfassen:

- Abrechnungs-, Verwaltungs-, Support- und andere AWS Kundendienste — der Kundendienst verwendet die in der verwalteten Richtlinie gewährten Berechtigungen, um eine Reihe von Dienstleistungen im Rahmen Ihres Supportplans auszuführen. Dazu gehören die Untersuchung und Beantwortung von Konto- und Abrechnungsfragen, die administrative Unterstützung Ihres Kontos, die Erhöhung von Service Quotas und die Bereitstellung von zusätzlichem Kundensupport.
- Verarbeitung von Serviceattributen und Nutzungsdaten für Ihr AWS Konto — AWS Support möglicherweise werden die in der verwalteten Richtlinie gewährten Berechtigungen verwendet, um auf Serviceattribute und Nutzungsdaten für Ihr AWS Konto zuzugreifen. Diese Richtlinie ermöglicht AWS Support die Bereitstellung von Abrechnungs-, administrativen und technischen Support für Ihr Konto. Serviceattribute umfassen die Ressourcenkennungen, Metadaten-Tags, Rollen und Berechtigungen Ihres Kontos. Zu den Nutzungsdaten zählen die Nutzungsrichtlinien, Nutzungsstatistiken und Analysen.
- Aufrechterhaltung der Funktionsfähigkeit Ihres Kontos und seiner Ressourcen — AWS Support verwendet automatisierte Tools zur Durchführung von Aktionen im Zusammenhang mit betrieblichem und technischem Support.

Weitere Informationen zu den zulässigen Diensten und Aktionen finden Sie in der AWSSupportServiceRolePolicy-Richtlinie in der IAM-Konsole.

> **Note**
>
> AWS Support aktualisiert die `AWSSupportServiceRolePolicy` Richtlinie automatisch einmal pro Monat, um Berechtigungen für neue AWS Dienste und Aktionen hinzuzufügen.

Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Support.

Erstellen einer dienstbezogenen Rolle für AWS Support

Sie müssen die Rolle `AWSServiceRoleForSupport` nicht manuell erstellen. Wenn Sie ein AWS Konto erstellen, wird diese Rolle automatisch für Sie erstellt und konfiguriert.

> **Important**
>
> Wenn Sie sie AWS Support vor Beginn der Unterstützung von dienstbezogenen Rollen verwendet haben, haben Sie die `AWSServiceRoleForSupport` Rolle dann in Ihrem Konto

AWS erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Bearbeiten und Löschen einer dienstbezogenen Rolle für AWS Support

Sie können die IAM für das Bearbeiten der Beschreibung der serviceverknüpften Rolle `AWSServiceRoleForSupport` verwenden. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Die `AWSServiceRoleForSupport` Rolle ist erforderlich, AWS Support um administrativen, betrieblichen und technischen Support für Ihr Konto bereitzustellen. Daher kann diese Rolle nicht über die IAM-Konsole, API oder AWS Command Line Interface (AWS CLI) gelöscht werden. Dies schützt Ihr AWS -Konto, da Sie nicht versehentlich die erforderlichen Berechtigungen für die Administration von Supportservices entfernen können.

Weitere Informationen über die Rolle `AWSServiceRoleForSupport` oder deren Benutzer erhalten Sie von AWS Support.

Verwenden von serviceverknüpften Rollen für Trusted Advisor

AWS Trusted Advisor verwendet die AWS Identity and Access Management dienstverknüpfte Rolle (IAM). Eine serviceverknüpfte Rolle ist eine eindeutige IAM-Rolle, mit der direkt verknüpft ist. AWS Trusted Advisor Dienstbezogene Rollen sind von vordefiniert und enthalten alle Berechtigungen Trusted Advisor, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Trusted Advisor verwendet diese Rolle, um Ihre Nutzung zu überprüfen AWS und Empfehlungen zur Verbesserung Ihrer AWS Umgebung abzugeben. Trusted Advisor Analysiert beispielsweise die Nutzung Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instance, um Ihnen zu helfen, Kosten zu senken, die Leistung zu steigern, Ausfälle zu tolerieren und die Sicherheit zu verbessern.

> **Note**
>
> AWS Support verwendet eine separate, mit dem IAM-Dienst verknüpfte Rolle für den Zugriff auf die Ressourcen Ihres Kontos, um Abrechnungs-, Verwaltungs- und Supportdienste bereitzustellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AWS Support.

Weitere Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Themen

Berechtigungen von serviceverknüpften Rollen für Trusted Advisor

Trusted Advisor verwendet zwei dienstbezogene Rollen:

- AWSServiceRoleForTrustedAdvisor— Diese Rolle vertraut darauf, dass der Trusted Advisor Dienst die Rolle übernimmt, in Ihrem Namen auf AWS Dienste zuzugreifen. Die Richtlinie für Rollenberechtigungen ermöglicht den Trusted Advisor schreibgeschützten Zugriff für alle Ressourcen. AWS Diese Rolle vereinfacht die ersten Schritte mit Ihrem AWS Konto, da Sie nicht die erforderlichen Berechtigungen für hinzufügen müssen. Trusted Advisor Wenn Sie ein AWS Konto eröffnen, Trusted Advisor erstellt diese Rolle für Sie. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Sie können die Berechtigungsrichtlinie keiner anderen IAM-Entität zuordnen.

  Weitere Informationen zu der beigefügten Richtlinie finden Sie unter AWSTrustedAdvisorServiceRolePolicy.
- AWSServiceRoleForTrustedAdvisorReporting – Diese Rolle vertraut dem Trusted Advisor Dienst, die Rolle für das Feature „Organisationsansicht“ zu übernehmen. Diese Rolle wird Trusted Advisor als vertrauenswürdiger Dienst in Ihrer AWS Organizations Organisation aktiviert. Trusted Advisor erstellt diese Rolle für Sie, wenn Sie die Organisationsansicht aktivieren.

  Weitere Informationen über die beigefügte Richtlinie finden Sie unter AWSTrustedAdvisorReportingServiceRolePolicy.

Sie können die Organisationsansicht verwenden, um Berichte mit Trusted Advisor Prüfergebnissen für alle Konten in Ihrer Organisation zu erstellen. Weitere Informationen über dieses Feature finden Sie unter Organisationsansicht für AWS Trusted Advisor.

Verwalten von Berechtigungen für dienstverknüpft Rollen

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Die folgenden Beispiele verwenden die `AWSServiceRoleForTrustedAdvisor` dienstverknüpft Rolle.

Example : Erlauben Sie einer IAM-Entität, die **`AWSServiceRoleForTrustedAdvisor`** dienstverknüpfte Rolle zu erstellen

Dieser Schritt ist nur erforderlich, wenn das Trusted Advisor Konto deaktiviert ist, die mit dem Dienst verknüpfte Rolle gelöscht wurde und der Benutzer die Rolle neu erstellen muss, um sie erneut zu aktivieren. Trusted Advisor

Sie können die folgende Anweisung zur Berechtigungsrichtlinie für die IAM-Entität hinzufügen, um die dienstverknüpfte Rolle zu erstellen.

```
{
    "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 : Erlauben Sie einer IAM-Entität, die Beschreibung der **`AWSServiceRoleForTrustedAdvisor`** dienstverknüpften Rolle zu bearbeiten

Sie können nur die Beschreibung der `AWSServiceRoleForTrustedAdvisor` Rolle bearbeiten. Sie können die folgende Anweisung zur Berechtigungsrichtlinie für die IAM-Entität hinzufügen, um die Beschreibung einer dienstverknüpften Rolle zu bearbeiten.

```
{
    "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 : Erlauben Sie einer IAM-Entität, die **`AWSServiceRoleForTrustedAdvisor`** dienstverknüpfte Rolle zu löschen

Sie können die folgende Anweisung zur Berechtigungsrichtlinie für die IAM-Entität hinzufügen, um eine serviceverknüpfte Rolle zu löschen.

```
{
    "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"}}
}
```

Sie können auch eine AWS verwaltete Richtlinie verwenden, um z. B. vollen AdministratorAccessZugriff auf zu gewähren. Trusted Advisor

Erstellen einer serviceverknüpften Rolle für Trusted Advisor

Sie müssen die serviceverknüpfte Rolle `AWSServiceRoleForTrustedAdvisor` nicht manuell erstellen. Wenn Sie ein AWS Konto eröffnen, Trusted Advisor wird die dienstbezogene Rolle für Sie erstellt.

> **Important**
>
> Wenn Sie den Trusted Advisor Dienst genutzt haben, bevor er mit der Unterstützung von dienstbezogenen Rollen begann, dann Trusted Advisor haben Sie die `AWSServiceRoleForTrustedAdvisor` Rolle bereits in Ihrem Konto erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt im IAM-Benutzerhandbuch.

Wenn Ihr Konto nicht über die serviceverknüpfte Rolle `AWSServiceRoleForTrustedAdvisor` verfügt, funktioniert Trusted Advisor nicht wie erwartet. Dies kann passieren, wenn ein Benutzer Trusted Advisor in Ihrem Konto deaktiviert und die serviceverknüpfte Rolle löscht. In diesem Fall können Sie die `AWSServiceRoleForTrustedAdvisor` serviceverknüpfte Rolle mit IAM erstellen und Trusted Advisor erneut aktivieren.

Um Trusted Advisor (Konsole) zu aktivieren

1. Verwenden Sie die IAM-Konsole oder die IAM-API AWS CLI, um eine serviceverknüpfte Rolle für zu erstellen. Trusted Advisor Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle.
2. Melden Sie sich bei der AWS Management Console an und navigieren Sie dann zur Konsole unter Trusted Advisor . https://console.aws.amazon.com/trustedadvisor

   Der Trusted Advisor deaktiviert-Statusbanner wird in der Konsole angezeigt.
3. Wählen Sie im Statusbanner die Option Trusted Advisor Rolle aktivieren aus. Wenn die erforderliche `AWSServiceRoleForTrustedAdvisor` nicht erkannt wird, bleibt der Statusbanner "Disabled (Deaktiviert)" bestehen.

Bearbeiten einer serviceverknüpften Rolle für Trusted Advisor

Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung nicht geändert werden. Sie können jedoch die IAM-Konsole oder die IAM-API verwenden AWS CLI, um die Beschreibung der Rolle zu bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Trusted Advisor

Wenn Sie die Funktionen oder Dienste von nicht verwenden müssen Trusted Advisor, können Sie die `AWSServiceRoleForTrustedAdvisor` Rolle löschen. Sie müssen Trusted Advisor sie deaktivieren, bevor Sie diese dienstverknüpfte Rolle löschen können. Dadurch wird verhindert, dass Sie die erforderlichen Berechtigungen für Trusted Advisor -Operationen entfernen. Wenn Sie sie deaktivieren Trusted Advisor, deaktivieren Sie alle Servicefunktionen, einschließlich Offline-Verarbeitung und Benachrichtigungen. Wenn Sie die Deaktivierung Trusted Advisor für ein Mitgliedskonto vornehmen, wirkt sich dies auch auf das separate Konto des Zahlers aus. Das bedeutet, dass Sie keine Trusted Advisor Schecks erhalten, die Aufschluss darüber geben, wie Sie Kosten sparen können. Sie können über die Konsole auf Trusted Advisor zugreifen. API-Aufrufe Trusted Advisor geben den Fehler „Zugriff verweigert“ zurück.

Sie müssen die`AWSServiceRoleForTrustedAdvisor`Die -serviceverknüpfte Rolle im -Konto verwenden, bevor Sie die Trusted Advisor aus.

Sie müssen die Funktion zunächst Trusted Advisor in der Konsole deaktivieren, bevor Sie die `AWSServiceRoleForTrustedAdvisor` dienstbezogene Rolle löschen können.

Um zu deaktivieren Trusted Advisor

1. Melden Sie sich bei der an AWS Management Console und navigieren Sie zur Trusted Advisor Konsole unterhttps://console.aws.amazon.com/trustedadvisor.
2. Klicken Sie im Navigationsbereich auf Präferenzen.
3. Wählen Sie im Abschnitt Service Linked Role Permissions (Berechtigungen der serviceverknüpften Rolle) die Option Disable Trusted Advisor(&SERVICENAME; deaktivieren) aus.
4. Bestätigen Sie im Bestätigungsdialogfeld, dass Sie deaktivieren möchten, indem Sie OK Trusted Advisor auswählen.

Nach der Deaktivierung Trusted Advisor sind alle Trusted Advisor Funktionen deaktiviert, und auf der Trusted Advisor Konsole wird nur das deaktivierte Statusbanner angezeigt.

Anschließend können Sie die IAM-Konsole, die oder die IAM-API verwenden
AWS CLI, um die angegebene Trusted Advisor dienstverknüpfte Rolle zu löschen.
`AWSServiceRoleForTrustedAdvisor` Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für AWS Support

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Themen

- AWS verwaltete Richtlinien für AWS Support
- AWS verwaltete Richtlinien für AWS Support Apps in Slack
- AWS verwaltete Richtlinien für AWS Trusted Advisor
- AWS verwaltete Richtlinien für AWS Support Pläne

AWS verwaltete Richtlinien für AWS Support

AWS Support hat die folgenden verwalteten Richtlinien.

Inhalt

- AWS verwaltete Richtlinie: AWSSupportServiceRolePolicy
- AWS Support Aktualisierungen der AWS verwalteten Richtlinien
- Berechtigungsänderungen für AWSSupportServiceRolePolicy

AWS verwaltete Richtlinie: AWSSupportServiceRolePolicy

AWS Support verwendet die AWSSupportServiceRolePolicy AWS verwaltete Richtlinie. Diese verwaltete Richtlinie ist mit der `AWSServiceRoleForSupport` dienstverknüpften Rolle verbunden. Die Richtlinie erlaubt es der mit dem dienstverknüpften Rolle, Aktionen in Ihrem Namen durchzuführen. Sie können diese Richtlinie nicht mit Ihren IAM-Entitäten verknüpfen. Weitere Informationen finden Sie unter Berechtigungen von serviceverknüpften Rollen für AWS Support.

Eine Liste der Änderungen an der Richtlinie finden Sie unter AWS Support Aktualisierungen der AWS verwalteten Richtlinien und Berechtigungsänderungen für AWSSupportServiceRolePolicy.

AWS Support Aktualisierungen der AWS verwalteten Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AWS Support seit Beginn der Nachverfolgung dieser Änderungen durch diese Dienste vorgenommen wurden. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

In der folgenden Tabelle werden wichtige Aktualisierungen der AWS Support verwalteten Richtlinien seit dem 17. Februar 2022 beschrieben.

AWS Support

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Diensten wurden 17 neue Berechtigungen zur Durchführung von Aktionen zur Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, administrativem und technischem Support hinzugefügt: • Amazon CloudWatch Network Monitor — Zur Behebung von Problemen im Zusammenhang mit dem Network Monitor-Service. • Amazon CloudWatch Logs — Um Probleme im Zusammenhang mit Amazon CloudWatch Logs zu debuggen. • Amazon Managed Streaming for Apache Kafka — Zum Debuggen von	22. März 2024

Änderung	Beschreibung	Datum
	Problemen im Zusammenhang mit Amazon Managed Streaming for Apache Kafka. • Amazon Managed Service für Prometheus — Zur Behebung von Problemen im Zusammenhang mit dem Amazon Managed Service für Prometheus.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Für die folgenden Dienste wurden 63 neue Berechtigungen zur Durchführung von Aktionen zur Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, administrativem und technischem Support hinzugefügt: • AWS Reinräume — Zur Behebung von Problemen im Zusammenhang mit AWS Reinräumen. • CodeConnections — Zur Behebung von Problemen im Zusammenhang mit CodeConnections. • Amazon EKS — Zum Debuggen von Problemen im Zusammenhang mit Amazon EKS. • Image Builder — Zum Debuggen von Problemen im Zusammenhang mit dem Image Builder. • Amazon Inspector2 — Zur Behebung von Problemen im Zusammenhang mit Amazon Inspector2. • Amazon Inspector Scan — Zum Debuggen von Problemen im Zusammenh	17. Januar 2024

Änderung	Beschreibung	Datum
	ang mit dem Amazon Inspector Scan. • Amazon CloudWatch Logs — Zur Behebung von Problemen im Zusammenhang mit Amazon CloudWatch Logs. • AWS Outposts — Zur Behebung von Problemen im Zusammenhang mit dem AWS Outposts. • Amazon RDS – Zum Debuggen von Problemen im Zusammenhang mit Amazon RDS. • AWS IAM Identity Center — Zur Behebung von Problemen im Zusammenhang mit AWS IAM Identity Center. • Amazon S3 Express — Zum Debuggen von Problemen im Zusammenhang mit Amazon S3 Express. • AWS Trusted Advisor — Zur Behebung von Problemen im Zusammenhang AWS Trusted Advisor mit.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Es wurden 126 neue Berechtigungen für die folgenden Dienste hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit der Abrechnung, dem administrativen und technischen Support helfen: • AWS Direct Connect — Um Probleme im Zusammenhang mit dem AWS Direct Connect Service zu beheben. • Amazon SageMaker — Zur Behebung von Problemen im Zusammenhang mit dem SageMaker Service von Amazon. • Amazon AppStream — Zum Debuggen von Problemen im Zusammenhang mit Amazon AppStream. • AWS Ressourcen Explorer — Um Probleme im Zusammenhang mit dem zu debuggen. AWS Ressourcen Explorer • Amazon Redshift serverless — Zur Behebung von Problemen im Zusammenh	6. Dezember 2023

Änderung	Beschreibung	Datum
	ang mit Amazon Redshift serverless. • Amazon ElastiCache — Zum Debuggen von Problemen im Zusammenhang mit Amazon ElastiCache. • Amazon Comprehend – Zur Behebung von Problemen im Zusammenhang mit Amazon Comprehend. • Amazon EC2 — Zur Behebung von Problemen im Zusammenhang mit Amazon EC2. • Amazon Elastic Kubernetes Service — Zum Debuggen von Problemen im Zusammenhang mit Amazon Elastic Kubernetes Service. • AWS Elastic Disaster Recovery — Zur Behebung von Problemen im Zusammenhang mit. AWS Elastic Disaster Recovery • AWS AppSync — Zum Debuggen von Problemen im Zusammenhang AWS AppSync mit. • Amazon CloudWatch Logs — Zur Behebung von Problemen im Zusammenh	

Änderung	Beschreibung	Datum
	ang mit Amazon CloudWatch Logs. • AWS Health — Um Probleme im Zusammenhang mit dem AWS Health Service zu debuggen. • Amazon Connect — Zum Debuggen von Problemen im Zusammenhang mit Amazon Connect. • AWS Snowball — Zur Behebung von Problemen im Zusammenhang AWS Snowball mit. • AWS Health Imaging — Zur Behebung von Problemen im Zusammenhang mit AWS Health Imaging.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 163 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Amazon CloudFront — Zur Behebung von Problemen im Zusammenhang mit dem CloudFront Service. • Amazon EC2 – Zur Behebung von Problemen im Zusammenhang mit Amazon EC2. • Amazon AppStream — Zum Debuggen von Problemen im Zusammenhang mit Amazon AppStream. • AWS WAF — Um Probleme im Zusammenhang mit der AWS Web Application Firewall zu debuggen. • Amazon Connect – Zur Behebung von Problemen im Zusammenhang mit Amazon Connect. • AWS IoT — Zum Debuggen von Problemen im	27. Oktober 2023

Änderung	Beschreibung	Datum
	Zusammenhang mit dem. AWS IoT • Amazon Route 53 – Zur Behebung von Problemen im Zusammenhang mit Amazon Route 53. • AWS Verifizierter Zugriff — Zur Behebung von Problemen im Zusammenhang mit dem AWS Verified Access-Dienst. • Amazon Simple Email Service – Zum Debuggen von Problemen im Zusammenhang mit Amazon Simple Email Service. • AWS Elastic Beanstalk — Zur Behebung von Problemen im Zusammenhang mit AWS Elastic Beanstalk. • Amazon DynamoDB – Zum Debuggen von Problemen im Zusammenhang mit Amazon DynamoDB. • AWS EC2 Image Builder — Zur Behebung von Problemen im Zusammenhang mit AWS EC2 Image Builder. • AWS Outposts — Um Probleme im Zusammenh	

Änderung	Beschreibung	Datum
	ang mit dem Service zu debuggen. AWS Outposts • AWS Glue — Um Probleme im Zusammenhang mit dem zu debuggen. AWS Glue • AWS Directory Service — Zur Behebung von Problemen im Zusammenh ang AWS Directory Service mit. • AWS Elastic Disaster Recovery — Zur Behebung von Problemen im Zusammenhang mit AWS Elastic Disaster Recovery. • AWS Step Functions — Zum Debuggen von Problemen im Zusammenh ang AWS Step Functions mit. • Amazon EMR – Zur Behebung von Problemen im Zusammenhang mit Amazon EMR. • Amazon Relational Database Service – Zur Behebung von Problemen im Zusammenhang mit Amazon Relational Database Service. • Amazon EC2 Systems Manager – Zum Debuggen von Problemen im	

Änderung	Beschreibung	Datum
	Zusammenhang mit Amazon EC2 Systems Manager.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 176 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • AWS Glue — Um Probleme im Zusammenhang mit dem AWS Glue Service zu beheben • Amazon EMR – Zur Behebung von Problemen im Zusammenhang mit dem Amazon-EMR-Service. • Amazon Security Lake – Zum Debuggen von Problemen im Zusammenhang mit Amazon Security Lake. • AWS Systems Manager — Zum Debuggen von Problemen im Zusammenhang mit dem Systems Manager Manager-Dienst. • Amazon Verified Permissions – Zur Behebung von Problemen im Zusammenhang mit Amazon Verified Permissions.	28. August 2023

Änderung	Beschreibung	Datum
	• AWS IAM Access Analyzer — Zum Debuggen von Problemen im Zusammenhang mit dem IAM Access Analyzer-Dienst. • AWS Backup — Zur Behebung von Problemen im Zusammenhang mit. AWS Backup • AWS Database Migration Service — Zur Behebung von Problemen im Zusammenhang mit dem DMS-Dienst. • Amazon DynamoDB – Zum Debuggen von Problemen im Zusammenhang mit DynamoDB. • Amazon Elastic Container Registry (Amazon ECR) – Zur Behebung von Problemen im Zusammenhang mit Amazon Elastic Container Registry (Amazon ECR). • Amazon Elastic Container Service – Zum Debuggen von Problemen im Zusammenhang mit Amazon Elastic Container Service. • Amazon Elastic Kubernetes Service – Zur Behebung von Problemen im Zusammenh	

Änderung	Beschreibung	Datum
	ang mit Amazon Elastic Kubernetes Service. • Amazon EMR Serverles s — Zum Debuggen von Problemen im Zusammenh ang mit dem Amazon-EMR-Serverless-Service. • AWS Identity and Access Management — Zur Behebung von Problemen im Zusammenhang AWS Identity and Access Management mit. • AWS Network Firewall — Zur Behebung von Problemen im Zusammenh ang mit der AWS Network Firewall. • AWS HealthOmics — Zum Debuggen von Problemen im Zusammenhang AWS HealthOmics mit. • Amazon QuickSight — Zum Debuggen von Problemen im Zusammenhang mit Amazon QuickSight. • Amazon Relational Database Service – Zur Behebung von Problemen im Zusammenhang mit Amazon Relational Database Service.	

Änderung	Beschreibung	Datum
	• Amazon Redshift – Zur Behebung von Problemen im Zusammenhang mit Amazon Redshift. • Amazon Redshift Serverless – Zum Debuggen von Problemen im Zusammenhang mit Amazon Redshift Serverless. • Amazon SageMaker — Zum Debuggen von Problemen im Zusammenhang mit Amazon SageMaker.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 141 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Lambda – Zur Behebung von Problemen im Zusammenhang mit dem Lambda-Service. • Amazon Lex – Zur Behebung von Problemen im Zusammenhang mit dem Amazon-Lex-Service. • AWS Transfer — Zum Debuggen von Problemen im Zusammenhang mit dem Transfer-Service. • AWS Amplify — Um Probleme im Zusammenhang mit dem Amplify-Dienst zu debuggen. • Amazon EventBridge Pipes — Zur Behebung von Genehmigungs- und Abrechnungsproblemen im Zusammenhang mit Pipes. • Amazon EventBridge — Um Probleme im Zusammenh	26. Juni 2023

Änderung	Beschreibung	Datum
	ang mit Amazon zu debuggen EventBridge • Amazon CloudWatch Logs — Zur Behebung von Problemen im Zusammenhang mit Amazon CloudWatch Logs. • AWS Systems Manager — Zur Behebung von Problemen im Zusammenhang mit Systems Manager. • Amazon CloudWatch — Zum Debuggen von Problemen im Zusammenhang CloudWatch mit. • Amazon ElastiCache — Zur Behebung von Problemen im Zusammenhang mit Amazon ElastiCache. • Amazon Athena – Zum Debuggen von Problemen im Zusammenhang mit Athena. • AWS Elastic Disaster Recovery — Zur Behebung von Problemen im Zusammenhang mit Elastic Disaster Recovery. • Amazon CloudWatch — Zur Fehlerbehebung bei Konfigurationen von Amazon CloudWatch.	

Änderung	Beschreibung	Datum
	• Amazon EC2 – Zum Debuggen von Problemen im Zusammenhang mit dem EC2-Service. • AWS Certificate Manager — Zur Behebung von Problemen im Zusammenhang mit Certificate Manager. • Amazon EventBridge Scheduler — Zur Behebung von Problemen im Zusammenhang mit EventBridge Scheduler. • Amazon OpenSearch Service — Zur Behebung von Problemen im Zusammenhang mit OpenSearch. • Amazon EventBridge Schemas — Zum Debuggen von Problemen im Zusammenhang EventBridge mit Schemas. • AWS Benutzerbenachrichtigungen — Zur Behebung von Problemen im Zusammenhang mit Benutzerbenachrichtigungen. • Amazon CloudWatch Application Insights — Zur Behebung von Problemen im Zusammenhang mit	

Änderung	Beschreibung	Datum
	CloudWatch Application Insights. • Amazon DynamoDB – Zur Behebung von Problemen im Zusammenhang mit DynamoDB. • Amazon DocumentDB Elastic Clusters – Zur Behebung von Problemen im Zusammenhang mit DocumentDB Elastic Clusters.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 53 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Auto Scaling – Zur Behebung von Problemen im Zusammenhang mit dem Auto-Scaling-Service. • Amazon CloudWatch — Zur Behebung von Problemen im Zusammenhang mit Amazon CloudWatch. • AWS Compute Optimizer — Um Probleme im Zusammenhang mit Compute Optimizer zu beheben. • Amazon CloudWatch Evidently — Zur Behebung von Problemen im Zusammenhang mit Eviently. • EC2 Image Builder – Zur Behebung von Problemen im Zusammenhang mit dem Image-Builder-Service.	02. Mai 2023

Änderung	Beschreibung	Datum
	• AWS IoT TwinMaker — Zur Behebung von Problemen im Zusammenhang mit. AWS IoT TwinMaker • Amazon CloudWatch Logs — Zur Behebung von Problemen im Zusammenhang mit Amazon CloudWatch Logs. • Amazon Pinpoint – Zur Behebung von Problemen im Zusammenhang mit Amazon Pinpoint. • AWS OAM-Link — Zum Debuggen von Problemen im Zusammenhang mit OAM-Ressourcen. • AWS Outposts — Zur Behebung von Problemen im Zusammenhang mit. AWS Outposts • Amazon RDS – Zum Debuggen von Problemen im Zusammenhang mit Amazon RDS. • AWS Ressourcen Explorer — Zur Behebung von Problemen im Zusammenhang mit Resource Explorer. • Amazon CloudWatch RUM — Zur Fehlerbehebung bei Konfigurationen von RUM-Serviceressourcen.	

Änderung	Beschreibung	Datum
	• Amazon SNS – Zur Behebung von Problemen im Zusammenhang mit Amazon SNS. • Amazon CloudWatch Synthetics — Zur Behebung von Problemen im Zusammenhang mit CloudWatch Synthetics.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 52 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • AWS Backup gateway — Zur Behebung von Problemen im Zusammenhang mit dem Backup-Gateway. • Amazon S3 – Zum Debuggen von Problemen im Zusammenhang mit Amazon S3. • AWS Application Migration Service — Zur Behebung von Problemen im Zusammenhang mit dem Application Migration Service. • AWS Reinräume — Um Probleme im Zusammenhang mit AWS Reinräumen zu beheben; • AWS Systems Manager für SAP — Zur Behebung von Problemen im Zusammenh	16. März 2023

Änderung	Beschreibung	Datum
	ang mit AWS Systems Manager für SAP. • Amazon VPC Lattice – Zum Debuggen von Problemen im Zusammenhang mit Amazon VPC Lattice.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 220 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Amazon Athena — Um die Entwicklung von Tools AWS Support zu ermöglichen, mit denen Kunden bei ihren Fragen zu Athena unterstützt werden können. • Amazon Chime – Zur Behebung von Problemen im Zusammenhang mit Amazon Chime. • Amazon CloudWatch Internet Monitor — Zum Debuggen von Problemen im Zusammenhang mit Internet Monitor. • Amazon Comprehend – Zur Behebung von Problemen im Zusammenhang mit Amazon Comprehend. • Amazon Elastic Compute Cloud – Zum Debuggen von Problemen im Zusammenhang mit Transit Gateway	10. Januar 2023

Änderung	Beschreibung	Datum
	Connect und Multicast-Funktionen. • Amazon EventBridge Pipes — Zur Behebung von Problemen im Zusammenhang mit EventBridge Pipes. • Amazon Interactive Video Service — Um die Abfrage von Amazon IVS-Ressourcen zur Behebung von Kundenproblemen zu ermöglichen AWS Support . • Amazon FSx — Um die Entwicklung von Tools AWS Support zur Unterstützung des Imports und Exports für ein Amazon FSx-Datenrepository zu ermöglichen. • Amazon GameLift — Zur Behebung von Problemen im Zusammenhang mit Amazon GameLift. • AWS Glue– Zur Behebung von Problemen im Zusammenhang mit AWS Glue -Datenqualität. • Amazon Kinesis Video Streams – Um Probleme im Zusammenhang mit Kinesis Video Streams zu beheben. • Amazon Managed Service for Prometheus – Zur Behebung von Problemen	

Änderung	Beschreibung	Datum
	im Zusammenhang mit Amazon Managed Service for Prometheus. • Amazon Managed Streaming for Apache Kafka – Zur Behebung von Problemen im Zusammenhang mit Amazon MSK Connect. • AWS Network Manager — Zur Behebung von Problemen im Zusammenhang mit Network Manager. • Amazon Nimble Studio – Zum Debuggen von Problemen im Zusammenhang mit Nimble Studio. • Amazon Personalize – Zum Debuggen von Problemen im Zusammenhang mit Amazon Personalize. • Amazon Pinpoint – Zur Behebung von Problemen im Zusammenhang mit Amazon Pinpoint. • AWS HealthOmics — Zur Behebung von Problemen im Zusammenhang mit HealthOmics. • Amazon Transcribe – Zum Debuggen von Problemen im Zusammenhang mit Amazon Transcribe.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 47 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • AWS Application Migration Service — Zur Behebung von Problemen bei der Replikation und beim Start. • AWS CloudFormation Hooks — Um die Entwicklung von Automatisierungstools AWS Support zu ermöglichen, die bei der Lösung von Problemen helfen können. • Amazon Elastic Kubernetes Service – Zur Behebung von Problemen im Zusammenhang mit Amazon EKS. • AWS IoT FleetWise – Zur Behebung von Problemen im Zusammenhang mit AWS IoT FleetWise. • AWS Mainframe Modernization — Um Probleme im Zusammenhang mit der	4. Oktober 2022

Änderung	Beschreibung	Datum
	Mainframe-Modernisierung zu debuggen. • AWS Outposts — Um zu helfen, eine Liste mit dedizierten Hosts und Ressourcen zu AWS Support erhalten. • AWS Private 5G – Zur Behebung von Problemen im Zusammenhang mit Private 5G. • AWS Tiros – Zum Debuggen von Problemen im Zusammenhang mit Tiros.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 46 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Amazon Managed Streaming for Apache Kafka – Zur Behebung von Problemen im Zusammenhang mit Amazon MSK. • AWS DataSync — Zur Behebung von Problemen im Zusammenhang mit DataSync. • AWS Elastic Disaster Recovery — Zur Behebung von Problemen bei der Replikation und beim Start. • Amazon GameSparks — Zur Behebung von Problemen im Zusammenhang mit GameSparks. • AWS IoT TwinMaker — Zum Debuggen von Problemen im Zusammenhang AWS IoT TwinMaker mit.	17. August 2022

Änderung	Beschreibung	Datum
	• AWS Lambda — Um die Konfiguration einer Funktions-URL zur Behebung von Problemen anzuzeigen. • Amazon Lookout für Equipment – Zur Behebung von Problemen im Zusammenhang mit Lookout for Equipment. • Amazon Route 53 und Amazon Route 53 Resolver — Um Resolver-Konfigurationen abzurufen, mit denen das DNS-Auflösungsverhalten einer VPC überprüft werden AWS Support kann.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • Amazon CloudWatch Logs — Um bei der Behebung von Problemen im Zusammenhang mit CloudWatch Logs zu helfen. • Amazon Interactive Video Service — Zur Unterstützung bei der AWS Support Überprüfung vorhandener Amazon IVS-Ressourcen für Supportfälle im Zusammenhang mit Betrug oder kompromittierten Konten. • Amazon Inspector – Zur Behebung von Problemen mit Amazon Inspector. Berechtigungen für Dienste wie Amazon wurden entfernt WorkLink. Amazon WorkLink wurde am 19. April 2022 als veraltet eingestuft.	23. Juni 2022

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 25 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • AWS Amplify UI Builder — Zur Behebung von Problemen im Zusammenhang mit der Generierung von Komponenten und Designs. • Amazon AppStream — Um Probleme zu beheben, indem Ressourcen für Funktionen abgerufen werden, die kürzlich eingeführt wurden. • AWS Backup — Zur Behebung von Problemen im Zusammenhang mit Backup-Jobs. • AWS CloudFormation — Zur Durchführung von Diagnosen bei Problemen im Zusammenhang mit IAM, Erweiterungen und Versionierung.	27. April 2022

Änderung	Beschreibung	Datum
	• Amazon Kinesis: Um Probleme im Zusammenh ang mit Kinesis zu beheben. • AWS Transfer Family — Um Probleme im Zusammenh ang mit Transfer Family zu beheben.	

Änderung	Beschreibung	Datum

AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 54 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen:
	• Amazon Elastic Compute Cloud
	  • Um Probleme im Zusammenhang mit Kunden und von AWS verwalteten Listen mit Präfix zu beheben.
	  • Um Probleme im Zusammenhang mit Amazon VPC IP Address Manager (IPAM) zu beheben.
	• AWS Network Manager — Zur Behebung von Problemen im Zusammenhang mit Network Manager.
	• Savings Plans - Um Metadaten über ausstehende Savings Plans Verpflichtungen zu erhalten.
	• AWS Serverless Application Repository — Zur Verbesserung und Unterstützung von
		14. März 2022

Änderung	Beschreibung	Datum
	Reaktionsmaßnahmen im Rahmen der Untersuchung und Lösung von Supportfällen. • Amazon WorkSpaces Web — Zum Debuggen und Beheben von Problemen mit WorkSpaces Webdiensten.	

Änderung	Beschreibung	Datum
AWSSupportServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Den folgenden Services wurden 74 neue Berechtigungen hinzugefügt, um Aktionen durchzuführen, die bei der Behebung von Kundenproblemen im Zusammenhang mit Abrechnung, Administration und technischem Support helfen: • AWS Application Migration Service — Zur Unterstützung der agentenlosen Replikation im Application Migration Service. • AWS CloudFormation — Zur Durchführung von Diagnosen bei Problemen im Zusammenhang mit IAM, Erweiterungen und Versionierung. • Amazon CloudWatch Logs — Zur Validierung von Ressourcenrichtlinien. • Amazon EC2 Recycle Bin – Rufen Sie Metadaten zu Aufbewahrungsregeln für den Recycle Bin (Papierkorb) ab. • AWS Elastic Disaster Recovery — Zur Behebung von Replikations- und	17. Februar 2022

Änderung	Beschreibung	Datum
	Startproblemen in Kundenkonten. • Amazon FSx – Zeigen Sie die Beschreibung von Amazon-FSx-Snapshots an. • Amazon Lightsail – Zeigen Sie Metadaten und Konfigurationsdetails für Lightsail-Buckets an. • Amazon Macie – Zeigen Sie Macie-Konfiguratio nen wie Klassifizierungsau fträge, benutzerdefinierte Datenbezeichner, reguläre Ausdrücke und Ergebnisse an. • Amazon S3 – Sammeln Sie Metadaten und Konfigura tionen für Amazon-S3-Buckets. • AWS Storage Gateway — Um Metadaten zu den Richtlinien der Kunden für die automatische Banderste llung einzusehen. • Elastic Load Balancing – Zeigen Sie bei der Verwendung der Service–Quotas-Konsole die Beschreibung der Ressourcenlimits an.	

Änderung	Beschreibung	Datum
	Weitere Informationen finden Sie unter Berechtigungsänderungen für AWSSupportServiceRolePolicy.	
Änderungsprotokoll veröffentlicht	Änderungsprotokoll für die AWS Support verwalteten Richtlinien.	17. Februar 2022

Berechtigungsänderungen für AWSSupportServiceRolePolicy

Die meisten Berechtigungen wurden hinzugefügt, AWS Support um das Aufrufen einer API-Operation mit demselben Namen zu `AWSSupportServiceRolePolicy` ermöglichen. Einige API-Vorgänge erfordern jedoch Berechtigungen mit einem anderen Namen.

In der folgenden Tabelle sind nur die API-Vorgänge aufgeführt, die Berechtigungen mit einem anderen Namen erfordern. Diese Tabelle beschreibt diese Unterschiede ab dem 17. Februar 2022.

Datum	Name des API-Vorgangs	Erforderliche Richtlinien-Berechtigung
Berechtigungen wurden am 17. Februar 2022 hinzugefügt	`s3.GetBucketAnalyticsConfiguration` `s3.ListBucketAnalyticsConfiguration`	`s3:GetAnalyticsConfiguration`
	`s3.GetBucketNotificationConfiguration`	`s3:GetBucketNotification`
	`s3.GetBucketEncryption`	`s3:GetEncryptionConfiguration`
	`s3.GetBucketIntelligentTieringConfiguration`	`s3:GetIntelligentTieringConfiguration`

Datum	Name des API-Vorgangs	Erforderliche Richtlinien-Berechtigung
	s3.ListBucketIntelligentTieringConfiguration	
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	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 verwaltete Richtlinien für AWS Support Apps in Slack

> **Note**
>
> Informationen zum Zugriff auf und zum Anzeigen von Supportfällen in der AWS Support Center Console finden Sie unterZugriff auf das AWS Support Center verwalten.

AWS Support Die App verfügt über die folgenden verwalteten Richtlinien.

Inhalt

- AWS verwaltete Richtlinie: AWSSupportAppFullAccess
- AWS verwaltete Richtlinie: AWSSupportAppReadOnlyAccess
- AWS Support App-Updates für verwaltete AWS Richtlinien

AWS verwaltete Richtlinie: AWSSupportAppFullAccess

Sie können die AWSSupportAppFullAccess-verwaltete Richtlinie verwenden, um der IAM-Rolle die Berechtigungen für Ihre Slack-Kanalkonfigurationen zu gewähren. Sie können die AWSSupportAppFullAccess-Richtlinie auch Ihren IAM-Entitäten anfügen.

Weitere Informationen finden Sie unter AWS Support App in Slack.

Diese Richtlinie gewährt der Entität Berechtigungen, die es der Entität ermöglichen AWS Support, Service Quotas und IAM-Aktionen für die AWS Support App durchzuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `servicequotas` – Beschreibt Ihre bestehenden Servicekontingente und Anforderungen und erstellt Servicekontingent-Erhöhungen für Ihr Konto.
- `support` – Erstellt, aktualisiert und löst Ihre Support-Fälle. Aktualisiert und beschreibt Informationen zu Ihren Fällen, z. B. Dateianhänge, Korrespondenzen und Schweregrade. Initiiert Live-Chat-Sitzungen mit einem Support-Kundendienstmitarbeiter.

- `iam` – Erstellt eine serviceverknüpfte Rolle für Service Quotas.

```
{
    "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"}
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support-App.

AWS verwaltete Richtlinie: AWSSupportAppReadOnlyAccess

Die AWSSupportAppReadOnlyAccessRichtlinie gewährt der Entität Berechtigungen, die es der Entität ermöglichen, schreibgeschützte AWS Support App-Aktionen auszuführen. Weitere Informationen finden Sie unter AWS Support App in Slack.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `support` – Beschreibt Support-Falldetails und Mitteilungen, die den Support-Fällen hinzugefügt wurden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Support App-Updates für verwaltete AWS Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Support App an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

In der folgenden Tabelle werden wichtige Aktualisierungen der von der AWS Support App verwalteten Richtlinien seit dem 17. August 2022 beschrieben.

AWS Support App

Änderung	Beschreibung	Datum
AWSSupportAppFullAccessund AWSSupportAppReadOnlyAccess Neue AWS verwaltete Richtlinien für die AWS Support App	Sie können diese Richtlinien für die IAM-Rolle verwenden, die Sie für die Konfiguration Ihres Slack-Kanals konfigurieren. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support-App.	19. August 2022
Änderungsprotokoll veröffentlicht	Änderungsprotokoll für die von der AWS Support App verwalteten Richtlinien.	19. August 2022

AWS verwaltete Richtlinien für AWS Trusted Advisor

Trusted Advisor hat die folgenden AWS verwalteten Richtlinien.

Inhalt

- AWS verwaltete Richtlinie: AWSTrustedAdvisorPriorityFullAccess
- AWS verwaltete Richtlinie: AWSTrustedAdvisorPriorityReadOnlyAccess
- AWS verwaltete Richtlinie: AWSTrustedAdvisorServiceRolePolicy
- AWS verwaltete Richtlinie: AWSTrustedAdvisorReportingServiceRolePolicy
- Trusted Advisor Aktualisierungen AWS verwalteter Richtlinien

AWS verwaltete Richtlinie: AWSTrustedAdvisorPriorityFullAccess

Die AWSTrustedAdvisorPriorityFullAccessRichtlinie gewährt vollen Zugriff auf Trusted Advisor Priority. Diese Richtlinie ermöglicht es dem Benutzer auch, Trusted Advisor als vertrauenswürdigen Dienst Priority hinzuzufügen AWS Organizations und die delegierten Administratorkonten für Trusted Advisor Priority anzugeben.

Details zu Berechtigungen

In der ersten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `trustedadvisor`:

- Beschreibt Ihr Konto und Ihre Organisation.
- Beschreibt die identifizierten Risiken von Trusted Advisor Priority. Mit den Berechtigungen können Sie den Risikostatus herunterladen und aktualisieren.
- Beschreibt Ihre Konfigurationen für Trusted Advisor Priority-E-Mail-Benachrichtigungen. Mit den Berechtigungen können Sie die E-Mail-Benachrichtigungen konfigurieren und für Ihre delegierten Administratoren deaktivieren.
- Wird Trusted Advisor so eingerichtet, dass Ihr Konto aktiviert werden kann AWS Organizations.

In der zweiten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `organizations`:

- Beschreibt Ihr Trusted Advisor Konto und Ihre Organisation.
- Führt die Organizations auf AWS-Services , die Sie für die Verwendung von Organisationen aktiviert haben.

In der dritten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `organizations`:

- Führt die delegierten Administratoren für Trusted Advisor Priorität auf.
- Aktiviert und deaktiviert den vertrauenswürdigen Zugriff mit Organisationen.

In der vierten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `iam`:

- Erstellt die `AWSServiceRoleForTrustedAdvisorReporting`-serviceverknüpfte Rolle.

In der fünften Anweisung enthält die Richtlinie die folgenden Berechtigungen für `organizations`:

- Ermöglicht es Ihnen, delegierte Administratoren für die Trusted Advisor -Priorität zu registrieren und abzumelden.

```
{
 "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 verwaltete Richtlinie: AWSTrustedAdvisorPriorityReadOnlyAccess

Die AWSTrustedAdvisorPriorityReadOnlyAccessRichtlinie gewährt Trusted Advisor Priority nur Leseberechtigungen, einschließlich der Berechtigung, die delegierten Administratorkonten einzusehen.

Details zu Berechtigungen

In der ersten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `trustedadvisor`:

- Beschreibt Ihr Trusted Advisor Konto und Ihre Organisation.
- Beschreibt die in Trusted Advisor Priority identifizierten Risiken und ermöglicht es Ihnen, sie herunterzuladen.

- Beschreibt die Konfigurationen für Trusted Advisor Priority E-Mail-Benachrichtigungen.

In der zweiten und dritten Anweisung enthält die Richtlinie die folgenden Berechtigungen für `organizations`:

- Beschreibt Ihre Organisation mit Organisationen.
- Führt die Organizations auf AWS-Services , die Sie für die Verwendung von Organisationen aktiviert haben.
- Führt die delegierten Administratoren für Priorität auf Trusted Advisor

```
{
 "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 verwaltete Richtlinie: AWSTrustedAdvisorServiceRolePolicy

Diese Richtlinie ist mit der `AWSServiceRoleForTrustedAdvisor` dienstverknüpften Rolle verbunden. Es ermöglicht der serviceverknüpften Rolle, Aktionen für Sie durchzuführen. Sie können die AWSTrustedAdvisorServiceRolePolicy nicht an Ihre AWS Identity and Access Management (IAM)-Entitäten anhängen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Trusted Advisor.

Diese Richtlinie gewährt administrative Berechtigungen, die der serviceverknüpften Rolle den Zugriff auf AWS-Services ermöglichen. Diese Berechtigungen ermöglichen es den Checks für Trusted Advisor , Ihr Konto zu bewerten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `accessanalyzer`— Beschreibt AWS Identity and Access Management Access Analyzer Ressourcen
- `Auto Scaling` – Beschreibt die Kontingente und Ressourcen von Amazon EC2 Auto Scaling
- `cloudformation`— Beschreibt AWS CloudFormation (CloudFormation) Kontokontingente und -stapel
- `cloudfront`— Beschreibt CloudFront Amazon-Distributionen
- `cloudtrail`— Beschreibt AWS CloudTrail (CloudTrail) Wege
- `dynamodb` – Beschreibt die Amazon DynamoDB-Kontingente und -Ressourcen

- `dynamodbaccelerator`— Beschreibt DynamoDB Accelerator-Ressourcen
- `ec2` – Beschreibt die Kontingente und Ressourcen von Amazon Elastic Compute Cloud (Amazon EC2)
- `elasticloadbalancing` – Beschreibt Konto-Kontingente und -Ressourcen für Elastic Load Balancing (ELB)
- `iam` – Ruft IAM-Ressourcen ab, z. B. Anmeldedaten, Kennwortrichtlinien und Zertifikate
- `networkfirewall`— Beschreibt Ressourcen AWS Network Firewall
- `kinesis` – Beschreibt die Kontokontingente von Amazon Kinesis (Kinesis)
- `rds` – Beschreibt die Ressourcen von Amazon Relational Database Service (Amazon RDS)
- `redshift` – Beschreibt die Ressourcen von Amazon Redshift
- `route53` – Beschreibt die Kontingente und Ressourcen von Amazon Route 53
- `s3` – Beschreibt die Ressourcen des Amazon Simple Storage Service (Amazon S3)
- `ses` – Erhält Amazon Simple Email Service (Amazon SES) Sendekontingente
- `sqs` – Listet Amazon Simple Queue Service (Amazon SQS)-Warteschlangen auf
- `cloudwatch`— Ruft Metrikstatistiken von Amazon CloudWatch CloudWatch Events (Events) ab
- `ce` – Ruftvon Empfehlungen des Cost Explorer Service (Cost Explorer) ab
- `route53resolver`— Ruft Amazon Route 53 Resolver Resolver-Endpunkte und Ressourcen ab
- `kafka` – Ruft Amazon Managed Streaming für Apache-Kafka-Ressourcen ab
- `ecs`— Ruft Amazon ECS-Ressourcen ab
- `outposts`— Ruft AWS Outposts Ressourcen ab

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

Diese Richtlinie ist der `AWSServiceRoleForTrustedAdvisorReporting` dienstbezogenen Rolle zugeordnet, mit der Aktionen für die Funktion Trusted Advisor „Organisationsansicht“ ausgeführt werden können. Sie können die AWSTrustedAdvisorReportingServiceRolePolicy nicht an Ihre IAM-Entitäten anhängen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Trusted Advisor.

Diese Richtlinie gewährt Administratorberechtigungen, die es der dienstbezogenen Rolle ermöglichen, Aktionen auszuführen AWS Organizations .

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations` – Beschreibt Ihre Organisation und listet den Servicezugang, Konten, Eltern, Kinder und Organisationseinheiten auf.

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

Trusted Advisor Aktualisierungen AWS verwalteter Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für AWS Support und Trusted Advisor seit Beginn der Nachverfolgung dieser Änderungen durch diese Dienste. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

In der folgenden Tabelle werden wichtige Aktualisierungen der Trusted Advisor verwalteten Richtlinien seit dem 10. August 2021 beschrieben.

Trusted Advisor

Änderung	Beschreibung	Datum
AWSTrustedAdvisorServiceRolePolicy	Trusted Advisor neue Aktionen hinzugefügt, um die `sqs:GetQu`	11. Juni 2024

Änderung	Beschreibung	Datum
Aktualisierung einer vorhandenen Richtlinie.	`eueAttributes` Berechtigungen `access-an alyzer:ListAnalyze rs cloudwatch:ListMet rics ,dax:Descr ibeCluste rs ,,ec2:Descr ibeNatGat eways ,ec2:Descr ibeRouteT ables ,ec2:Descr ibeVpcEnd points ,ec2:GetMa nagedPref ixListEntries , elasticloadbalanci ng:DescribeTargetH ealth iam:ListS AMLProviders , kafka:DescribeClus terV2 network-f irewall:ListFirewa lls network-f irewall:DescribeFi rewall` und zu gewähren.	

Änderung	Beschreibung	Datum
AWSTrustedAdvisorServiceRolePolicy Aktualisierung einer bestehenden Richtlinie.	Trusted Advisor neue Aktionen hinzugefügt, um die `cloudtrail:GetTrail` `cloudtrail:ListTrails` `cloudtrail:GetEventSelectors` `outposts:GetOutpost` , `outposts:ListAssets` und `outposts:ListOutposts` Berechtigungen zu gewähren.	18. Januar 2024
AWSTrustedAdvisorPriorityFullAccess Aktualisierung einer bestehenden Richtlinie.	Trusted Advisor `AWSTrustedAdvisorPriorityFullAccess` AWS hat die verwaltete Richtlinie aktualisiert, sodass sie Kontoausweis-IDs enthält.	6. Dezember 2023
AWSTrustedAdvisorPriorityReadOnlyAccess Aktualisierung auf eine bestehende Richtlinie.	Trusted Advisor `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS hat die verwaltete Richtlinie aktualisiert, sodass sie Kontoausweis-IDs enthält.	6. Dezember 2023
AWSTrustedAdvisorServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Trusted Advisor neue Aktionen hinzugefügt, um die `ec2:DescribeRegions` `s3:GetLifecycleConfiguration` `ecs:DescribeTaskDefinition` und `ecs:ListTaskDefinitions` -Berechtigungen zu gewähren.	9. November 2023

Änderung	Beschreibung	Datum
AWSTrustedAdvisorServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Trusted Advisor neue IAM-Aktionen `route53resolver:ListResolverEndpoints` , `route53resolver:ListResolverEndpointIpAddresses` `ec2:DescribeSubnets` , `kafka:ListClustersV2` und `kafka:ListNodes` um neue Resilienzprüfungen zu integrieren, hinzugefügt.	14. September 2023
AWSTrustedAdvisorReportingServiceRolePolicy Version 2 der verwalteten Richtlinie, die der Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` serviceverknüpften Rolle zugeordnet ist	Führen Sie für die Trusted Advisor `AWSServiceRoleForTrustedAdvisorReporting` dienstverknüpfte Rolle ein Upgrade der AWS verwalteten Richtlinie auf Version 2 durch. Mit V2 wird eine weitere IAM-Aktion `organizations:ListDelegatedAdministrators` hinzugefügt	28. Februar 2023
AWSTrustedAdvisorPriorityFullAccess und AWSTrustedAdvisorPriorityReadOnlyAccess Neue AWS verwaltete Richtlinien für Trusted Advisor	Trusted Advisor hat zwei neue verwaltete Richtlinien hinzugefügt, mit denen Sie den Zugriff auf Trusted Advisor Priority steuern können.	17. August 2022

Änderung	Beschreibung	Datum
AWSTrustedAdvisorServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	Trusted Advisor neue Aktionen hinzugefügt, um die `DescribeTargetGroups` und `GetAccountPublicAccessBlock` -Berechtigungen zu gewähren. Diese `DescribeTargetGroup` Berechtigung ist erforderlich, damit die Zustandsprüfung der Auto Scaling-Gruppe nicht-klassische Load Balancer abrufen kann, die an eine Auto Scaling-Gruppe angeschlossen sind. Die `GetAccountPublicAccessBlock` Berechtigung ist erforderlich, damit die Prüfung der Amazon S3 Bucket-Berechtigungen die Einstellungen für öffentlichen Blockzugriff für ein AWS-Konto abrufen kann.	10. August 2021
Änderungsprotokoll veröffentlicht	Trusted Advisor hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	10. August 2021

AWS verwaltete Richtlinien für AWS Support Pläne

AWS Support Plans verfügt über die folgenden verwalteten Richtlinien.

Inhalt

AWS verwaltete Richtlinie: AWSSupportPlansFullAccess

AWS Support Plans verwendet die AWSSupportPlansFullAccess AWS verwaltete Richtlinie. Die IAM-Einheit verwendet diese Richtlinie, um die folgenden Aktionen von Support Plans für Sie durchzuführen:

- Sehen Sie sich Ihren Supportplan für AWS-Konto
- Anzeigen von Details zum Status einer Anforderung zur Änderung Ihres Support-Plans
- Ändern Sie den Supportplan für Ihr AWS-Konto
- Erstellen Sie Supportplanpläne für Ihr AWS-Konto

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

Eine Liste der Änderungen an den Richtlinien finden Sie unter AWS Support Pläne und Aktualisierungen AWS verwalteter Richtlinien.

AWS verwaltete Richtlinie: AWSSupportPlansReadOnlyAccess

AWS Support Plans verwendet die AWSSupportPlansReadOnlyAccess AWS verwaltete Richtlinie. Die IAM-Einheit verwendet diese Richtlinie, um die folgenden schreibgeschützten Aktionen von Support Plans für Sie durchzuführen:

- Sehen Sie sich Ihren Supportplan für AWS-Konto
- Anzeigen von Details zum Status einer Anforderung zur Änderung Ihres Support-Plans

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Eine Liste der Änderungen an den Richtlinien finden Sie unter AWS Support Pläne und Aktualisierungen AWS verwalteter Richtlinien.

AWS Support Pläne und Aktualisierungen AWS verwalteter Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Supportpläne an, seit diese Dienste begonnen haben, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

In der folgenden Tabelle finden Sie wichtige Aktualisierungen für die von Support Plans verwalteten Richtlinien vom 29. September 2022.

AWS Support

Änderung	Beschreibung	Datum
AWSSupportPlansFullAccess – Aktualisierung auf eine bestehende Richtlinie	Der `AWSSupportPlansFullAccess` -verwalteten Richtlinie eine `CreateSupportPlanSchedule` - Aktion hinzufügen.	8. Mai 2023
Änderungsprotokoll veröffentlicht	Änderungsprotokoll für die von Support Plans verwalteten Richtlinien.	29. September 2022

Zugriff auf das AWS Support Center verwalten

Sie müssen über die erforderlichen Berechtigungen verfügen, um auf das Support Center zuzugreifen und einen Supportfall zu erstellen.

Sie können eine der folgenden Optionen verwenden, um auf das Support Center zuzugreifen:

- Verwenden Sie die E-Mail-Adresse und das Passwort, die mit Ihrem AWS Konto verknüpft sind. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet.
- Verwenden Sie AWS Identity and Access Management (IAM).

Wenn Sie einen Business-, Enterprise On-Ramp- oder Enterprise Support-Plan haben, können Sie die AWS Support API auch für den programmgesteuerten Zugriff AWS Support und den Trusted Advisor Betrieb verwenden. Weitere Informationen finden Sie in der AWS Support -API-Referenz.

> **Note**
>
> Wenn Sie sich nicht im Support Center anmelden können, können Sie stattdessen die Seite Kontakt verwenden. Auf dieser Seite erhalten Sie Hilfe bei Fragen zur Rechnungsstellung und zum Konto.

AWS Konto

Sie können sich mit der E-Mail-Adresse AWS Management Console und dem Passwort Ihres AWS Kontos im Support Center anmelden und darauf zugreifen. Diese Identität wird als Root-Benutzer des AWS Kontos bezeichnet. Wir empfehlen jedoch dringend, den root-Benutzer nicht für alltägliche Aufgaben zu verwenden, auch nicht für administrative Aufgaben. Stattdessen empfehlen wir Ihnen die Verwendung von IAM, mit dem Sie steuern können, wer bestimmte Aufgaben in Ihrem Konto ausführen darf.

AWS unterstützende Maßnahmen

Sie können die folgenden AWS Support Aktionen in der Konsole ausführen. Sie können diese AWS Support Aktionen auch in einer IAM-Richtlinie angeben, um bestimmte Aktionen zuzulassen oder abzulehnen.

> **Note**
>
> Wenn Sie eine der folgenden Aktionen in Ihren IAM-Richtlinien ablehnen, kann dies zu unbeabsichtigtem Verhalten im Support-Center führen, wenn Sie einen Support-Fall erstellen oder bearbeiten.

Aktion	Beschreibung
`DescribeSupportLevel`	Gewährt die Berechtigung, die Support-Stufe für eine AWS -Konto-Kennung zurückzugeben Dies wird intern von AWS Support Center verwendet, um Ihr Support-Level zu ermitteln.
`InitiateCallForCase`	Erteilt die Erlaubnis, einen Anruf im AWS Support Center einzuleiten. Dies wird intern von AWS Support Center verwendet, um in Ihrem Namen einen Anruf zu starten.
`InitiateChatForCase`	Gewährt die Berechtigung, einen Chat im AWS Support -Center zu starten. Dies wird intern von AWS Support Center verwendet, um in Ihrem Namen einen Chat zu starten.

Aktion	Beschreibung
`RateCaseCommunication`	Erteilt die Erlaubnis, eine AWS Support Kundenvorgangsmitteilung zu bewerten.
`DescribeCaseAttributes`	Gewährt die Berechtigung, sekundären Services das Lesen von Attributen zu AWS Support -Fällen zu gestatten. Dies wird intern von AWS Support Center verwendet, um Attribute für Ihren Fall zu kennzeichnen.
`DescribeIssueTypes`	Gewährt die Berechtigung, Problemtypen für AWS Support -Fälle zurückzugeben. Dies wird intern von AWS Support Center verwendet , um verfügbare Problemtypen für Ihr Konto abzurufen.
`SearchForCases`	Erteilt die Erlaubnis, eine Liste von AWS Support Fällen zurückzugeben, die den angegebenen Eingaben entspricht. Dies wird intern von AWS Support Center verwendet, um gesuchte Fälle zu finden.
`PutCaseAttributes`	Erteilt die Erlaubnis, sekundären Diensten das Anhängen von Attributen an Anfragen zu AWS Support gestatten. Dies wird intern von AWS Support Center verwendet, um Ihren AWS Support Fällen operative Tags hinzuzufügen.

IAM

Standardmäßig können IAM-Benutzer nicht auf das Support Center zugreifen. Sie können IAM verwenden, um einzelne Benutzer oder Gruppen zu erstellen. Anschließend fügen Sie diesen Entitäten IAM-Richtlinien hinzu, sodass sie berechtigt sind, Aktionen durchzuführen und auf Ressourcen zuzugreifen, z. B. Support Center-Anfragen zu öffnen und die AWS Support API zu verwenden.

Nachdem Sie IAM-Benutzer erstellt haben, können Sie diesen Benutzern individuelle Kennwörter und eine kontospezifische Anmeldeseite zuweisen. Sie können sich dann bei Ihrem AWS Konto anmelden und im Support Center arbeiten. IAM-Benutzer, die AWS Support Zugriff haben, können alle Fälle sehen, die für das Konto erstellt wurden.

Weitere Informationen finden Sie unter AWS Management Console Als IAM-Benutzer anmelden im IAM-Benutzerhandbuch.

Der einfachste Weg, Berechtigungen zu erteilen, besteht darin, die AWS verwaltete Richtlinie AWSSupportAccessdem Benutzer, der Gruppe oder der Rolle zuzuordnen. AWS Support ermöglicht Berechtigungen auf Aktionsebene, um den Zugriff auf bestimmte AWS Support Operationen zu kontrollieren. AWS Support bietet keinen Zugriff auf Ressourcenebene, daher ist das `Resource` Element immer auf eingestellt. * Sie können den Zugriff auf bestimmte Support-Fälle nicht zulassen oder verweigern.

Example : Erlaubt den Zugriff auf alle Aktionen AWS Support

Die AWS verwaltete Richtlinie AWSSupportAccessgewährt einem IAM-Benutzer Zugriff auf AWS Support. Ein IAM-Benutzer mit dieser Richtlinie kann auf alle AWS Support Operationen und Ressourcen zugreifen.

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

Weitere Informationen darüber, wie Sie die `AWSSupportAccess` Richtlinie Ihren Entitäten zuordnen, finden Sie unter Hinzufügen von IAM-Identitätsberechtigungen (Konsole) im IAM-Benutzerhandbuch.

Example : Erlaubt den Zugriff auf alle Aktionen außer der ResolveCase Aktion

Sie können in IAM auch kundenverwaltete Richtlinien erstellen, um festzulegen, welche Aktionen zugelassen oder verweigert werden sollen. Die folgende Richtlinienerklärung ermöglicht es einem IAM-Benutzer, alle Aktionen auszuführen, AWS Support mit Ausnahme der Lösung eines Falls.

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

Weitere Informationen über die Erstellung einer vom Kunden verwalteten IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Wenn der Benutzer oder die Gruppe bereits über eine Richtlinie verfügt, können Sie die AWS Support-spezifische Richtlinienanweisung zu dieser Richtlinie hinzufügen.

> **Important**
>
> - Wenn Sie die Fälle im Support Center nicht sehen können, stellen Sie sicher, dass Sie die erforderlichen Berechtigungen haben. Möglicherweise müssen Sie sich an Ihren IAM-Administrator wenden. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für AWS Support.

Zugriff auf AWS Trusted Advisor

In der AWS Management Console steuert ein separater `trustedadvisor` IAM-Namespace den Zugriff auf. Trusted Advisor In der AWS Support API steuert der `support` IAM-Namespace den Zugriff auf. Trusted Advisor Weitere Informationen finden Sie unter Zugriff verwalten auf AWS Trusted Advisor.

Zugriff auf Pläne verwalten AWS Support

Themen

- Berechtigungen für die Support-Plans-Konsole

- Aktionen für Support-Plans
- Beispiel-IAM-Richtlinien für Support Plans
- Fehlerbehebung

Berechtigungen für die Support-Plans-Konsole

Um auf die Support-Plans-Konsole zugreifen zu können, muss ein Benutzer über einen Mindestsatz an Berechtigungen verfügen. Diese Berechtigungen müssen dem Benutzer das Auflisten und Anzeigen von Details zu den Support-Plans-Ressourcen in Ihrem AWS-Konto ermöglichen.

Sie können eine AWS Identity and Access Management (IAM-) Richtlinie mit dem `supportplans` Namespace erstellen. Sie können diese Richtlinie verwenden, um Berechtigungen für Aktionen und Ressourcen anzugeben.

Wenn Sie eine Richtlinie erstellen, können Sie den Namespace des Dienstes angeben, um eine Aktion zuzulassen oder zu verweigern. Der Namespace für Support-Plans ist `supportplans`.

Sie können AWS verwaltete Richtlinien verwenden und sie an Ihre IAM-Entitäten anhängen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Support Pläne.

Aktionen für Support-Plans

Sie können in der Konsole die folgenden Aktionen für Support Plans durchführen. Sie können diese Support-Plans-Aktionen auch in einer IAM-Richtlinie angeben, um bestimmte Aktionen zuzulassen oder zu verweigern.

Aktion	Beschreibung
`GetSupportPlan`	Gewährt die Berechtigung, Details zum aktuellen Support-Plan für dieses AWS-Konto anzuzeigen.
`GetSupportPlanUpdateStatus`	Gewährt die Berechtigung, Details zum Status einer Anfrage zur Aktualisierung eines Support-Plans anzuzeigen.
`StartSupportPlanUpdate`	Gewährt die Berechtigung zum Starten der Anforderung zum Aktualisieren des Support-P lans für dieses AWS-Konto.

Aktion	Beschreibung
`CreateSupportPlanSchedule`	Gewährt die Berechtigung zur Erstellung von Support-Plan-Zeitplänen für dieses AWS-Konto .

Beispiel-IAM-Richtlinien für Support Plans

Sie können die folgenden Beispielrichtlinien verwenden, um den Zugriff auf Support Plans zu verwalten.

Vollständiger Zugriff auf Support Plans

Die folgende Richtlinie gewährt Benutzern vollständigen Zugriff auf Support Plans.

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

Schreibgeschützter Zugriff auf Support Plans

Die folgende Richtlinie ermöglicht schreibgeschützten Zugriff auf Support Plans.

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

Zugriff auf Support Plans verweigern

Die folgende Richtlinie gewährt Benutzern keinen Zugriff auf Support Plans.

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

Fehlerbehebung

Informationen zum Verwalten des Zugriffs auf Supportpläne finden Sie in den folgenden Themen.

Wenn ich versuche, meinen Supportplan einzusehen oder zu ändern, meldet die Support-Plans-Konsole, dass mir die **`GetSupportPlan`**-Berechtigung fehlt

IAM-Benutzer müssen über die erforderlichen Berechtigungen verfügen, um auf die Support-Plans-Konsole zugreifen zu können. Sie können Ihre IAM-Richtlinie aktualisieren, um die fehlende Berechtigung aufzunehmen oder eine AWS -verwaltete Richtlinie verwenden, z. B. AWSSupportPlansFullAccess oder AWSSupportPlansReadOnlyAccess. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Support Pläne.

Wenn Sie keinen Zugriff zum Aktualisieren Ihrer IAM-Richtlinien haben, wenden Sie sich an Ihren AWS-Konto -Administrator.

Ähnliche Informationen

Weitere Informationen finden Sie unter folgenden Themen im IAM-Benutzerhandbuch:

- Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator
- Fehlerbehebung von Meldungen aufgrund Zugriffsverweigerung

Ich habe die richtigen Support-Plans-Berechtigungen, erhalte aber immer noch dieselbe Fehlermeldung

Wenn Sie AWS-Konto ein Mitgliedskonto sind, zu dem Sie gehören AWS Organizations, muss die Service Control Policy (SCP) möglicherweise aktualisiert werden. SCPs sind eine Art von Richtlinie, die Berechtigungen in einer Organisation verwaltet.

Da es sich bei Support Plans um einen globalen Service handelt, können Richtlinien, die Einschränkungen zu AWS-Regionen enthalten, dazu führen, dass Mitgliedskonten ihren Supportplan nicht einsehen oder ändern können. Um globale Services für Ihr Unternehmen zuzulassen, wie z. B. IAM und Support Plans, müssen Sie den Service zur Ausschlussliste in jedem entsprechenden SCP hinzufügen. Das bedeutet, dass Konten in der Organisation auf diese Dienste zugreifen können, auch wenn der SCP einen bestimmten Dienst verweigert. AWS-Region

Um Support Plans als Ausnahme hinzuzufügen, geben Sie `"supportplans:*"` in der `"NotAction"`-Liste im SCP ein.

```
"supportplans:*",
```

Ihr SCP wird möglicherweise als der folgende Richtlinienausschnitt angezeigt.

Example : SCP, das Support-Plans-Zugriff in einer Organisation ermöglicht

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

Wenn Sie über ein Mitgliedskonto verfügen und das SCP nicht aktualisieren können, wenden Sie sich an Ihren AWS-Konto -Administrator. Möglicherweise muss das Verwaltungskonto das SCP aktualisieren, damit alle Mitgliedskonten auf Support Plans zugreifen können.

Hinweise für AWS Control Tower

- Wenn Ihre Organisation ein SCP mit verwendet AWS Control Tower, können Sie die Einstellung Zugriff verweigern auf AWS basierend auf der angeforderten AWS-Region Kontrolle ändern (allgemein als Regionsverweigerungssteuerung bezeichnet).
- Wenn Sie den SCP AWS Control Tower auf „Zulassen“ aktualisieren`supportplans`, wird Ihr SCP-Update durch das Reparieren der Abweichung entfernt. Weitere Informationen finden Sie unter Drift in erkennen und beheben. AWS Control Tower

Ähnliche Informationen

Weitere Informationen finden Sie unter den folgenden Themen:

- Service Control Policies (SCPs) im AWS Organizations -Benutzerhandbuch.
- Konfigurieren von Region-Deny-Control im AWS Control Tower -Benutzerhandbuch
- Verweigern Sie den Zugriff auf AWS basierend auf den AWS-Region im AWS Control Tower Benutzerhandbuch angeforderten Angaben

Zugriff verwalten auf AWS Trusted Advisor

Sie können von der AWS Trusted Advisor aus darauf zugreifen. AWS Management Console Alle AWS-Konten haben Zugriff auf ausgewählte Trusted Advisor Kernprüfungen. Wenn Sie einen Business-, Enterprise-On-Ramp- oder Enterprise-Supportplan haben, können Sie auf alle Prüfungen zugreifen. Weitere Informationen finden Sie unter AWS Trusted Advisor Referenz überprüfen.

Sie können AWS Identity and Access Management (IAM) verwenden, um den Zugriff auf zu Trusted Advisor kontrollieren.

Themen

- Berechtigungen für die Trusted Advisor Konsole
- Trusted Advisor Aktionen
- Beispiele für IAM-Richtlinien
- Weitere Informationen finden Sie auch unter

Berechtigungen für die Trusted Advisor Konsole

Um auf die Trusted Advisor Konsole zugreifen zu können, muss ein Benutzer über Mindestberechtigungen verfügen. Diese Berechtigungen müssen es dem Benutzer ermöglichen, Informationen zu den Trusted Advisor Ressourcen in Ihrem Verzeichnis aufzulisten und einzusehen AWS-Konto.

Sie können die folgenden Optionen zum Steuern des Zugriffs auf Trusted Advisor verwenden:

- Verwenden Sie die Tag-Filterfunktion der Trusted Advisor Konsole. Der Benutzer oder die Rolle muss über Berechtigungen verfügen, die mit den Tags verknüpft sind.

  Sie können AWS verwaltete oder benutzerdefinierte Richtlinien verwenden, um Berechtigungen anhand von Tags zuzuweisen. Weitere Informationen finden Sie unter Controlling access to and for IAM users and roles using tags (Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Ressourcen-Tags).
- Erstellen Sie eine IAM-Richtlinie mit dem `trustedadvisor`-Namespace. Sie können diese Richtlinie verwenden, um Berechtigungen für Aktionen und Ressourcen anzugeben.

Wenn Sie eine Richtlinie erstellen, können Sie den Namespace des Dienstes angeben, um eine Aktion zuzulassen oder zu verweigern. Der Namespace für Trusted Advisor ist`trustedadvisor`. Sie können den `trustedadvisor` Namespace jedoch nicht verwenden, um Trusted Advisor API-Operationen in der AWS Support API zuzulassen oder abzulehnen. Sie müssen stattdessen den `support`-Namespace für AWS Support verwenden.

> **Note**
>
> Wenn Sie über Berechtigungen für die AWS SupportAPI verfügen, AWS Management Console zeigt das Trusted Advisor Widget in der eine Übersichtsansicht Ihrer Trusted Advisor Ergebnisse. Um Ihre Ergebnisse in der Trusted Advisor Konsole anzeigen zu können, benötigen Sie Berechtigungen für den `trustedadvisor` Namespace.

Trusted Advisor Aktionen

Sie können die folgenden Trusted Advisor Aktionen in der Konsole ausführen. Sie können diese Trusted Advisor Aktionen auch in einer IAM-Richtlinie angeben, um bestimmte Aktionen zuzulassen oder abzulehnen.

Aktion	Beschreibung
`DescribeAccount`	Erteilt die Erlaubnis, den AWS Support Plan und verschiedene Trusted Advisor Einstellungen einzusehen.
`DescribeAccountAccess`	Erlaubt die Anzeige, ob der aktiviert oder deaktiviert AWS-Konto wurde Trusted Advisor.
`DescribeCheckItems`	Erteilt die Berechtigung zum Anzeigen von Details für die Prüfelemente
`DescribeCheckRefreshStatuses`	Erteilt die Erlaubnis, die Aktualisierungsstatus der Trusted Advisor Prüfungen einzusehen.
`DescribeCheckSummaries`	Erteilt die Berechtigung zum Anzeigen von Trusted Advisor Scheckzusammenfassungen.
`DescribeChecks`	Erteilt die Erlaubnis, Details zu Trusted Advisor Schecks einzusehen.
`DescribeNotificationPreferences`	Erteilt die Berechtigung zum Anzeigen der Benachrichtigungseinstellungen für das AWS -Konto.
`ExcludeCheckItems`	Erteilt die Berechtigung zum Ausschließen von Empfehlungen für Trusted Advisor -Prüfungen.
`IncludeCheckItems`	Erteilt die Berechtigung zum Einschließen von Empfehlungen für Trusted Advisor -Prüfungen.
`RefreshCheck`	Erteilt die Erlaubnis, einen Trusted Advisor Scheck zu aktualisieren.
`SetAccountAccess`	Erteilt die Erlaubnis, das Konto zu aktivieren oder zu deaktivieren Trusted Advisor .

Aktion	Beschreibung
`UpdateNotificationPreferences`	Erteilt die Berechtigung zum Aktualisieren der Benachrichtigungseinstellungen für Trusted Advisor.
`DescribeCheckStatusHistoryChanges`	Gewährt die Berechtigung zum Anzeigen von Ergebnissen und geänderten Status für Überprüfungen der letzten 30 Tage.

Trusted Advisor Aktionen für die organisatorische Ansicht

Die folgenden Trusted Advisor Aktionen beziehen sich auf die Funktion „Organisatorische Ansicht“. Weitere Informationen finden Sie unter Organisationsansicht für AWS Trusted Advisor.

Aktion	Beschreibung
`DescribeOrganization`	Erteilt die Berechtigung zur Anzeige, ob die AWS-Konto Anforderungen für die Aktivierung der Funktion „Organisationsansicht“ erfüllt sind.
`DescribeOrganizationAccounts`	Erteilt die Berechtigung zum Anzeigen der verknüpften AWS Konten in der Organisation.
`DescribeReports`	Erteilt die Berechtigung zum Anzeigen von Details für Organisationsansichtsberichte, z. B. Berichtsname, Laufzeit, Erstellungsdatum, Status und Format.
`DescribeServiceMetadata`	Erteilt die Berechtigung zum Anzeigen von Informationen zu Berichten mit organisatorischen Ansichten, wie z. B. Check-Kategorien, Schecknamen und Ressourcenstatus. AWS-Regionen
`GenerateReport`	Erteilt die Berechtigung, einen Bericht für Trusted Advisor Schecks in Ihrer Organisation zu erstellen.

Aktion	Beschreibung
`ListAccountsForParent`	Erteilt die Berechtigung, in der Trusted Advisor Konsole alle Konten einer AWS Organisation anzuzeigen, die zu einem Stamm oder einer Organisationseinheit (OU) gehören.
`ListOrganizationalUnitsForParent`	Erteilt die Berechtigung, in der Trusted Advisor Konsole alle Organisationseinheiten (OUs) einer übergeordneten Organisationseinheit oder einem Stamm anzuzeigen.
`ListRoots`	Erteilt die Berechtigung, in der Trusted Advisor Konsole alle Stammverzeichnisse anzuzeigen, die in einer AWS Organisation definiert sind.
`SetOrganizationAccess`	Erteilt die Berechtigung, die Funktion zur Organisationsansicht für zu aktivieren Trusted Advisor.

Trusted Advisor Vorrangige Aktionen

Wenn Sie Trusted Advisor Priority für Ihr Konto aktiviert haben, können Sie die folgenden Trusted Advisor Aktionen in der Konsole ausführen. Sie können diese Trusted Advisor -Aktionen auch in einer IAM-Richtlinie hinzufügen, um bestimmte Aktionen zuzulassen oder zu verweigern. Weitere Informationen finden Sie unter Beispiel-IAM-Richtlinien für Trusted Advisor -Priorität..

> **Note**
>
> Bei den unter Trusted Advisor Priorität aufgeführten Risiken handelt es sich um Empfehlungen, die Ihr Technical Account Manager (TAM) für Ihr Konto identifiziert hat. Empfehlungen von einem Dienst, z. B. ein Trusted Advisor Scheck, werden automatisch für Sie erstellt. Empfehlungen von Ihrem TAM werden manuell für Sie erstellt. Als Nächstes sendet Ihr TAM diese Empfehlungen, sodass sie in Ihrem Konto als Trusted Advisor Priorität angezeigt werden.

Weitere Informationen finden Sie unter Erste Schritte mit der AWS Trusted Advisor-Priorität.

Aktion	Beschreibung
`DescribeRisks`	Erteilt die Erlaubnis, Risiken mit Trusted Advisor Priorität anzuzeigen.
`DescribeRisk`	Erteilt die Erlaubnis, Risikodetails in Trusted Advisor Priority anzuzeigen.
`DescribeRiskResources`	Gewährt die Berechtigung zum Anzeigen von betroffener Ressourcen für ein Risiko in der Trusted Advisor -Priorität.
`DownloadRisk`	Erteilt die Erlaubnis, eine Datei herunterz uladen, die Details zum Risiko in Trusted Advisor Priority enthält.
`UpdateRiskStatus`	Gewährt die Berechtigung zum Aktualisieren des Risikostatus in der Trusted Advisor -Prioritä t.
`DescribeNotificationConfigu rations`	Erteilt die Erlaubnis, Ihre E-Mail-Benachricht igungseinstellungen für Trusted Advisor Priority abzurufen.
`UpdateNotificationConfigurations`	Gewährt die Berechtigung zum Erstellen oder Aktualisieren Ihrer E-Mail-Benachrichtigungsein stellungen für die Trusted Advisor -Priorität.
`DeleteNotificationConfigura tionForDelegatedAdmin`	Erteilt dem Organisationsverwaltungskonto die Berechtigung, E-Mail-Benachrichtigungsein stellungen aus einem delegierten Administr atorkonto für Trusted Advisor Priority zu löschen.

Trusted Advisor Aktionen einleiten

Wenn Sie Trusted Advisor Engage für Ihr Konto aktiviert haben, können Sie die folgenden Trusted Advisor Aktionen in der Konsole ausführen. Sie können diese Trusted Advisor Aktionen auch zu

einer IAM-Richtlinie hinzufügen, um bestimmte Aktionen zuzulassen oder abzulehnen. Weitere Informationen finden Sie unter Beispiel-IAM-Richtlinien für Trusted Advisor Engage.

Weitere Informationen finden Sie unter Erste Schritte mit AWS Trusted Advisor Engage (Vorschau).

Aktion	Beschreibung
`CreateEngagement`	Erteilt die Erlaubnis, ein Engagement in Trusted Advisor Engage zu erstellen.
`CreateEngagementAttachment`	Erteilt die Erlaubnis, einen Engagement-Anhang in Trusted Advisor Engage zu erstellen.
`CreateEngagementCommunication`	Erteilt die Erlaubnis, eine Interaktionsmitteilung in Trusted Advisor Engage zu erstellen.
`GetEngagement`	Erteilt die Erlaubnis, ein Engagement in Trusted Advisor Engage anzusehen.
`GetEngagementAttachment`	Erteilt die Erlaubnis, einen Verlobungsanhang in Trusted Advisor Engage anzusehen.
`GetEngagementType`	Erteilt die Erlaubnis, einen bestimmten Interaktionstyp in Trusted Advisor Engage anzuzeigen.
`ListEngagementCommunications`	Gewährt die Berechtigung zum Anzeigen aller Mitteilungen für ein Engagement in Trusted Advisor Engage.
`ListEngagements`	Erteilt die Erlaubnis, alle Interaktionen in Trusted Advisor Engage einzusehen.
`ListEngagementTypes`	Erteilt die Erlaubnis, alle Arten von Interaktionen in Trusted Advisor Engage anzuzeigen.
`UpdateEngagement`	Erteilt die Erlaubnis, die Details eines Engagements in Trusted Advisor Engage zu aktualisieren.

Aktion	Beschreibung
`UpdateEngagementStatus`	Erteilt die Erlaubnis, den Status eines Engagements in Trusted Advisor Engage zu aktualisieren.

Beispiele für IAM-Richtlinien

Die folgenden Richtlinien zeigen Ihnen, wie Sie den Zugriff auf Trusted Advisor zulassen und verweigern können. Sie können eine der folgenden Richtlinien verwenden, um eine vom Kunden verwaltete Richtlinie in der IAM-Konsole zu erstellen. Sie können z. B. eine Beispielrichtlinie kopieren und sie dann in die Registerkarte JSON der IAM-Konsole einfügen. Anschließend verknüpfen Sie die Richtlinie mit Ihrem IAM-Benutzer, Ihrer Gruppe oder Ihrer Rolle.

Weitere Informationen über die Erstellung einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Beispiele

- Voller Zugriff auf Trusted Advisor
- Schreibgeschützter Zugriff auf Trusted Advisor
- Verweigern Sie den Zugriff auf Trusted Advisor
- Zulassen und Verweigern bestimmter Aktionen
- Steuern Sie den Zugriff auf die AWS Support API-Operationen für Trusted Advisor
- Beispiel-IAM-Richtlinien für Trusted Advisor -Priorität.
- Beispiel-IAM-Richtlinien für Trusted Advisor Engage

Voller Zugriff auf Trusted Advisor

Die folgende Richtlinie ermöglicht es Benutzern, alle Trusted Advisor Prüfungen in der Trusted Advisor Konsole einzusehen und alle Aktionen auszuführen.

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

```
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

Schreibgeschützter Zugriff auf Trusted Advisor

Die folgende Richtlinie gewährt Benutzern nur Lesezugriff auf die Trusted Advisor Konsole. Benutzer können keine Änderungen vornehmen, bspw. Prüfungen aktualisieren oder Benachrichtigungseinstellungen ändern.

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

Verweigern Sie den Zugriff auf Trusted Advisor

Die folgende Richtlinie erlaubt es Benutzern nicht, Trusted Advisor Schecks in der Trusted Advisor Konsole einzusehen oder Aktionen für diese zu ergreifen.

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

Zulassen und Verweigern bestimmter Aktionen

Mit der folgenden Richtlinie können Benutzer alle Trusted Advisor Schecks in der Trusted Advisor Konsole anzeigen, sie können jedoch keine Schecks aktualisieren.

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

Steuern Sie den Zugriff auf die AWS Support API-Operationen für Trusted Advisor

In der AWS Management Console steuert ein separater `trustedadvisor` IAM-Namespace den Zugriff auf. Trusted Advisor Sie können den `trustedadvisor` Namespace nicht verwenden, um Trusted Advisor API-Operationen in der API zuzulassen oder abzulehnen. AWS Support Verwenden Sie stattdessen den `support`-Namespace. Sie müssen über Berechtigungen für die AWS Support API verfügen, um sie Trusted Advisor programmgesteuert aufrufen zu können.

Wenn Sie den RefreshTrustedAdvisorCheckVorgang beispielsweise aufrufen möchten, müssen Sie in der Richtlinie über Berechtigungen für diese Aktion verfügen.

Example : Nur Trusted Advisor API-Operationen zulassen

Die folgende Richtlinie ermöglicht Benutzern den Zugriff auf die AWS Support API-Operationen für Trusted Advisor, jedoch nicht auf die übrigen AWS Support API-Operationen. Zum Beispiel können die Nutzer die API nutzen, um Prüfungen einzusehen und zu aktualisieren. Sie können keine AWS Support Fälle erstellen, anzeigen, aktualisieren oder lösen.

Sie können diese Richtlinie verwenden, um die Trusted Advisor API-Operationen programmgesteuert aufzurufen, aber Sie können diese Richtlinie nicht verwenden, um Prüfungen in der Trusted Advisor Konsole anzuzeigen oder zu aktualisieren.

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

Weitere Informationen darüber, wie IAM mit AWS Support und Trusted Advisor arbeitet, finden Sie unter. Aktionen

Beispiel-IAM-Richtlinien für Trusted Advisor -Priorität.

Sie können die folgenden AWS verwalteten Richtlinien verwenden, um den Zugriff auf Trusted Advisor Priority zu steuern. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS Trusted Advisor und Erste Schritte mit der AWS Trusted Advisor-Priorität.

Beispiel-IAM-Richtlinien für Trusted Advisor Engage

> **Note**
>
> Trusted Advisor Engage befindet sich in der Vorschauversion und hat derzeit keine AWS verwalteten Richtlinien. Sie können eine der folgenden Richtlinien verwenden, um eine vom Kunden verwaltete Richtlinie in der IAM-Konsole zu erstellen.

Eine Beispielrichtlinie, die Lese- und Schreibzugriff in Trusted Advisor Engage gewährt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

Eine Beispielrichtlinie, die nur Lesezugriff in Trusted Advisor Engage gewährt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Eine Beispielrichtlinie, die Lese- und Schreibzugriff in Trusted Advisor Engage gewährt und die Möglichkeit bietet, vertrauenswürdigen Zugriff zu ermöglichen auf: 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"
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie auch unter

Weitere Informationen zu Trusted Advisor Berechtigungen finden Sie in den folgenden Ressourcen:

- Im IAM-Benutzerhandbuch durch AWS Trusted Advisor definierte Aktionen.
- Steuern des Zugriffs auf die Trusted Advisor -Konsole

Beispiel für Service-Kontrollrichtlinien für AWS Trusted Advisor

AWS Trusted Advisor unterstützt Service Control Policies (SCPs). SCPs sind Richtlinien, die Sie an Elemente in einer Organisation anfügen, um Berechtigungen innerhalb dieser Organisation zu verwalten. Ein SCP gilt für alle AWS Konten unter dem Element, dem Sie den SCP zuordnen. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen aller Konten Ihrer Organisation. Sie können Ihnen dabei helfen, sicherzustellen, dass Ihre AWS Konten die Richtlinien Ihrer Organisation zur Zugriffskontrolle einhalten. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

Themen

- Voraussetzungen
- Beispiel für Service-Kontrollrichtlinien

Voraussetzungen

Um SCPs zu verwenden, müssen Sie Folgendes ausführen:

- Aktivieren aller Funktionen in der Organisation. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.

- Aktivieren Sie SCPs für die Verwendung in Ihrer Organisation. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von Richtlinientypen im AWS Organizations -Benutzerhandbuch.
- Erstellen Sie die SCPs, die Sie benötigen. Weitere Informationen zum Erstellen von SCPs finden Sie im AWS Organizations -Benutzerhandbuch unter So erstellen, aktualisieren und löschen Sie Service-Kontrollrichtlinien.

Beispiel für Service-Kontrollrichtlinien

In den folgenden Beispielen wird veranschaulicht, wie Sie verschiedene Aspekte der Ressourcenfreigabe in einer Organisation steuern können.

Example : Hindern Sie Benutzer daran, Interaktionen in Trusted Advisor Engage zu erstellen oder zu bearbeiten

Die folgende SCP verhindert, dass Benutzer neue Engagements erstellen oder bestehende Engagements bearbeiten.

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

Example : Trusted Advisor Engage und Trusted Advisor Priority Access verweigern

Das folgende SCP verhindert, dass Benutzer auf Engage und Priority zugreifen oder Aktionen innerhalb von Trusted Advisor Engage und Trusted Advisor Priority ausführen.

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

```
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Fehlerbehebung bei AWS Support Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Support IAM auftreten können.

Themen

Ich bin nicht berechtigt, IAM durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Supportübergeben zu können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Support auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte meine Zugriffsschlüssel anzeigen

Nachdem Sie Ihre IAM-Benutzerzugriffsschlüssel erstellt haben, können Sie Ihre Zugriffsschlüssel-ID jederzeit anzeigen. Sie können Ihren geheimen Zugriffsschlüssel jedoch nicht erneut anzeigen. Wenn Sie den geheimen Zugriffsschlüssel verlieren, müssen Sie ein neues Zugriffsschlüsselpaar erstellen.

Zugriffsschlüssel bestehen aus zwei Teilen: einer Zugriffsschlüssel-ID (z. B. `AKIAIOSFODNN7EXAMPLE`) und einem geheimen Zugriffsschlüssel (z. B. `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Ähnlich wie bei Benutzernamen und Passwörtern müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zusammen verwenden, um Ihre Anforderungen zu authentifizieren. Verwalten Sie Ihre Zugriffsschlüssel so sicher wie Ihren Benutzernamen und Ihr Passwort.

> **Important**
>
> Geben Sie Ihre Zugriffsschlüssel nicht an Dritte weiter, auch nicht für die Suche nach Ihrer kanonischen Benutzer-ID. Auf diese Weise können Sie jemandem dauerhaften Zugriff auf Ihre gewähren AWS-Konto.

Während der Erstellung eines Zugriffsschlüsselpaars werden Sie aufgefordert, die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel an einem sicheren Speicherort zu speichern. Der geheime Zugriffsschlüssel ist nur zu dem Zeitpunkt verfügbar, an dem Sie ihn erstellen. Wenn Sie Ihren geheimen Zugriffsschlüssel verlieren, müssen Sie Ihrem IAM-Benutzer neue Zugriffsschlüssel hinzufügen. Sie können maximal zwei Zugriffsschlüssel besitzen. Wenn Sie bereits zwei

Zugriffschlüssel besitzen, müssen Sie ein Schlüsselpaar löschen, bevor Sie ein neues erstellen. Anweisungen hierfür finden Sie unter Verwalten von Zugriffsschlüsseln im IAM-Benutzerhandbuch.

Ich bin Administrator und möchte anderen Zugriff gewähren AWS Support

Um anderen den Zugriff zu ermöglichen AWS Support, müssen Sie eine IAM-Entität (Benutzer oder Rolle) für die Person oder Anwendung erstellen, die Zugriff benötigt. Sie werden die Anmeldeinformationen für diese Einrichtung verwenden, um auf AWS zuzugreifen. Anschließend müssen Sie der Entität eine Richtlinie anfügen, die dieser die korrekten Berechtigungen in AWS Support gewährt.

Informationen zum Einstieg finden Sie unter Erstellen Ihrer ersten delegierten IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Support Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Support unterstützt werden, finden Sie unterWie AWS Support funktioniert mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Vorfallreaktion

Die Reaktion auf Vorfälle für AWS Support ist eine AWS Verantwortung. AWS verfügt über eine formelle, dokumentierte Richtlinie und ein Programm, die die Reaktion auf Vorfälle regeln. Weitere Informationen finden Sie im Whitepaper Introducing the AWS Security Incident Response.

Nutzen Sie die folgenden Optionen, um sich über Probleme beim Betrieb zu informieren:

- Sehen Sie sich AWS betriebliche Probleme mit weitreichenden Auswirkungen auf dem AWS Service Health Dashboard an. Beispielsweise Ereignisse, die sich auf einen Dienst oder eine Region auswirken, der/die nicht spezifisch für Ihr Konto ist.
- Lassen Sie sich Probleme beim Betrieb für einzelne Konten im AWS Health Dashboard anzeigen. Zum Beispiel Ereignisse, die sich auf Dienste oder Ressourcen in Ihrem Konto auswirken. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Health Dashboard im AWS Health - Benutzerhandbuch.

Anmeldung und Überwachung AWS Support und AWS Trusted Advisor

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS Support AWS Trusted Advisor und Ihrer anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AWS Support und melden können AWS Trusted Advisor, wenn etwas nicht stimmt, und gegebenenfalls Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Amazon EventBridge liefert nahezu in Echtzeit einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben. EventBridge ermöglicht automatisiertes ereignisgesteuertes Rechnen, da Sie Regeln schreiben können, die auf bestimmte Ereignisse achten und automatisierte Aktionen in anderen AWS Diensten auslösen können, wenn

diese Ereignisse eintreten. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Aufrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail - Benutzerhandbuch.

Weitere Informationen finden Sie unter Überwachung und Protokollierung für AWS Support und Überwachung und Protokollierung für AWS Trusted Advisor.

Überprüfung der Einhaltung der Vorschriften für AWS Support

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Support

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability

Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS Support

Als verwalteter Service AWS Support ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Support über das Netzwerk. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfiguration und Schwachstellenanalyse in AWS Support

For AWS Trusted Advisor AWS erledigt grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewall-Konfiguration und die Notfallwiederherstellung.

Konfiguration und IT-Steuerung liegen in der gemeinsamen Verantwortung AWS von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Codebeispiele für die AWS Support Verwendung von AWS SDKs

Die folgenden Codebeispiele zeigen, wie die Verwendung AWS Support mit einem AWS Software Development Kit (SDK) funktioniert.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie eine bestimmte Aufgabe ausführen können, indem Sie mehrere Funktionen innerhalb desselben Services aufrufen.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Support mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte

Hallo AWS Support

Die folgenden Codebeispiele veranschaulichen, wie Sie mit der Verwendung von AWS Support beginnen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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.");
    }
}
```

- Einzelheiten zur API finden Sie DescribeServicesin der AWS SDK for .NET API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
        }
    }
}
```

- Einzelheiten zur API finden Sie DescribeServicesin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Rufen Sie „main()“ auf, um das Beispiel auszuführen.

```
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.",
      );
    } else {
      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);
  }
};
```

- Einzelheiten zur API finden Sie DescribeServicesin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/**
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++
            }
        }
    }
}
```

- Einzelheiten zur API finden Sie DescribeServicesin der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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"))
```

- Einzelheiten zur API finden Sie DescribeServicesin AWS SDK for Python (Boto3) API Reference.

Codebeispiele

Aktionen zur Verwendung von SDKs AWS SupportAWS

Die folgenden Codebeispiele zeigen, wie einzelne AWS Support Aktionen mit AWS SDKs ausgeführt werden. Diese Auszüge rufen die AWS Support API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der AWS Support -API-Referenz.

Beispiele

- Verwendung DescribeAttachment mit einem AWS SDK oder CLI
- Verwendung DescribeCases mit einem AWS SDK oder CLI
- Verwendung DescribeCommunications mit einem AWS SDK oder CLI
- Verwendung DescribeServices mit einem AWS SDK oder CLI
- Verwendung DescribeSeverityLevels mit einem AWS SDK oder CLI
- Verwendung DescribeTrustedAdvisorCheckRefreshStatuses mit einem AWS SDK oder CLI
- Verwendung DescribeTrustedAdvisorCheckResult mit einem AWS SDK oder CLI
- Verwendung DescribeTrustedAdvisorCheckSummaries mit einem AWS SDK oder CLI
- Verwendung DescribeTrustedAdvisorChecks mit einem AWS SDK oder CLI
- Verwendung RefreshTrustedAdvisorCheck mit einem AWS SDK oder CLI
- Verwendung ResolveCase mit einem AWS SDK oder CLI

Verwendung **`AddAttachmentsToSet`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`AddAttachmentsToSet`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <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;
    }
```

- Einzelheiten zur API finden Sie AddAttachmentsToSetin der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einem Set einen Anhang hinzuzufügen

Im folgenden `add-attachments-to-set` Beispiel wird einem Set ein Bild hinzugefügt, das Sie dann für einen Support-Fall in Ihrem AWS Konto angeben können.

```
aws support add-attachments-to-set \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

Ausgabe:

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie AddAttachmentsToSetin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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 "";
    }
```

- Einzelheiten zur API finden Sie AddAttachmentsToSetin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie AddAttachmentsToSetin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
    }
}
```

- Einzelheiten zur API finden Sie AddAttachmentsToSetin der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie AddAttachmentsToSetin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **AddCommunicationToCase** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`AddCommunicationToCase`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <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;
    }
```

- Einzelheiten zur API finden Sie AddCommunicationToCasein der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einem Fall eine Kommunikation hinzuzufügen

Im folgenden `add-communication-to-case` Beispiel werden Mitteilungen zu einem Supportfall in Ihrem AWS Konto hinzugefügt.

```
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"
```

Ausgabe:

```
{
    "result": true
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie AddCommunicationToCasein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
       }
   }
```

- Einzelheiten zur API finden Sie AddCommunicationToCasein der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie AddCommunicationToCasein der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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")
        }
    }
}
```

- Einzelheiten zur API finden Sie AddCommunicationToCasein der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Fügt dem angegebenen Fall den Text einer E-Mail-Kommunikation hinzu.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

Beispiel 2: Fügt dem angegebenen Fall den Text einer E-Mail-Nachricht sowie eine oder mehrere E-Mail-Adressen hinzu, die in der CC-Zeile der E-Mail enthalten sind.

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

- Einzelheiten zur API finden Sie unter AddCommunicationToCase AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie AddCommunicationToCasein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CreateCase`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateCase`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <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;
    }
```

- Einzelheiten zur API finden Sie CreateCasein der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einen Fall zu erstellen

Im folgenden `create-case` Beispiel wird ein Support-Fall für Ihr AWS Konto erstellt.

```
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"
```

Ausgabe:

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie CreateCasein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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 "";
    }
```

- Einzelheiten zur API finden Sie CreateCasein der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie CreateCasein der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
    }
}
```

- Einzelheiten zur API finden Sie CreateCasein der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Erstellt einen neuen Fall im AWS Support Center. Werte für die CategoryCode Parameter - ServiceCode und - können mit dem Cmdlet Get-AsaService abgerufen werden. Der Wert für den SeverityCode Parameter - kann mit dem Cmdlet Get-ASA abgerufen werden. SeverityLevel Der Wert des IssueType Parameters - kann entweder „Kundenservice“ oder „technisch“ sein. Bei Erfolg wird die AWS Support-Fallnummer ausgegeben. Standardmäßig wird der Fall auf Englisch behandelt. Um Japanisch zu verwenden, fügen Sie den Parameter -Language „ja“ hinzu. Die CommunicationBody Parameter -ServiceCode, -CategoryCode, -Subject und - sind verpflichtend.

```
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"
```

- Einzelheiten zur API finden Sie unter CreateCase AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie CreateCasein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeAttachment`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeAttachment`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <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;
    }
```

- Einzelheiten zur API finden Sie DescribeAttachmentin der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einen Anhang zu beschreiben

Das folgende `describe-attachment` Beispiel gibt Informationen über den Anhang mit der angegebenen ID zurück.

```
aws support describe-attachment \
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

Ausgabe:

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeAttachmentin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
       }
   }
```

- Einzelheiten zur API finden Sie DescribeAttachmentin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie DescribeAttachmentin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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}")
    }
}
```

- Einzelheiten zur API finden Sie DescribeAttachmentin der API-Referenz zum AWS SDK für Kotlin.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie DescribeAttachmentin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeCases`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeCases`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <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;
    }
```

- Einzelheiten zur API finden Sie DescribeCasesin der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einen Fall zu beschreiben

Das folgende `describe-cases` Beispiel gibt Informationen über den angegebenen Supportfall in Ihrem AWS Konto zurück.

```
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
```

Ausgabe:

```
{
    "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"
        }
    ]
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeCasesin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
       }
   }
```

- Einzelheiten zur API finden Sie DescribeCasesin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie DescribeCasesin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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}")
        }
    }
}
```

- Einzelheiten zur API finden Sie DescribeCasesin der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die Details aller Supportfälle zurück.

```
Get-ASACase
```

Beispiel 2: Gibt die Details aller Supportfälle seit dem angegebenen Datum und der angegebenen Uhrzeit zurück.

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

Beispiel 3: Gibt die Details der ersten 10 Supportfälle zurück, einschließlich derer, die gelöst wurden.

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

Beispiel 4: Gibt die Details des einzelnen angegebenen Supportfalls zurück.

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Beispiel 5: Gibt die Details der angegebenen Supportfälle zurück.

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

Beispiel 6: Gibt alle Supportanfragen mithilfe von manuellem Paging zurück. Die Anfragen werden in Stapeln von 20 abgerufen.

```
$nextToken = $null
do {
  Get-ASACase -NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Einzelheiten zur API finden Sie unter DescribeCases AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie DescribeCasesin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeCommunications`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeCommunications`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <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;
    }
```

- Einzelheiten zur API finden Sie DescribeCommunicationsin der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um die neueste Mitteilung zu einem Fall zu beschreiben

Das folgende `describe-communications` Beispiel gibt die neueste Kommunikation für den angegebenen Supportfall in Ihrem AWS Konto zurück.

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

Ausgabe:

```
{
    "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":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeCommunicationsin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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 "";
   }
```

- Einzelheiten zur API finden Sie DescribeCommunicationsin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie DescribeCommunicationsin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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 ""
}
```

- Einzelheiten zur API finden Sie DescribeCommunicationsin der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die gesamte Kommunikation für den angegebenen Fall zurück.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Beispiel 2: Gibt für den angegebenen Fall alle Mitteilungen seit Mitternacht UTC am 1. Januar 2012 zurück.

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

Beispiel 3: Gibt alle Kommunikationen seit Mitternacht UTC am 1. Januar 2012 für den angegebenen Fall zurück, wobei manuelles Paging verwendet wird. Die Mitteilungen werden in Stapeln von 20 abgerufen.

```
$nextToken = $null
do {
  Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
NextToken $nextToken -MaxResult 20
  $nextToken = $AWSHistory.LastServiceResponse.NextToken
} while ($nextToken -ne $null)
```

- Einzelheiten zur API finden Sie unter DescribeCommunications AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie DescribeCommunicationsin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeServices`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeServices`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <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;
    }
```

- Einzelheiten zur API finden Sie DescribeServicesin der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um AWS Dienste und Servicekategorien aufzulisten

Das folgende `describe-services` Beispiel listet die verfügbaren Dienstkategorien für die Anforderung allgemeiner Informationen auf.

```
aws support describe-services \
    --service-code-list "general-info"
```

Ausgabe:

```
{
    "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"
                }
            ]
        }
    ]
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeServicesin der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   // 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;
    }
```

- Einzelheiten zur API finden Sie DescribeServicesin der AWS SDK for Java 2.x API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// 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
}
```

- Einzelheiten zur API finden Sie DescribeServicesin der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt alle verfügbaren Servicecodes, Namen und Kategorien zurück.

```
Get-ASAService
```

Beispiel 2: Gibt den Namen und die Kategorien für den Dienst mit dem angegebenen Code zurück.

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

Beispiel 3: Gibt den Namen und die Kategorien für die angegebenen Servicecodes zurück.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

Beispiel 4: Gibt den Namen und die Kategorien (auf Japanisch) für die angegebenen Servicecodes zurück. Derzeit werden die Sprachcodes Englisch („en“) und Japanisch („ja“) unterstützt.

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

- Einzelheiten zur API finden Sie unter DescribeServices AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie DescribeServicesin AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeSeverityLevels`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeSeverityLevels`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <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;
   }
```

- Einzelheiten zur API finden Sie unter DescribeSeverityStufen in der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um die verfügbaren Schweregrade aufzulisten

Im folgenden `describe-severity-levels` Beispiel werden die verfügbaren Schweregrade für einen Supportfall aufgeführt.

```
aws support describe-severity-levels
```

Ausgabe:

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

Weitere Informationen finden Sie unter Auswählen eines Schweregrads im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie unter DescribeSeverityStufen in der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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 "";
   }
```

- Einzelheiten zur API finden Sie unter DescribeSeverityStufen in der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie unter DescribeSeverityStufen in der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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-Details finden Sie unter DescribeSeverityLevels in AWS SDK for Kotlin API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die Liste der Schweregrade zurück, die einem AWS Support-Fall zugewiesen werden können.

```
Get-ASASeverityLevel
```

Beispiel 2: Gibt die Liste der Schweregrade zurück, die einem AWS Support-Fall zugewiesen werden können. Die Namen der Stufen werden auf Japanisch zurückgegeben.

```
Get-ASASeverityLevel -Language "ja"
```

- Einzelheiten zur API finden Sie unter DescribeSeverityLevels in AWS Tools for PowerShell Cmdlet Reference.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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-Einzelheiten finden Sie unter DescribeSeverityLevels in AWS SDK for Python (Boto3) API-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **DescribeTrustedAdvisorCheckRefreshStatuses** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeTrustedAdvisorCheckRefreshStatuses`.

CLI

AWS CLI

Um den Aktualisierungsstatus von AWS Trusted Advisor Advisor-Prüfungen aufzulisten

Im folgenden `describe-trusted-advisor-check-refresh-statuses` Beispiel werden die Aktualisierungsstatus für zwei Trusted Advisor Advisor-Prüfungen aufgeführt: Amazon S3 Bucket Permissions und IAM Use.

```
aws support describe-trusted-advisor-check-refresh-statuses \
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

Ausgabe:

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeTrustedAdvisorCheckRefreshStatusesunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt den aktuellen Status der Aktualisierungsanforderungen für die angegebenen Prüfungen zurück. Request-ASA TrustedAdvisorCheckRefresh kann verwendet werden, um anzufordern, dass die Statusinformationen der Prüfungen aktualisiert werden.

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorCheckRefreshStatusesCmdlet-Referenz.AWS Tools for PowerShell

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeTrustedAdvisorCheckResult`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeTrustedAdvisorCheckResult`.

CLI

AWS CLI

Um die Ergebnisse einer AWS Trusted Advisor-Prüfung aufzulisten

Das folgende `describe-trusted-advisor-check-result` Beispiel listet die Ergebnisse der IAM-Nutzungsprüfung auf.

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

Ausgabe:

```
{
```

```
    "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
            }
        ]
    }
}
```

Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorCheckResult in AWS CLI Command Reference.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die Ergebnisse einer Trusted Advisor zurück. Die Liste der verfügbaren Trusted Advisor Advisor-Prüfungen kann mit Get-ASA TrustedAdvisor Checks abgerufen werden. Die Ausgabe enthält den Gesamtstatus der Prüfung, den Zeitstempel, zu dem die Prüfung zuletzt ausgeführt wurde, und die eindeutige Prüf-ID für die jeweilige Prüfung. Um die Ergebnisse auf Japanisch ausgeben zu lassen, fügen Sie den Parameter -Language „ja“ hinzu.

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorCheckResult in AWS Tools for PowerShell Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeTrustedAdvisorCheckSummaries`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeTrustedAdvisorCheckSummaries`.

CLI

AWS CLI

Um die Zusammenfassungen der AWS Trusted Advisor Advisor-Prüfungen aufzulisten

Das folgende `describe-trusted-advisor-check-summaries` Beispiel listet die Ergebnisse von zwei Trusted Advisor Advisor-Prüfungen auf: Amazon S3 Bucket Permissions und IAM Use.

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

Ausgabe:

```
{
    "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
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorCheckZusammenfassungen in der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die neueste Zusammenfassung für die angegebene Trusted Advisor Advisor-Prüfung zurück.

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

Beispiel 2: Gibt die neuesten Zusammenfassungen für die angegebenen Trusted Advisor Advisor-Prüfungen zurück.

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorCheckZusammenfassungen in der AWS Tools for PowerShell Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DescribeTrustedAdvisorChecks`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DescribeTrustedAdvisorChecks`.

CLI

AWS CLI

Um die verfügbaren AWS Trusted Advisor Advisor-Checks aufzulisten

Das folgende `describe-trusted-advisor-checks` Beispiel listet die verfügbaren Trusted Advisor Advisor-Checks in Ihrem AWS Konto auf. Zu diesen Informationen gehören der Name, die ID, die Beschreibung, die Kategorie und die Metadaten des Schecks. Beachten Sie, dass die Ausgabe aus Gründen der Lesbarkeit gekürzt ist.

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

Ausgabe:

```
{
    "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": []
        }
    ]
}
```

Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie DescribeTrustedAdvisorChecksunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt die Sammlung von Trusted Advisor Advisor-Checks zurück. Sie müssen den Sprachparameter angeben, der entweder „en“ für die englische Ausgabe oder „ja“ für die japanische Ausgabe akzeptiert.

```
Get-ASATrustedAdvisorCheck -Language "en"
```

- Einzelheiten zur API finden Sie unter DescribeTrustedAdvisorChecks AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **RefreshTrustedAdvisorCheck** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`RefreshTrustedAdvisorCheck`.

CLI

AWS CLI

So aktualisieren Sie eine AWS Trusted Advisor Advisor-Prüfung

Im folgenden `refresh-trusted-advisor-check` Beispiel wird der Trusted Advisor Advisor-Check für Amazon S3 Bucket Permissions in Ihrem AWS Konto aktualisiert.

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

Ausgabe:

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie RefreshTrustedAdvisorCheckunter AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Fordert eine Aktualisierung für die angegebene Trusted Advisor Advisor-Prüfung an.

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

- Einzelheiten zur API finden Sie unter RefreshTrustedAdvisorCheck AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ResolveCase`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ResolveCase`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Fällen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <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;
```

```
    }
```

- Einzelheiten zur API finden Sie ResolveCasein der AWS SDK for .NET API-Referenz.

CLI

AWS CLI

Um einen Support-Fall zu lösen

Das folgende `resolve-case` Beispiel löst einen Supportfall in Ihrem AWS Konto.

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

Ausgabe:

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

Weitere Informationen finden Sie unter Fallmanagement im AWS Support-Benutzerhandbuch.

- Einzelheiten zur API finden Sie ResolveCasein der AWS CLI Befehlsreferenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   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);
        }
    }
```

- Einzelheiten zur API finden Sie ResolveCasein der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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);
  }
};
```

- Einzelheiten zur API finden Sie ResolveCasein der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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}")
    }
}
```

- Einzelheiten zur API finden Sie ResolveCasein der API-Referenz zum AWS SDK für Kotlin.

PowerShell

Tools für PowerShell

Beispiel 1: Gibt den Anfangsstatus des angegebenen Falls und den aktuellen Status nach Abschluss des Aufrufs zur Lösung des Falls zurück.

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

- Einzelheiten zur API finden Sie unter ResolveCase AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
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
```

- Einzelheiten zur API finden Sie ResolveCasein AWS SDK for Python (Boto3) API Reference.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Verwendung AWS Support mit einem AWS SDK Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für die AWS Support Verwendung von AWS SDKs

Die folgenden Codebeispiele zeigen Ihnen, wie Sie allgemeine Szenarien AWS Support mit AWS SDKs implementieren. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben erledigen können, indem Sie darin mehrere Funktionen aufrufen. AWS Support Jedes Szenario enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Beispiele

- Beginnen Sie mit AWS Support Fällen, in denen Sie ein AWS SDK verwenden

Beginnen Sie mit AWS Support Fällen, in denen Sie ein AWS SDK verwenden

Die folgenden Code-Beispiele veranschaulichen Folgendes:

- Rufen Sie verfügbare Services und Schweregrade für Fälle ab und zeigen Sie sie an.
- Erstellen Sie einen Supportfall mit einem ausgewählten Service, einer ausgewählten Kategorie und einem ausgewählten Schweregrad.
- Rufen Sie eine Liste der offenen Fälle für den aktuellen Tag ab und zeigen Sie sie an.
- Fügen Sie dem neuen Fall einen Anhangssatz und eine Mitteilung hinzu.
- Beschreiben Sie den neuen Anhang und die Mitteilung für den Fall.
- Lösen Sie den Fall.
- Rufen Sie eine Liste der gelösten Fälle für den aktuellen Tag ab und zeigen Sie sie an.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
/// <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));
    }
```

```
}
```

Wrapper-Methoden, die vom Szenario für AWS Support Aktionen verwendet werden.

```
/// <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-Details finden Sie in den folgenden Themen der AWS SDK for .NET -API-Referenz.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityStufen
  - ResolveCase

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie verschiedene AWS Support Operationen aus.

```
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-Details finden Sie in den folgenden Themen der AWS SDK for Java 2.x -API-Referenz.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityStufen
  - ResolveCase

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario im Terminal aus.

```
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.",
      );
    } else {
      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-Details finden Sie in den folgenden Themen der AWS SDK for JavaScript -API-Referenz.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases

- DescribeCommunications
- DescribeServices
- DescribeSeverityStufen
- ResolveCase

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/**
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
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Kotlin.
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityStufen
  - ResolveCase

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
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.")
```

Definieren Sie eine Klasse, die unterstützende Client-Aktionen umschließt.

```
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
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityStufen
  - ResolveCase

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterVerwendung AWS Support mit einem AWS SDK. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Überwachung und Protokollierung für AWS Support

Die Überwachung ist wesentlich zur Wahrung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Support und Ihren anderen AWS-Lösungen. AWS bietet folgende Überwachungswerkzeuge, mit denen Sie AWS Support beobachten, Missstände melden und ggf. automatisch Maßnahmen ergreifen können:

- Amazon EventBridge liefert nahezu in Echtzeit einen Strom von Systemereignissen, die Änderungen in AWS-Ressourcen beschreiben. EventBridge ermöglicht automatisierte, ereignisgesteuerte Datenverarbeitung, indem Sie Regeln schreiben können, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen AWS-Services auslösen, wenn diese Ereignisse auftreten. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon EventBridge.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen

Überwachung von AWS Support Fällen mit Amazon EventBridge

Sie können Amazon verwenden EventBridge , um Änderungen in Ihren AWS Support Fällen zu erkennen und darauf zu reagieren. Ruft dann auf der Grundlage der von Ihnen erstellten Regeln EventBridge eine oder mehrere Zielaktionen auf, wenn ein Ereignis den Werten entspricht, die Sie in einer Regel angeben.

Abhängig vom Ereignis können Sie Benachrichtigungen senden, Ereignisinformationen erfassen, Korrekturmaßnahmen ausführen, Ereignisse auslösen oder anderweitige Aktionen ausführen. Sie können beispielsweise benachrichtigt werden, wenn die folgenden Aktionen in Ihrem Konto auftreten:

- Einen Support-Fall erstellen
- Fügen Sie einem bestehenden Supportfall eine Korrespondenz hinzu
- Lösen eines Support-Falls
- Wiedereröffnen eines Supportfalls

> **Note**
>
> AWS Support liefert Ereignisse nach bestem Bemühen aus. Es ist nicht immer garantiert, dass Ereignisse an EventBridge geliefert werden.

Eine EventBridge-Regel für AWS Support-Fälle erstellen

Sie können eine EventBridge Regel erstellen, um bei Fallereignissen benachrichtigt zu AWS Support werden. Die Regel überwacht Updates für Supportfälle in Ihrem Konto, einschließlich der Aktionen, die Sie, Ihre IAM-Benutzer oder Support-Mitarbeiter ausführen. Führen Sie vor dem Erstellen von Ereignisregeln für AWS Support die folgenden Schritte aus:

- Machen Sie sich mit Ereignissen, Regeln und Zielen in vertraut EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im EventBridgeAmazon-Benutzerhandbuch.
- Erstellen Sie das zu nutzende Ziel für die Ereignisregeln. Sie können zum Beispiel ein Amazon Simple Notification Service (Amazon SNS)-Thema erstellen, damit Sie bei der Aktualisierung eines Supportfalls eine SMS oder E-Mail erhalten. Weitere Informationen finden Sie unter EventBridge Targets (Ziele).

> **Note**
>
> AWS Support ist ein globaler Service. Um Aktualisierungen für Ihre Supportfälle zu erhalten, können Sie eine der folgenden Regionen wählen: Region USA Ost (Nord-Virginia), Region USA West (Oregon) oder Region Europa (Irland).

Um eine EventBridge Regel für Fallereignisse AWS Support zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.

2. Verwenden Sie die Region selector (Regionsauswahl) in der oberen rechten Ecke der Seite und wählen Sie US East (N. Virginia) (USA Ost (Nord-Virginia)), falls Sie das noch nicht getan haben.
3. Wählen Sie im Navigationsbereich Rules aus.
4. Wählen Sie Regel erstellen.
5. Geben Sie auf der Seite Define rule detail (Regeldetail festlegen) einen Namen und eine Beschreibung für Ihre Regel ein.
6. Behalten Sie die Standardwerte für Event Bus und Regeltyp bei und wählen Sie dann Weiter aus.
7. Wählen Sie auf der Seite „Event-Pattern erstellen“ unter Ereignisquelle die Option AWSEreignisse oder EventBridge Partnerereignisse aus.
8. Behalten Sie unter Event pattern (Ereignismuster) den Standardwert für AWS-Services.
9. Wählen Sie für AWS-Service Support (Support) aus.
10. Für Event type (Ereignistyp), wählen Sie Support Case Update (Supportfall-Aktualisierung) aus.
11. Wählen Sie Weiter.
12. Wählen Sie im Abschnitt Select target(s) (Ziel(e) auswählen) das Ziel aus, das Sie für diese Regel erstellt haben, und konfigurieren Sie dann weitere für diesen Typ erforderliche Optionen. Wenn Sie zum Beispiel Amazon SNS wählen, stellen Sie sicher, dass Ihr SNS-Thema korrekt konfiguriert ist, damit Sie per E-Mail oder SMS benachrichtigt werden.
13. Wählen Sie Weiter.
14. (Optional) Fügen Sie auf der Seite Configure tags (Tags konfigurieren) beliebige Tags hinzu und wählen Sie Next (Weiter).
15. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die eingerichteten Regeln, um sicherzustellen, dass sie den Anforderungen Ihrer Ereignisüberwachung entsprechen.
16. Wählen Sie Regel erstellen. Ihre Regel überwacht nun AWS Support-Prüfungen und sendet das Ereignis an das von Ihnen angegebene Ziel.

Hinweise

- Wenn Sie eine Ereignis erhalten, können Sie die `origin`-Parameter nutzen, um festzustellen, ob Sie oder ein AWS Support-Agent einem Supportfall eine Fallkorrespondenz hinzugefügt haben. Der Wert für `origin` kann entweder `CUSTOMER` oder `AWS` sein.

Derzeit werden nur Ereignisse für `AddCommunicationToCase`-Aktionen diesen Wert haben.

- Weitere Informationen zum Erstellen von Ereignismustern finden Sie unter Ereignismuster im EventBridge Amazon-Benutzerhandbuch.
- Sie können auch eine andere Regel für den Ereignistyp AWS API-Aufruf über CloudTrail erstellen. Diese Regel wird AWS CloudTrail-Protokolle für AWS Support-API-Aufrufe in Ihrem Konto überwachen.

Beispielereignisse für AWS Support

Die folgenden Ereignisse werden erstellt, sobald Support-Aktionen in Ihrem Konto auftreten.

Example : Erstellen eines Supportfalls

Das folgende Ereignis wird erstellt, wenn ein Supportfall erstellt wurde.

```
{
    "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 : Aktualisieren eines Supportfalls

Das folgende Ereignis wird erstellt, wenn AWS Support auf einen Supportfall antwortet.

```
{
```

```
    "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 : Lösen eines Supportfalls

Das folgende Ereignis wird erstellt, wenn ein Supportfall gelöst wurde.

```
{
    "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 : Öffnen eines Supportfalls

Das folgende Ereignis wird erstellt, wenn ein Supportfall erneut geöffnet wurde.

```
{
    "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": ""
    }
}
```


Weitere Informationen finden Sie auch unter

Weitere Informationen zur Verwendung EventBridge von finden Sie in den folgenden Ressourcen: AWS Support

- So automatisieren Sie die AWS Support API mit Amazon EventBridge
- AWS SupportBenachrichtigung über Fallaktivitäten aktiviert GitHub

Protokollierung von AWS Support-API-Aufrufen mit AWS CloudTrail

AWS Support ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in AWS Support protokolliert. CloudTrail erfasst alle API-Aufrufe für AWS Support als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Support-Konsole und Code-Aufrufe der AWS Support-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon Simple Storage Service (Amazon S3)-Bucket aktivieren, einschließlich der Ereignisse für AWS Support. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen.

Mit den von CloudTrail erfassten Informationen können Sie die an AWS Support gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen über CloudTrail, einschließlich Konfiguration und Aktivierung, finden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS Support-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Wenn die unterstützte Ereignisaktivität in AWS Support eintritt, wird diese Aktivität in einem CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen im Event history (Ereignisverlauf) aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-API-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Support, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle AWS Support-API-Aktionen werden von CloudTrail protokolliert und sind in der AWS Support-API-Referenz dokumentiert.

Zum Beispiel werden durch Aufrufe der `CreateCase`, `DescribeCases` und `ResolveCase`-Operationen Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Sie können die AWS Support-Protokolldateien aus mehreren AWS-Regionen und AWS-Konten auch in einem einzigen Amazon-S3-Bucket zusammenfassen.

AWS Trusted Advisor-Informationen in der CloudTrail Protokollierung

Trusted Advisor ist ein AWS Support-Dienst, mit dem Sie Ihr AWS-Konto prüfen können, um Kosten zu sparen, die Sicherheit zu verbessern und Ihr Konto zu optimieren.

Alle Trusted Advisor-API-Aktionen werden von CloudTrail protokolliert und sind in der AWS Support-API-Referenz dokumentiert.

Zum Beispiel werden durch Aufrufe der `DescribeTrustedAdvisorCheckRefreshStatuses`, `DescribeTrustedAdvisorCheckResult` und `RefreshTrustedAdvisorCheck`-Operationen Einträge in den CloudTrail-Protokolldateien generiert.

> **Note**
>
> CloudTrail protokolliert auch Trusted Advisor-Konsolenaktionen. Siehe AWS Trusted Advisor Konsolenaktionen protokollieren mit AWS CloudTrail.

Grundlagen zu AWS Support-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen

Quelle dar. Es enthält unter anderem Informationen über die angeforderte Operation, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Operation. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Example : Protokolleintrag für CreateCase

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für den Vorgang CreateCase.


```
{
   "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 : Protokolleintrag für RefreshTrustedAdvisorCheck

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für den Vorgang RefreshTrustedAdvisorCheck.

```
{
    "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"
}
```

Protokollieren der AWS Support-App in Slack-API-Aufrufen mit AWS CloudTrail

Die AWS Support-App in Slack ist mit AWS CloudTrail integriert. CloudTrail stellt eine Aufzeichnung von Aktionen bereit, die von einem Benutzer, einer Rolle oder einem AWS-Service in der AWS Support-App durchgeführt wurden. Um diesen Datensatz zu erstellen, erfasst CloudTrail alle öffentlichen API-Aufrufe für die AWS Support-App als Ereignisse. Zu diesen erfassten Aufrufen gehören Aufrufe aus der AWS Support-App-Konsole und Codeaufrufe der öffentlichen API-Operationen der AWS Support-App. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket aktivieren. Dazu gehören Ereignisse für AWS Support-App. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Sie können die von CloudTrail erfassten Informationen verwenden, um festzustellen, dass die Anfrage an AWS Support-App gestellt wurde. Sie können auch die IP-Adresse erfahren, von der der Aufruf ausging, wer die Anforderung gestellt hat, wann sie gestellt wurde und weitere Details.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS Support-App-Informationen in CloudTrail

Wenn Sie Ihr AWS-Konto erstellen, wird CloudTrail auf dem Konto aktiviert. Wenn in der AWS Support-App eine öffentliche API-Aktivität erfolgt, wird diese Aktivität in einem CloudTrail-Ereignis zusammen mit anderen AWS-Service-Ereignissen im Event history (Ereignisverlauf) aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für die AWS Support-App, einen Trail. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und auf die Daten zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien von mehreren Konten.

CloudTrail protokolliert alle öffentlichen AWS Support-App-Aktionen. Diese Aktionen sind auch in der AWS Support-App in Slack-API-Referenz dokumentiert. Zum Beispiel generieren Aufrufe der Aktionen `CreateSlackChannelConfiguration`, `GetAccountAlias` und `UpdateSlackChannelConfiguration` Einträge in den CloudTrail-Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Grundlagen zu AWS Support-App-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolldateien sind keine geordnete Stack-Ablaufverfolgung der öffentlichen API-Aufrufe. Dies bedeutet, dass die Protokolle nicht in einer bestimmten Reihenfolge angezeigt werden.

Example : Protokollbeispiel für **`CreateSlackChannelConfiguration`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die Operation CreateSlackChannelConfiguration.

```
{
    "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 : Protokollbeispiel für **`ListSlackChannelConfigurations`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für ie Operation ListSlackChannelConfigurations.

```
{
    "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 : Protokollbeispiel für **`GetAccountAlias`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für ie Operation GetAccountAlias.

```
{
    "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"
}
```

Überwachung und Protokollierung für AWS Support Plans

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Support Plans und Ihrer anderen AWS-Lösungen. AWS bietet die folgenden Tools zur Überwachung von Support Plans, zur Meldung von Fehlern und zur Einleitung automatischer Maßnahmen, wenn dies erforderlich ist:

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen

Protokollieren von AWS Support-Plans-API-Aufrufen mit AWS CloudTrail

AWS Support Plans ist in AWS CloudTrail integriert, einem Service, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführt werden. CloudTrail erfasst alle API-Aufrufe für AWS Support Plans als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Support-Plans-Konsole und Codeaufrufe an die AWS Support-Plans-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail-Ereignissen an einen Amazon Simple Storage Service (Amazon S3)-Bucket aktivieren, einschließlich Ereignisse für AWS Support Plans. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen.

Anhand der von CloudTrail erfassten Informationen können Sie die an AWS Support Plans gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und zusätzliche Details bestimmen.

Weitere Informationen über CloudTrail, einschließlich Konfiguration und Aktivierung, finden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS Support-Plans-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Konto für Sie aktiviert. Wenn die unterstützte Ereignisaktivität in AWS Support Plans eintritt, wird diese Aktivität in einem CloudTrail-Ereignis zusammen mit anderen AWS-Service-Ereignissen im Event history (Ereignisverlauf) aufgezeichnet. Sie können die neusten Ereignisse in Ihr -Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-API-Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem Konto, einschließlich Ereignissen für AWS Support Plans, einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle AWS Support-Plans-API-Operationen werden von CloudTrail protokolliert. Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Sie können auch AWS Support-Plans-Protokolldateien von mehreren AWS-Regionen und mehreren Konten in einem einzigen Amazon-S3-Bucket zusammenfassen.

Grundlagen von AWS Support-Plans-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar. Es enthält unter anderem Informationen über die angeforderte Operation, etwaige Anforderungsparameter und das Datum und die Uhrzeit der Operation. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Example : Protokolleintrag für **`GetSupportPlan`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `GetSupportPlan`-Operation.


```
{
    "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 : Protokolleintrag für **`GetSupportPlanUpdateStatus`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `GetSupportPlanUpdateStatus`-Operation.

```
{
    "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 : Protokolleintrag für **`StartSupportPlanUpdate`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `StartSupportPlanUpdate`-Operation.


```
{
    "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 : Protokolleintrag für **`CreateSupportPlanSchedule`**

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `CreateSupportPlanSchedule`-Operation.


```
{
    "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"
}
```

Protokollieren von Änderungen an Ihrem AWS Support Plan

Important

Seit dem 03. August 2022 sind die folgenden Operationen veraltet und werden nicht in Ihren neuen CloudTrail-Protokollen angezeigt. Eine Liste der unterstützten Operationen finden Sie unter Grundlagen von AWS Support-Plans-Protokolldateieinträgen.

- `DescribeSupportLevelSummary` – Diese Aktion erscheint in Ihrem Protokoll, wenn Sie die Seite Support-Pläne öffnen.
- `UpdateProbationAutoCancellation` – Wenn Sie sich für den Entwickler-Support oder den Business-Support anmelden und dann versuchen, innerhalb von 30 Tagen zu kündigen, wird Ihr Plan automatisch zum Ende dieses Zeitraums gekündigt. Diese Aktion wird in Ihrem Protokoll angezeigt, wenn Sie im Banner, das auf der Seite mit den Supportplänen angezeigt wird, Opt-out of automatic cancellation (Automatische Kündigung ablehnen) wählen. Sie werden Ihren Plan für Entwickler-Support oder Business-Support fortsetzen.
- `UpdateSupportLevel` – Diese Aktion wird in Ihrem Protokoll angezeigt, wenn Sie Ihren Support-Plan ändern.

Note

Das `eventSource`-Feld enthält den `support-subscription.amazonaws.com` Namespace für diese Aktionen.

Example : Protokolleintrag für DescribeSupportLevelSummary

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `DescribeSupportLevelSummary`-Aktion.


```
{
  "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 : Protokolleintrag für UpdateProbationAutoCancellation

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `UpdateProbationAutoCancellation`-Aktion.


```
{
  "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 : Protokolleintrag für UpdateSupportLevel

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für die `UpdateSupportLevel`-Aktion zum Wechsel zum Entwickler-Support.


```
{
  "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"
}
```

Überwachung und Protokollierung für AWS Trusted Advisor

Die Überwachung ist wesentlich zur Wahrung der Zuverlässigkeit, Verfügbarkeit und Leistung von Trusted Advisor und Ihren anderen AWS-Lösungen. AWS bietet folgende Überwachungswerkzeuge, mit denen Sie Trusted Advisor beobachten, Missstände melden und ggf. automatisch Maßnahmen ergreifen können:

- Amazon EventBridge liefert nahezu in Echtzeit einen Strom von Systemereignissen, die Änderungen in AWS-Ressourcen beschreiben. EventBridge ermöglicht automatisierte, ereignisgesteuerte Datenverarbeitung, da Sie Regeln schreiben können, die bestimmte Ereignisse überwachen und automatisierte Aktionen in anderen AWS-Services auslösen, wenn diese Ereignisse auftreten.

  Zum Beispiel Trusted Advisor bietet die Prüfung der Amazon S3 Bucket-Berechtigungen. Diese Prüfung identifiziert, ob Sie Buckets haben, die über Open-Access-Berechtigungen verfügen oder einen authentifizierten AWS-Benutzer Zugriff gewähren. Wenn sich eine Bucket-Genehmigung ändert, ändert sich der Status der Trusted Advisor Prüfung. EventBridge erkennt dieses Ereignis und sendet Ihnen dann eine Benachrichtigung, so dass Sie Maßnahmen ergreifen können. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon EventBridge.
- AWS Trusted Advisor prüft, wie Sie die Kosten senken, die Leistung steigern und die Sicherheit Ihres AWS-Kontos verbessern können. Sie können den Status der Trusted Advisor-Prüfungen mit EventBridge überwachen. Anschließend können Sie mit Amazon CloudWatch Alarme für Trusted Advisor-Metriken erstellen. Diese Alarme benachrichtigen Sie, wenn sich der Status für eine Trusted Advisor-Prüfung ändert, z. B. eine aktualisierte Ressource oder ein erreichtes Service-Kontingent.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen

AWS Trusted AdvisorPrüfergebnisse mit Amazon überwachen EventBridge

Sie können sie verwenden EventBridge , um zu erkennen, wann sich der Status Ihrer Schecks Trusted Advisor ändert. Ruft dann auf der Grundlage der von Ihnen erstellten Regeln eine oder EventBridge mehrere Zielaktionen auf, wenn sich der Status auf einen Wert ändert, den Sie in einer Regel angeben.

Abhängig von der Art der Statusänderung können Sie Benachrichtigungen versenden, Statusinformationen erfassen, Korrekturmaßnahmen ausführen, Ereignisse auslösen oder anderweitige Aktionen ausführen. Sie können beispielsweise die folgenden Zieltypen angeben, wenn eine Prüfung den Status von „Keine Probleme erkannt“ (grün) in „empfohlene Aktion“ (rot) ändert.

- Verwenden Sie eine AWS Lambda-Funktion, um eine Benachrichtigung an einen Slack-Channel zu senden.
- Übertragen Sie Daten von Prüfungen an einen Amazon-Kinesis-Stream, um eine umfassende Echtzeit-Statusüberwachung zu unterstützen.
- Senden Sie ein Thema von Amazon Simple Notification Service an Ihre E-Mail.
- Lassen Sie sich mit einer CloudWatch Amazon-Alarmaktion benachrichtigen.

Weitere Informationen zur Verwendung EventBridge von Lambda-Funktionen zur Automatisierung von Antworten für finden Sie Trusted Advisor unter Trusted AdvisorTools unter GitHub.

> **Hinweise**
>
> - Trusted Advisor liefert Ereignisse nach bestem Bemühen aus. Es ist nicht immer garantiert, dass Ereignisse an EventBridge geliefert werden.
> - Sie müssen über einen Business-, Enterprise-On-Ramp- oder Enterprise-AWS Support-Plan verfügen, um eine Regel für Trusted Advisor-Prüfungen zu erstellen. Weitere Informationen finden Sie unter AWS Support Pläne ändern.
> - Da Trusted Advisor es sich um einen globalen Service handelt, werden alle Ereignisse EventBridge in die Region USA Ost (Nord-Virginia) gesendet.

Gehen Sie wie folgt vor, um eine EventBridge Regel für zu erstellenTrusted Advisor. Führen Sie vor dem Erstellen von Ereignisregeln die folgenden Schritte aus:

- Machen Sie sich mit Ereignissen, Regeln und Zielen in vertraut EventBridge. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch.
- Erstellen Sie das Ziel, das Sie für die Ereignisregeln nutzen möchten.

Um eine EventBridge Regel zu erstellen für Trusted Advisor

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Um die Region zu ändern, verwenden Sie die Region selector (Regionsauswahl) in der oberen rechten Ecke der Seite und wählen Sie US East (N. Virginia) (USA Ost (Nord-Virginia)).
3. Wählen Sie im Navigationsbereich Rules aus.
4. Wählen Sie Regel erstellen.
5. Geben Sie auf der Seite Define rule detail (Regeldetail festlegen) einen Namen und eine Beschreibung für Ihre Regel ein.
6. Behalten Sie die Standardwerte für Event Bus und Regeltyp bei und wählen Sie dann Weiter aus.
7. Wählen Sie auf der Seite „Event-Pattern erstellen“ unter Ereignisquelle die Option AWSEreignisse oder EventBridge Partnerereignisse aus.
8. Behalten Sie unter Event pattern (Ereignismuster) den Standardwert für AWS-Services.
9. Wählen Sie für AWS-Service Trusted Advisor aus.
10. Für Event type (Ereignistyp), wählen Sie Check Item Refresh Status (Aktualisierungsstatus des Artikels prüfen) aus.
11. Wählen Sie für die Prüfstatus eine der folgenden Optionen aus:
    - Wählen Sie Any status (Jeder Status) um eine Regel zu erstellen, die auf jegliche Statusänderung überwacht.
    - Klicken Sie auf Specific status(es) (Spezifische Status) und wählen Sie die Werte aus, die Ihre Regel überwachen soll.
      - ERROR (Fehler) – Trusted Advisor empfiehlt eine Maßnahme für die Prüfung.
      - INFO – Trusted Advisor kann den Status der Prüfung nicht feststellen.
      - OK – Trusted Advisor stellt keine Probleme bei der Prüfung fest.
      - WARN (Warnung) – Trusted Advisor stellt ein mögliches Problem bei der Prüfung fest und empfiehlt eine Untersuchung.
12. Wählen Sie für die Prüfstatus eine der folgenden Optionen aus:

- Wählen Sie Any check (beliebige Prüfung) aus.
- Wählen Sie Specific check(s) (Spezifische Prüfung/en), und wählen Sie einen oder mehrere Prüfnamen aus der Liste aus.

13. Wählen Sie eine der folgenden Optionen für AWS-Ressourcen aus:

    - Wählen Sie Any resource ID (Beliebige Ressourcen-ID), um eine Regel zu erstellen, die alle Ressourcen überwacht.
    - Wählen Sie Specific resource ID(s) by ARN (Bestimmte Ressourcen-ID/s nach ARN), und geben Sie die gewünschten Amazon-Ressourcennamen (ARNs) ein.

14. Wählen Sie Weiter.
15. Wählen Sie in der Liste Select target(s) (Ziel(e) auswählen) den Zieltyp aus, den Sie für die Verwendung mit dieser Regel erstellt haben, und konfigurieren Sie dann weitere für diesen Typ erforderliche Optionen. Beispielsweise können Sie das Ereignis an eine Amazon-SQS-Warteschlange oder ein Amazon-SNS-Thema senden.
16. Wählen Sie Weiter.
17. (Optional) Fügen Sie auf der Seite Configure tags (Tags konfigurieren) beliebige Tags hinzu und wählen Sie Next (Weiter).
18. Überprüfen Sie auf der Seite Review and create (Überprüfen und erstellen) die eingerichteten Regeln, um sicherzustellen, dass sie den Anforderungen Ihrer Ereignisüberwachung entsprechen.
19. Wählen Sie Regel erstellen. Ihre Regel überwacht nun Trusted Advisor-Prüfungen und sendet das Ereignis an das von Ihnen angegebene Ziel.

Erstellen von Amazon CloudWatch-Alarmen zur Überwachung von AWS Trusted Advisor-Metriken

Wenn AWS Trusted Advisor Ihre Prüfungen aktualisiert, veröffentlicht Trusted Advisor Metriken über Ihre Prüfungsergebnisse in CloudWatch. Sie können die Metriken in CloudWatch anzeigen. Sie können auch Alarme erstellen, um Statusänderungen bei Trusted Advisor-Prüfungen und Statusänderungen für Ressourcen und die Nutzung von Servicekontingenten (früher als Limits bezeichnet) zu erkennen. So können Sie beispielsweise einen Alarm erstellen, um Statusänderungen für Prüfungen in der Kategorie Service Limits zu verfolgen. Der Alarm benachrichtigt Sie dann, wenn Sie ein Dienstleistungskontingent für Ihr AWS-Konto erreichen oder überschreiten.

Folgen Sie diesem Verfahren, um einen CloudWatch-Alarm für eine bestimmte Trusted Advisor-Metrik zu erstellen.

Themen

Voraussetzungen

Bevor Sie CloudWatch-Alarme für Trusted Advisor-Metriken erstellen, lesen Sie die folgenden Informationen:

- Verstehen, wie CloudWatch Metriken und Alarme verwendet. Weitere Informationen finden Sie unter Funktionsweise von CloudWatch im Amazon CloudWatch Benutzerhandbuch.
- Verwenden Sie die Trusted Advisor-Konsole oder die AWS Support-API, um Ihre Prüfungen zu aktualisieren und die neuesten Prüfergebnisse zu erhalten. Weitere Informationen finden Sie unter Ergebnisse der Prüfung aktualisieren.

So erstellen Sie einen CloudWatch-Alarm für Trusted Advisor-Metriken

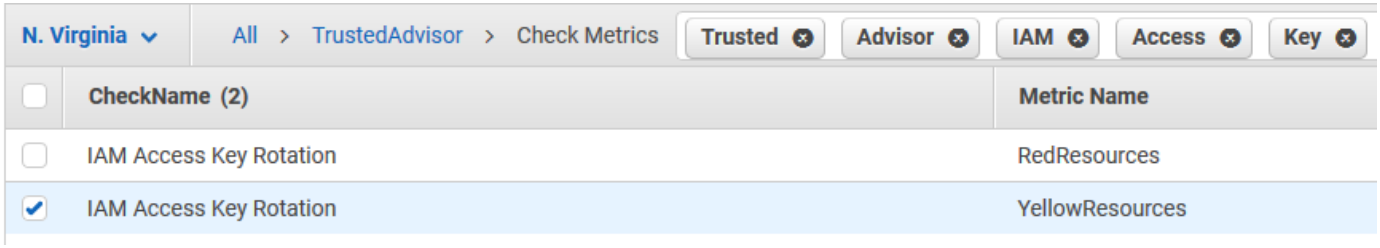
1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Verwenden Sie die Regionenauswahl und wählen Sie die AWS-Region US East (N. Virginia).
3. Klicken Sie im Navigationsbereich auf Alarms (Alarme).
4. Wählen Sie Create alarm (Alarm erstellen) aus.
5. Wählen Sie Select metric (Metrik auswählen) aus.
6. Geben Sie für Metriken einen oder mehrere Dimensionswerte ein, um die Liste der Metriken zu filtern. Sie können z. B. den Metriknamen ServiceLimitUsage oder die Dimension, z. B. den Namen der Trusted Advisor-Prüfung, eingeben.

> **Tip**
>
> - Sie können nach **`Trusted Advisor`** suchen, um alle Metriken für den Dienst aufzulisten.

- Eine Liste der Metrik- und Dimensionsnamen finden Sie unter Trusted Advisor-Metriken und -Dimensionen.

7. Aktivieren Sie in der Ergebnistabelle das Kontrollkästchen für die Metrik.

   Im folgenden Beispiel lautet der Name der Prüfung IAM Access Key Rotation und der Name der Metrik YellowResources.



8. Wählen Sie Select metric (Metrik auswählen) aus.
9. Vergewissern Sie sich auf der Seite Metrik und Bedingungen angeben, dass der Name der Metrik und der Name der Prüfung, die Sie ausgewählt haben, auf der Seite erscheinen.
10. Unter Zeitraum können Sie den Zeitraum angeben, in dem der Alarm ausgelöst werden soll, wenn sich der Status der Prüfung ändert, z. B. 5 Minuten.
11. Wählen Sie unter Bedingungen die Option Statisch, und geben Sie dann die Alarmbedingung an, unter der der Alarm ausgelöst werden soll.

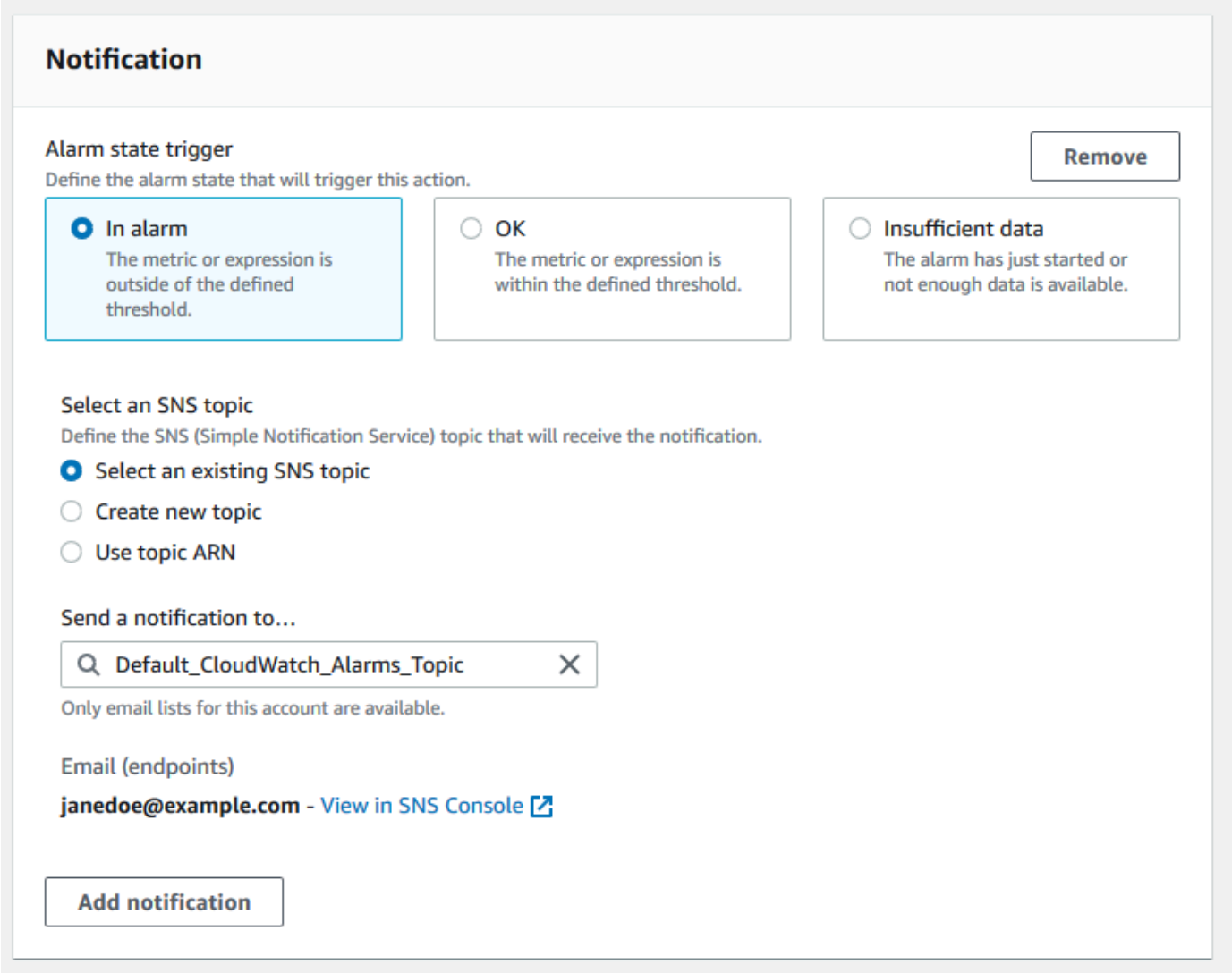
    Wenn Sie beispielsweise Größer/Gleich >= Schwellenwert wählen und **1** für den Schwellenwert eingeben, bedeutet dies, dass der Alarm ausgelöst wird, wenn Trusted Advisor mindestens ein IAM-Zugangsschlüssel entdeckt, der in den letzten 90 Tagen nicht gedreht wurde.

   Hinweise

   - Für die Metriken GreenChecks, RedChecks, YellowChecks, RedResources, und YellowResources kann dieser von Ihnen angegebene Schwellenwert jede beliebige Ganzzahl sein, die größer oder gleich Null ist.
   - Trusted Advisor sendet keine Metriken für GreenResources, d. h. Ressourcen, für die Trusted Advisor keine Probleme festgestellt hat.

12. Wählen Sie Next (Weiter).
13. Wählen Sie auf der Seite Aktionen konfigurieren für Alarmzustandsauslöser die Option In Alarm.

14. Wählen Sie für Ein SNS-Thema auswählen ein bestehendes Amazon Simple Notification Service (Amazon SNS)-Thema oder erstellen Sie eines.



15. Wählen Sie Next (Weiter).
16. Geben Sie unter Name und Beschreibung einen Namen und eine Beschreibung für Ihren Alarm ein.
17. Wählen Sie Next (Weiter).
18. Prüfen Sie auf der Seite Vorschau und Erstellen die Details Ihres Alarms und wählen Sie dann Alarm erstellen.

    Wenn der Status für die Prüfung der IAM-Zugangsschlüsselrotation 5 Minuten lang auf Rot wechselt, sendet Ihr Alarm eine Benachrichtigung an Ihr SNS-Thema.

Example : E-Mail-Benachrichtigung für einen CloudWatch-Alarm

Die folgende E-Mail-Nachricht zeigt an, dass ein Alarm eine Änderung bei der Prüfung der IAM-Zugangsschlüsselrotation festgestellt hat.

```
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:
```

CloudWatch-Metriken für Trusted Advisor

Sie können die CloudWatch-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden, um die Metriken zu finden, die für Trusted Advisor verfügbar sind.

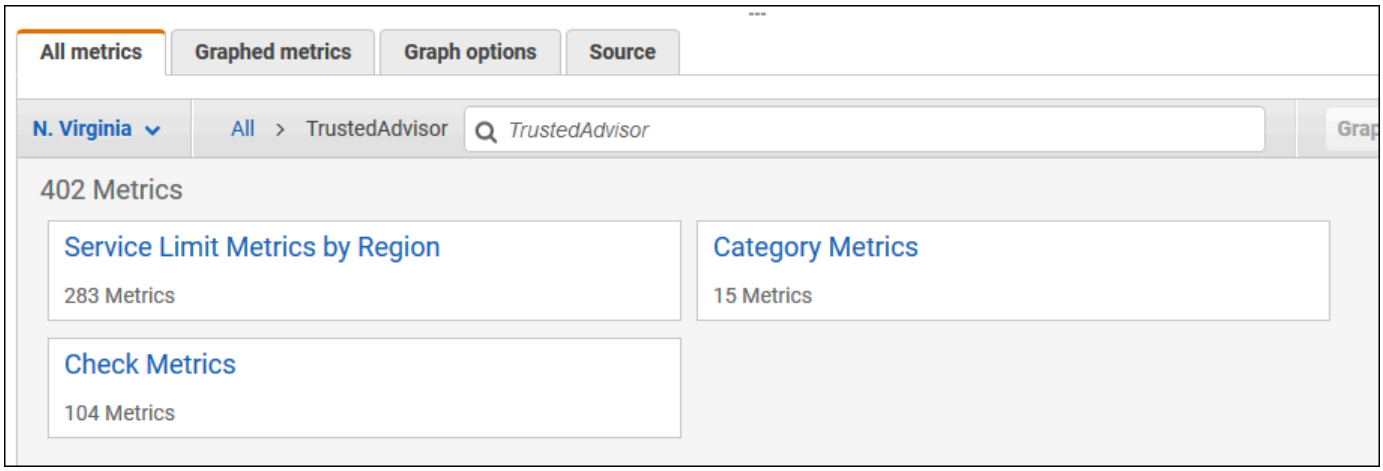
Eine Liste der Namespaces, Metriken und Dimensionen für alle Services, die Metriken veröffentlichen, finden Sie unter AWS Services, die CloudWatch-Metriken veröffentlichen im Amazon CloudWatch-Benutzerhandbuch.

Trusted Advisor-Metriken anzeigen (Konsole)

Sie können sich bei der CloudWatch-Konsole anmelden und die verfügbaren Metriken für Trusted Advisor anzeigen.

So zeigen Sie die verfügbaren Trusted Advisor-Metriken an (Konsole)

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Verwenden Sie die Regionenauswahl und wählen Sie die AWS-Region US East (N. Virginia).
3. Wählen Sie im Navigationsbereich Metriken aus.
4. Geben Sie einen metrischen Namespace ein, z. B. **`TrustedAdvisor`**.
5. Wählen Sie eine metrische Dimension, z. B. Metriken prüfen.



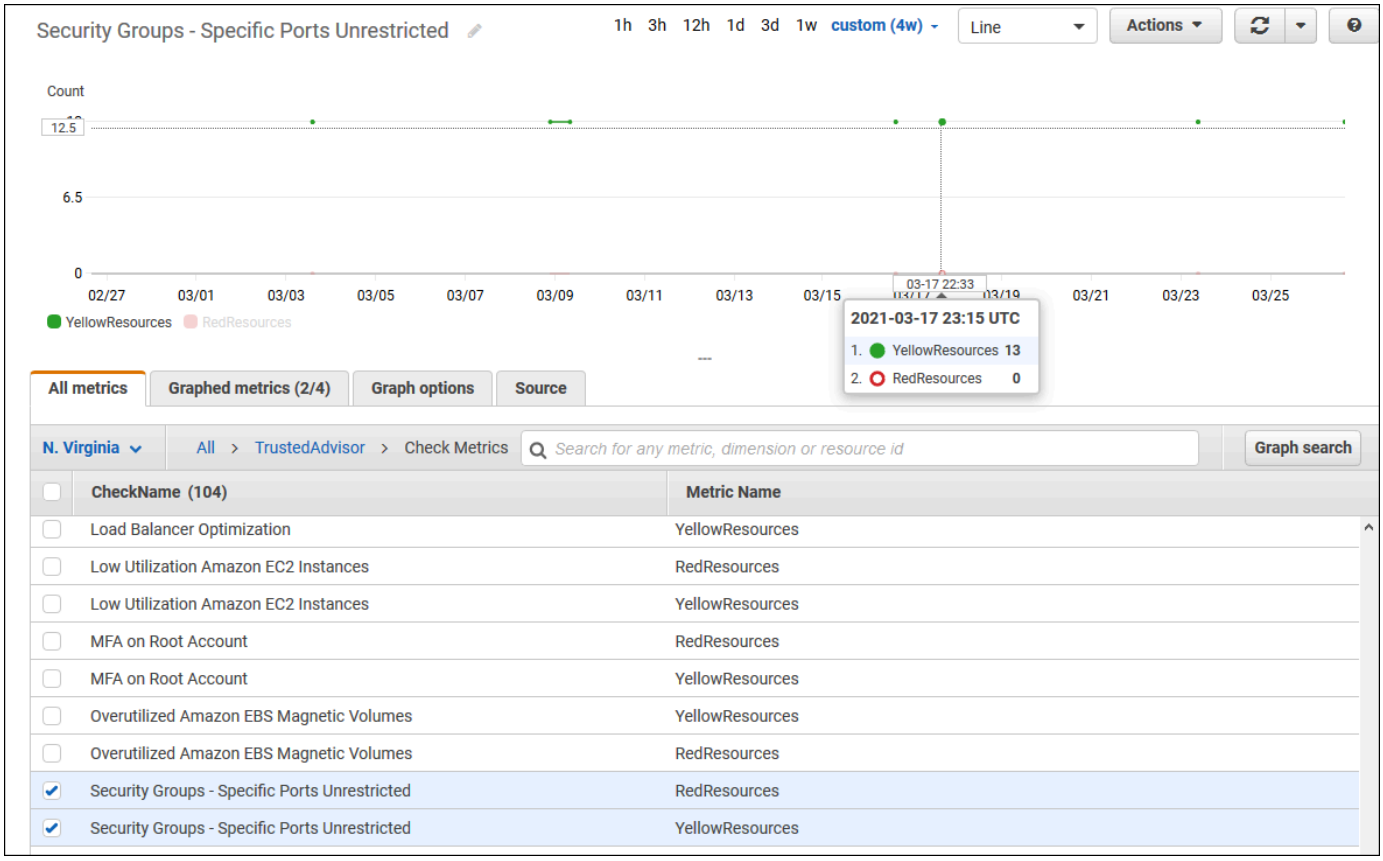
6. Die Registerkarte All metrics zeigt Metriken für diese Dimension im Namespace an. Sie haben die folgenden Möglichkeiten:

a. Um die Tabelle sortieren, wählen Sie die Spaltenüberschrift.

b. Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren. Um alle Metriken auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Tabelle.

c. Um nach Metrik zu filtern, müssen Sie den Metriknamen und anschließend Add to search (Zu Suche hinzufügen) wählen.

Das folgende Beispiel zeigt die Ergebnisse der Prüfung Sicherheitsgruppen - bestimmte Ports unbeschränkt. Die Prüfung identifiziert 13 Ressourcen, die gelb sind. Trusted Advisor empfiehlt, dass Sie Prüfungen, die gelb sind, untersuchen.



7. (Optional) Um dieses Diagramm zu einem CloudWatch-Dashboard hinzuzufügen, wählen Sie Aktionen und dann Zu Dashboard hinzufügen.

Weitere Informationen zur Erstellung eines Diagramms zur Anzeige Ihrer Metriken finden Sie unter Graphische Darstellung einer Metrik im Amazon CloudWatch-Benutzerhandbuch.

Trusted Advisor-Metriken anzeigen (CLI)

Sie können den AWS CLI-Befehl list-metrics verwenden, um die verfügbaren Metriken für Trusted Advisor anzuzeigen.

Example : Alle Metriken fürTrusted Advisor auflisten

Im folgenden Beispiel wird der `AWS/TrustedAdvisor`-Namespace angegeben, um alle Metriken für Trusted Advisor anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

Ihre Ausgabe könnte wie folgt aussehen.

```
{
    "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 : Auflistung aller Metriken für eine Dimension

Im folgenden Beispiel werden der `AWS/TrustedAdvisor` Namespace und die `Region`-Dimension angegeben, um die für die angegebene AWS-Region verfügbaren Metriken anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

Ihre Ausgabe könnte wie folgt aussehen.

```
{
    "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 : Auflisten der Metriken für einen bestimmten Metriknamen

Das folgende Beispiel gibt den `AWS/TrustedAdvisor`-Namespace und den `RedResources` Namen der Metrik an, um die Ergebnisse nur für diese spezifische Metrik anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

Ihre Ausgabe könnte wie folgt aussehen.

```
{
    "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-Metriken und -Dimensionen

In den folgenden Tabellen finden Sie die Trusted Advisor Metriken und Dimensionen, die Sie für Ihre CloudWatch Alarme und Diagramme verwenden können.

Trusted Advisor-Metriken Prüfungsebene

Sie können die folgenden Metriken für Trusted Advisor-Prüfungen verwenden.

Metrik	Beschreibung
`RedResources`	Die Anzahl der Ressourcen, die sich in einem roten Zustand befinden (Aktion empfohlen).
`YellowResources`	Die Anzahl der Ressourcen, die sich in einem gelben Zustand befinden (Untersuchung empfohlen).

Trusted Advisor-Metriken auf Kategorieebene

Sie können die folgenden Metriken für Trusted Advisor-Kategorien.

Metrik	Beschreibung
`GreenChecks`	Die Anzahl der Trusted Advisor-Prüfungen, die im grünen Bereich sind (keine Probleme festgestellt).
`RedChecks`	Die Anzahl der Trusted Advisor-Prüfungen, die sich im roten Bereich befinden (empfohlene Maßnahme).
`YellowChecks`	Die Anzahl der Trusted Advisor-Prüfungen, die sich im gelben Status befinden (Untersuchung empfohlen).

Trusted Advisor-Metriken auf Service-Kontingentenebene

Sie können die folgenden Metriken für AWS-Service-Quotas verwenden.

Metrik	Beschreibung
`ServiceLimitUsage`	Der Prozentsatz der Ressourcennutzung im Vergleich zu einem Servicekontingent (früher als Limits bezeichnet).

Dimensionen von Metriken auf Prüfungsebene

Sie können die folgende Dimension für Trusted Advisor-Prüfungen verwenden.

Dimension	Beschreibung
`CheckName`	Die Bezeichnung der Trusted Advisor-Prüfung. Sie finden alle Namen der Prüfungen in der Trusted Advisor Konsole oder im AWS Trusted Advisor Referenz überprüfen.

Dimensionen von Metriken auf Kategorieebene

Sie können die folgende Dimension für Trusted Advisor-Prüfungskategorien verwenden.

Dimension	Beschreibung
`Category`	Der Name einer Trusted Advisor-Prüfungskategorie. Sie können alle Prüfungskategorien in der Trusted Advisor-Konsole oder auf der Ansicht der Prüfungskategorien-Seite finden.

Dimensionen für Servicekontingent-Metriken

Sie können die folgenden Dimensionen für Trusted Advisor Servicekontingent-Metriken verwenden.

Dimension	Beschreibung
`Region`	Die AWS-Region für eine Service Quota.
`ServiceName`	Der Name der AWS-Service.
`ServiceLimit`	Der Name des Dienstkontingents. Weitere Informationen zu Service Quotas finden Sie unter AWS-Service-Kontingente im Allgemeine AWS-Referenz.

AWS Trusted Advisor Konsolenaktionen protokollieren mit AWS CloudTrail

Trusted Advisor ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die ein Benutzer, eine Rolle oder ein AWS Dienst in ausgeführt hat Trusted Advisor. CloudTrail erfasst Aktionen Trusted Advisor als Ereignisse. Zu den erfassten Anrufen gehören auch Anrufe von der Trusted Advisor Konsole. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren, einschließlich Ereignissen für Trusted Advisor. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde Trusted Advisor, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen darüber CloudTrail, einschließlich der Konfiguration und Aktivierung, finden Sie im AWS CloudTrail Benutzerhandbuch.

Trusted Advisor Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten in der Trusted Advisor Konsole auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für Trusted Advisor, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Überblick über das Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Trusted Advisor unterstützt die Protokollierung einer Teilmenge der Trusted Advisor Konsolenaktionen als Ereignisse in CloudTrail Protokolldateien. CloudTrail protokolliert die folgenden Aktionen:

- 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

Eine vollständige Liste der Trusted Advisor Konsolenaktionen finden Sie unterTrusted Advisor Aktionen.

> **Note**
>
> CloudTrail protokolliert auch die Trusted Advisor API-Operationen in der AWS Support API-Referenz. Weitere Informationen finden Sie unter Protokollierung von AWS Support-API-Aufrufen mit AWS CloudTrail.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Beispiel: Trusted Advisor Einträge in Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Example : Protokolleintrag für RefreshCheck

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `RefreshCheck` Aktion für den Amazon S3 Bucket Versioning Check (IDR365s2Qddf) demonstriert.

```
{
        "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 : Protokolleintrag für UpdateNotificationPreferences

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateNotificationPreferences` Aktion demonstriert.

```
{
        "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 : Protokolleintrag für GenerateReport

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `GenerateReport` Aktion demonstriert. Mit dieser Aktion wird ein Bericht für Ihre AWS -Organisation erstellt.

```
{
        "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"
        }
```

Ressourcen zur Fehlerbehebung

Antworten auf häufig gestellte Fragen zur Fehlersuche finden Sie im AWS Support Knowledge Center.

Für Windows bietet Amazon EC2 EC2 EC2Rescue an, mit dem Kunden ihre Windows-Instances überprüfen können, um häufige Probleme zu identifizieren, Protokolldateien AWS Support zu sammeln und bei der Behebung Ihrer Probleme zu helfen. Sie können auch EC2Rescue verwenden, um Startvolumes über nicht funktionale Instances zu analysieren. Weitere Informationen finden Sie unter How can I troubleshoot issues with my EC2 Windows instance by using the EC2Rescue tool?

Servicespezifische Fehlersuche

Die meisten AWS-Service Dokumentationen enthalten Themen zur Fehlerbehebung, die Ihnen den Einstieg erleichtern können, bevor Sie sich an wenden AWS Support. Die folgende Tabelle enthält Links zu Fehlersuchthemen, geordnet nach Service.

> **Note**
>
> Die folgende Tabelle enthält eine Liste der am häufigsten verwendeten Services. Verwenden Sie das Suchtextfeld auf der AWS -Dokumentations-Landingpage, um nach anderen Themen zur Problembehandlung zu suchen.

Service	Link
Amazon Web Services	Fehlerbehebung bei Fehlern mit AWS Signature Version 4
Amazon API Gateway	Fehlerbehebung bei Problemen mit HTTP-APIs
Amazon AppStream	Fehlerbehebung bei Amazon AppStream
Amazon Athena	Fehlerbehebung in Athena
Amazon Aurora MySQL	Fehlerbehebung für Amazon Aurora
Amazon Aurora PostgreSQL	Fehlerbehebung für Amazon Aurora

Service	Link
Amazon EC2 Auto Scaling	Fehlersuche bei Auto Scaling
AWS Certificate Manager (ACM)	Fehlersuche
AWS CloudFormation	Fehlerbehebung für AWS CloudFormation
Amazon CloudFront	Fehlerbehebung | Fehlerbehebung bei RTMP-Verteilungen
AWS CloudHSM	Fehlersuche
Amazon CloudSearch	Fehlerbehebung bei Amazon CloudSearch
AWS CodeDeploy	Fehlerbehebung für AWS CodeDeploy
Amazon CloudWatch	Fehlerbehebung für
AWS Database Migration Service	Fehlerbehebung bei Migrationsaufgaben in AWS Database Migration Service
AWS Data Pipeline	Fehlersuche
AWS Direct Connect	Fehlerbehebung für AWS Direct Connect
AWS Directory Service	Fehlerbehebung bei AWS Directory Service Verwaltungsproblemen
Amazon DynamoDB	Fehlerbehebung | Beheben von Problemen mit dem SSL-/TLS-Verbindungsaufbau
AWS Elastic Beanstalk	Fehlersuche
Amazon Elastic Compute Cloud (Amazon EC2)	Fehlerbehebung bei Instances | Fehlerbehebung bei Windows-Instances | Fehlerbehebung bei VM-Import/Export | Fehlerbehebung bei API-Anfragen | Fehlerbehebung beim AWS Management-Pack | Fehlerbehebung AWS Systems Manager für Microsoft SCVMM | AWS Diagnose für Microsoft Windows Server

Service	Link
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS-Fehlerbehebung
Amazon Elastic Kubernetes Service (Amazon EKS)	Amazon-EKS-Fehlerbehebung
Elastic Load Balancing	Fehlersuche bei Ihren Application Load Balancern | Fehlersuche für Ihren Classic Load Balancer
Amazon ElastiCache für Memcached	Fehlerbehebung bei Anwendungen
Amazon ElastiCache für Redis	Fehlerbehebung bei Anwendungen
Amazon EMR	Fehlersuche bei einem Cluster
AWS Flow Framework	Tipps zur Fehlersuche und Debugging
AWS Glue	Fehlersuche AWS Glue
AWS Glue DataBrew	Fehlerbehebung für Identität und Zugriff in AWS Glue DataBrew
AWS GovCloud (US)	Fehlersuche
AWS Identity and Access Management (IAM)	Fehlersuche bei IAM
Amazon Keyspaces (für Apache Cassandra)	Fehlerbehebung in Amazon Keyspaces (für Apache Cassandra)
Amazon Kinesis Data Streams	Fehlerbehebung bei Amazon-Kinesis-Data-Streams-Produzenten | Fehlersuche bei Amazon-Kinesis-Data-Streams-Konsumenten
Amazon Managed Service für Apache Flink	Fehlerbehebung bei der Leistung | Fehlerbehebung bei Amazon Managed Service für Apache Flink für SQL-Anwendungen
Amazon Data Firehose	Fehlerbehebung bei Amazon Data Firehose

Service	Link
AWS Lambda	Fehlerbehebungs- und AWS Lambda Überwachungsfunktionen mit CloudWatch
Amazon OpenSearch Service	Fehlerbehebung bei Amazon OpenSearch Service
AWS OpsWorks	Handbuch zur Fehlersuche und Fehlerbehebung
Amazon Personalize	Fehlersuche
Amazon QLDB	Fehlerbehebung bei Amazon QLDB
Amazon QuickSight	Fehlerbehebung bei Amazon QuickSight | Fehlerbehebung bei Fehlern übersprungener Zeilen
AWS Resource Access Manager (AWS RAM)	Beheben von Problemen mit AWS RAM
Amazon Redshift	Fehlerbehebung bei Abfragen | Fehlerbehebung bei Datenlade vorgängen | Fehlerbehebung bei Verbindungen in Amazon Redshift | Fehlerbehebung bei der Amazon-Redshift-Pr üfungsprotokollierung | Fehlerbehebung bei Abfragen in Amazon Redshift Spectrum
Amazon Relational Database Service (Amazon RDS)	Fehlerbehebung | Fehlerbehebung bei Anwendungen in Amazon RDS | Behebung von DB-Problemen für Amazon RDS Custom
Amazon Route 53	Fehlerbehebung bei Amazon Route 53
Amazon SageMaker	Fehlerbehebung | Fehlerbehebung bei Amazon SageMaker Studio
Amazon Silk	Fehlersuche
Amazon Simple Email Service (Amazon SES)	Fehlersuche bei Amazon SES
Amazon Simple Storage Service (Amazon S3)	Fehlerbehebung

Service	Link
Amazon Simple Workflow Service (Amazon SWF)	AWS Flow-Framework für Java: Tipps zur Fehlerbehebung und zum Debuggen | AWS Flow-Framework für Ruby: Fehlerbehebung und Debugging von Workflows
AWS Storage Gateway	Fehlerbehebung bei Ihrem Gateway
AWS Systems Manager	Fehlerbehebung bei SSM Agent
Amazon Virtual Private Cloud (Amazon VPC)	Fehlersuche
AWS Virtual Private Network (AWS VPN)	Fehlerbehebung bei Ihrem Kunden-Gateway-Gerät
AWS WAF	Testen und Optimieren Ihrer AWS WAF Schutzmaßnahmen
Amazon WorkMail	Fehlerbehebung bei der Amazon WorkMail -Webanwendung
Amazon WorkSpaces	Fehlerbehebung bei Amazon- WorkSpaces Problemen | Fehlerbehebung bei Amazon- WorkSpaces Client-Problemen

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation seit der letzten Version des AWS Support Dienstes beschrieben.

- AWS Support API-Version: 2013-04-15
- AWS Support App-API-Version: 20.08.2021

In der folgenden Tabelle werden wichtige Aktualisierungen der AWS Support AWS Trusted Advisor AND-Dokumentation ab dem 10. Mai 2021 beschrieben. Sie können den RSS-Feed abonnieren, um Benachrichtigungen über Aktualisierungen zu erhalten.

Änderung	Beschreibung	Datum
Aktualisierte Dokumentation für `AWSTrustedAdvisorServiceRolePolicy`	Es wurden neue IAM-Aktionen `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`	11. Juni 2024

	`rewall` und `sqs:GetQueueAttributes` zum Onboarding neuer Prüfungen hinzugefügt. Weitere Informationen finden Sie unter AWS managed policy: AWSTrustedAdvisorServiceRolePolicy (verwaltete Richtlinie).	
Dokumentation für AWS Support Empfehlungen hinzugefügt	Dokumentation für AWS Support Empfehlungen hinzugefügt.	22. Mai 2024
5 AWS Trusted Advisor Schecks aus der Dokumentation entfernt	5 AWS Trusted Advisor Prüfungen wurden entfernt, die jetzt veraltet sind. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	15. Mai 2024
Der Dokumentation wurde eine neue AWS Trusted Advisor Sicherheitsüberprüfung hinzugefügt	Der Dokumentation wurde 1 neuer AWS Trusted Advisor Sicherheitscheck hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	15. Mai 2024
3 Fehlertoleranzprüfungen wurden aus der Dokumentation entfernt	Es wurden 3 Fehlertoleranzprüfungen entfernt, die jetzt veraltet sind. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	25. April 2024

Die Dokumentation zu Fehlertoleranz und Sicherheitschecks wurde aktualisiert	Eine neue Fehlertoleranzprüfung wurde hinzugefügt. 1 Fehlertoleranz und 1 Sicherheitscheck wurden aktualisiert. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	29. März 2024
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	22. März 2024
Die Dokumentation für den AWS Support Plan wurde aktualisiert	Aktualisierungen der Funktionen von AWS Support Plänen. Weitere Informationen finden Sie unter AWS Support Pläne.	11. März 2024
Aktualisierte Dokumentation für Trusted Advisor	Es wurde eine Fehlertoleranzprüfung hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	29. Februar 2024

Aktualisierte Dokumentation für Trusted Advisor	Es wurde eine Fehlertoleranzprüfung hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	31. Januar 2024
Aktualisierte Dokumentation für `AWSTrustedAdvisorServiceRolePolicy`	Es wurden neue IAM-Aktionen `cloudtrail:GetTrail` ,`cloudtrail:ListTrails` , `cloudtrail:GetEventSelectors` `outposts:GetOutpost` , `outposts:ListAssets` und `outposts:ListOutposts` zum Integrieren neuer Prüfungen hinzugefügt. Weitere Informationen finden Sie unter AWS managed policy: AWSTrustedAdvisorServiceRolePolicy (verwaltete Richtlinie).	18. Januar 2024
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	17. Januar 2024

Aktualisierte Dokumentation für Trusted Advisor	Eine Fehlertoleranzprüfung wurde aktualisiert, um Titel und Beschreibung zu ändern. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	8. Januar 2024
Aktualisierte Dokumentation für Trusted Advisor	Eine Sicherheitsüberprüfung wurde aktualisiert, um der Änderung des Verfallszeitraums Rechnung zu tragen. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	21. Dezember 2023
Aktualisierte Dokumentation für Trusted Advisor	Es wurden 2 Sicherheitsüberprüfungen und 2 Leistungsprüfungen hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	20. Dezember 2023
Aktualisierte Dokumentation für Trusted Advisor	Eine Sicherheitsüberprüfung wurde hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	15. Dezember 2023
Die Dokumentation für Trusted Advisor Engage wurde aktualisiert	Die Trusted Advisor Engage-Dokumentation wurde mit Änderungen an der E-Mail-Benachrichtigungsoption aktualisiert.	14. Dezember 2023

Die Dokumentation für Trusted Advisor Engage wurde aktualisiert	Die Trusted Advisor Engage-Dokumentation wurde mit Änderungen für geplante Engagements aktualisiert.	11. Dezember 2023
Aktualisierte Dokumentation für Trusted Advisor	Es wurden 2 neue Fehlertoleranzprüfungen und 1 Kostenoptimierungsprüfung hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	07. Dezember 2023
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	6. Dezember 2023
Aktualisierte AWS verwaltete Richtlinien für Trusted Advisor	Die `AWSTrustedAdvisorPriorityFullAccess` und die `AWSTrustedAdvisorPriorityReadOnlyAccess` AWS verwalteten Richtlinien wurden aktualisiert und enthalten nun Kontoausgsnummern. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Trusted Advisor.	6. Dezember 2023

Die Dokumentation für wurde aktualisiert Trusted Advisor	Es wurden 3 neue Fehlertol eranzprüfungen hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	17. November 2023
Aktualisierte Dokumentation für Trusted Advisor	37 neue Schecks für Amazon RDS hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Schecks.	15. November 2023
Aktualisierte Dokumentation für `AWSTrustedAdvisorServiceRolePolicy`	Es wurden neue IAM-Aktio nen `ec2:DescribeRegions` `ecs:DescribeTaskDefinition` und neue Prüfungen `ecs:ListTaskDefinitions` hinzugefügt. `s3:GetLifecycleConfiguration` Weitere Informationen finden Sie unter AWS managed policy: AWSTrustedAdvisorServiceRolePolicy (verwaltete Richtlinie).	9. November 2023

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	27. Oktober 2023
Aktualisierte Dokumentation für Trusted Advisor	64 neue Prüfungen wurden hinzugefügt, die von integriert wurden AWS Config. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Schecks.	26. Oktober 2023
Aktualisierte Dokumentation für Trusted Advisor	Sechs neue Fehlertoleranz-Checks wurden hinzugefügt Trusted Advisor. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	12. Oktober 2023

Aktualisierte Dokumentation für `AWSTrustedAdvisorServiceRolePolicy`	Es wurden die neuen IAM-Aktionen `route53resolver:ListResolverEndpoints` , `route53resolver:ListResolverEndpointIpAddresses` , `ec2:DescribeSubnets` , `kafka:ListClustersV2` und `kafka:ListNodes` hinzugefügt, um neue Resilienzprüfungen einzuführen. Weitere Informationen finden Sie unter AWS managed policy: AWSTrustedAdvisorServiceRolePolicy (verwaltete Richtlinie).	14. September 2023
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	28. August 2023
Aktualisierte Dokumentation für Trusted Advisor	Es wurden 1 neue Service-Limit-Prüfungen für hinzugefügt AWS Lambda. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	17. August 2023

Aktualisierte Dokumentation für Trusted Advisor	Es wurde 1 neue Fehlertoleranzprüfung für Lambda hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	3. August 2023
Die Dokumentation für Trusted Advisor Engage wurde aktualisiert	Die Trusted Advisor Engage-Dokumentation wurde mit Änderungen an den Formularen für die Erstellung und Bearbeitung von Engagements aktualisiert. Seite mit Beispielen für Service Control-Richtlinien für hinzugefügt AWS Trusted Advisor.	27. Juli 2023
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	26. Juni 2023

Aktualisierte Dokumentation für Trusted Advisor	Es wurden zwei neue Fehlertoleranzprüfungen für Amazon MQ hinzugefügt. Es wurde eine neue Fehlertoleranzprüfung und eine neue Leistungsprüfung für Amazon Elastic File System hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	01. Juni 2023
Aktualisierte Dokumentation für Trusted Advisor	Es wurden zwei neue Fehlertoleranzprüfungen für NAT-Gateway hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	16. Mai 2023
Die Dokumentation für AWS Support Pläne wurde aktualisiert	Es wurden eine neue Genehmigung und CloudTrail Dokumentation für die Erstellung von Supportplänen hinzugefügt. Weitere Informationen finden Sie unter Zugriff auf AWS Support Pläne verwalten, Richtlinien für AWS Support Pläne verwalten und API-Aufrufe von AWSAWS Support Paketen protokollieren mit AWS CloudTrail.	8. Mai 2023

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	2. Mai 2023
Die Dokumentation für Trusted Advisor Engage und Trusted Advisor Priority wurde aktualisiert	Die Voraussetzungen für Trusted Advisor Engage und Trusted Advisor Priority wurden geklärt. Es wurde ein Beispiel für eine IAM-Richtlinie mit der Möglichkeit hinzugefügt, Trusted Advisor Engage zu verwenden und vertrauenswürdigen Zugriff auf Trusted Advisor zu aktivieren.	28. April 2023
Aktualisierte Dokumentation für Trusted Advisor	Zwei neue Fehlertoleranzprüfungen für AWS Resilience Hub und Incident Manager wurden hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	27. April 2023

Dokumentation für Trusted Advisor Engage hinzugefügt	Sie können AWS Trusted Advisor Engage verwenden, um das Beste aus Ihren AWS Support Plänen herauszuholen, indem Sie es Ihnen leicht machen, all Ihre proaktiven Interaktionen zu sehen, anzufordern und zu verfolgen und mit Ihrem AWS-Konto Team über laufende Engagements zu kommunizieren. Weitere Informationen finden Sie unter Erste Schritte mit AWS Trusted Advisor Engage.	06. April 2023
Aktualisierte Dokumentation für Trusted Advisor	Es wurden zwei neue Fehlertoleranzprüfungen für Amazon ECS hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	30. März 2023
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	16. März 2023

Dokumentation für Trusted Advisor Priority hinzugefügt	Die Trusted Advisor Priority-Konsole wurde aktualisiert: • Die Schaltflächen Acknowledge (Bestätigen) und Dismiss (Verwerfen) haben die Schaltflächen Accept (Akzeptieren) und Reject (Ablehnen) ersetzt. • Sie müssen Ihre Berufsbezeichnung oder Ihren Namen nicht eingeben, um Empfehlungen zu bestätigen, aufzulösen, zu verwerfen oder erneut zu öffnen. Weitere Informationen finden Sie unter Erste Schritte mit Trusted Advisor Priority.	16. Februar 2023
Aktualisierte Codebeispiele für AWS Support	Es wurden Codebeispiele für.NET, Java und Kotlin hinzugefügt, die zeigen, wie man es AWS Support mit einem AWS Software Development Kit (SDK) verwendet. Weitere Informationen finden Sie unter Codebeispiele für die AWS Support Verwendung von AWS SDKs.	16. Januar 2023

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	10. Januar 2023
Die Dokumentation für AWS Support App wurde aktualisiert	Sie können in Slack nach Support-Fällen suchen, indem Sie Filteroptionen verwenden oder nach der Fall-ID suchen. Weitere Informationen finden Sie unter Suchen nach Support-Fällen in Slack.	29. Dezember 2022
Die Dokumentation für die AWS Support App wurde aktualisiert	Sie können Terraform auch verwenden, um Ihre Ressourcen für die AWS Support App zu erstellen. Weitere Informationen finden Sie unter AWS Support App-Ressourcen mithilfe von Terraform erstellen.	22. Dezember 2022
Aktualisierte Dokumentation für Trusted Advisor	Drei neue Fehlertoleranzprüfungen für Amazon MemoryDB ElastiCache, Amazon und hinzugefügt. AWS CloudHSM Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	15. Dezember 2022

Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Sie können jetzt Live-Chat -Support für die folgenden Optionen anfordern: • Support für Abrechnungs- und Fakturierungsfälle • Unterstützung in japanisch er Sprache für technische Support-Fälle. • Weitere Informationen finden Sie unter Erstellen von Support-Fällen in einem Slack-Kanal.	14. Dezember 2022
Aktualisierte Dokumentation für AWS Support	Dokumentation über neue Endpunkte für die AWS Support API hinzugefügt. Weitere Informationen finden Sie unter Über die AWS Support -API.	14. Dezember 2022
Dokumentation für AWS CloudFormation Vorlagen zur Verwendung für die AWS Support App in Slack hinzugefügt	Du kannst CloudFormation Vorlagen verwenden, um Workspaces und Channels für die Slack-Konfiguration zu erstellen. AWS-Konten AWS Organizations Weitere Informationen findest du unter AWS Support App-Resso urcen erstellen mit. AWS CloudFormation	5. Dezember 2022

Die Dokumentation für wurde aktualisiert Trusted Advisor	Es wurden zwei neue Fehlertoleranzprüfungen für hinzugefügt AWS Resilience Hub. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	17. November 2022
Dokumentation zu Ihren AWS Security Hub Ergebnissen wurde hinzugefügt in Trusted Advisor	Ihre Ergebnisse aus den Security Hub Hub-Kontrollen werden Trusted Advisor schneller entfernt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Überprüfungen.	17. November 2022
Aktualisierte Dokumentation für AWS Trusted Advisor	Dokumentation für Trusted Advisor Empfehlungen hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	16. November 2022
Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Dokumentation für Japanische Sprachunterstützung hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Support-Fällen in einem Slack-Kanal.	11. November 2022

Die Dokumentation für AWS Support Pläne wurde aktualisiert	Informationen zur Fehlerbehebung wurden hinzugefügt, um Support Plans den Zugriff in einer Organisation zu ermöglichen. Weitere Informationen finden Sie unter Fehlerbehebung.	9. November 2022
Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Dokumentation für `supportapp` -Berechtigungen hinzugefügt. Weitere Informationen findest du unter Erforderliche Berechtigungen, damit die AWS Support App eine Verbindung zu Slack herstellen kann.	1. November 2022
Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Sie können den API-Vorgang `RegisterSlackWorkspaceForOrganization` verwenden, um einen Slack-Workspace für Ihr AWS-Konto zu registrieren. Um diese API aufrufen zu können, muss Ihr Konto Teil einer Organisation in AWS Organizations sein. Weitere Informationen finden Sie unter AWS Support -App in der Slack-API-Referenz.	19. Oktober 2022

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	4. Oktober 2022
Aktualisierte Dokumentation für Support Plans	Du kannst jetzt AWS Identity and Access Management (IAM) verwenden, um die Berechtigungen zur Änderung des Supportplans für dich zu verwalten. AWS-Konto Weitere Informationen finden Sie unter den folgenden Themen: • Zugriff für AWS Support Pläne verwalten • AWS verwaltete Richtlinien für AWS Support Pläne • AWS Support Pläne ändern • AWS Support API-Aufrufe protokollieren mit AWS CloudTrail	29. September 2022

Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Es wurde eine Dokumentation zur Konfiguration eines öffentlichen oder privaten Channels für die Verwendung mit der AWS Support App hinzugefügt. Weitere Informationen finden Sie unter Konfigurieren eines Slack-Kanals.	22. September 2022
Aktualisierte Dokumentation für AWS Support	Neuer Abschnitt zur Sicherheit für Ihre Support-Fälle hinzugefügt. Weitere Informationen finden Sie unter Sicherheit für Ihre AWS Support Fälle.	09. September 2022
Aktualisierte Dokumentation für Trusted Advisor	Neue Sicherheitsprüfung für Amazon EC2 hinzugefügt. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	01. September 2022

Die Dokumentation für die AWS Support App in Slack wurde aktualisiert	Weitere Informationen finden Sie in den folgenden Themen: Du kannst die AWS Support App verwenden, um deine Supportfälle zu verwalten, eine Erhöhung der Servicequ ote zu beantragen und direkt in deinen Slack-Kanälen mit Support-Mitarbeitern zu chatten. Weitere Informationen finden Sie in der Dokumenta tion zur AWS Support -App in Slack. Du kannst AWS verwaltet e Richtlinien an deine IAM-Rollen anhängen, um die AWS Support App zu nutzen. Weitere Informationen findest du unter AWS Verwaltete Richtlinien für AWS Support Apps in Slack. Neue API-Referenz für die AWS Support App. Informati onen finden Sie in der API-Referenz der AWS Support -App.	24. August 2022

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	17. August 2022
Dokumentation für Trusted Advisor Priority hinzugefügt	Trusted Advisor Priority fügt Unterstützung für die folgenden Funktionen hinzu: • Delegierte Administratoren • Tägliche und wöchentliche E-Mail-Benachrichtigungen für Zusammenfassungen von Empfehlungen • Gelöste oder abgelehnte Empfehlungen wieder aufnehmen • AWS verwaltete Richtlinien Weitere Informationen finden Sie unter Erste Schritte mit Trusted Advisor Priority.	17. August 2022
Die Dokumentation für wurde aktualisiert Trusted Advisor	Die Seite mit den Einstellungen in der Trusted Advisor Konsole wurde aktualisiert. Weitere Informationen finden Sie unter Erste Schritte mit AWS Trusted Advisor.	15. Juli 2022

Die Dokumentation für wurde aktualisiert Trusted Advisor	Die Überprüfungen wurden aktualisiert und enthalten nun die folgenden Informationen: • Warnungskriterien • Empfohlene Aktion • Weitere Ressourcen • Berichtsspalten Weitere Informationen finden Sie unter der AWS Trusted Advisor -Überprüfungsreferenz.	7. Juli 2022
Aktualisierte Dokumentation für AWS Support	Dokumentation hinzugefügt, die erläutert, wie Sie Ihre Supportfälle verwalten. • Aktualisieren eines vorhandenen Supportfalls • Fehlersuche	28. Juni 2022
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden Berechtigungen aktualisiert, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	23. Juni 2022

Aktualisierte Dokumentation für Trusted Advisor	Trusted Advisor unterstützt zusätzliche Sicherheitsstandardkontrollen von AWS Foundational Security Best Practices, von AWS Security Hub denen wir ausgehen. Weitere Informationen finden Sie im Änderungsprotokoll für AWS Trusted Advisor Überprüfungen.	23. Juni 2022
Aktualisierte Dokumentation für Trusted Advisor	Informationen zur Beantragung einer Erhöhung von Servicekontingenten wurden hinzugefügt. Weitere Informationen finden Sie unter Service-Limits.	21. Juni 2022
Aktualisierte Dokumentation für AWS Support	Das Erstellungserlebnis wurde in der Support-Center-Konsole aktualisiert. Weitere Informationen finden Sie unter Erstellung von Supportfällen und Fallmanagement.	18. Mai 2022
Aktualisierte Dokumentation für Trusted Advisor	Es wurden vier Überprüfungen für Amazon EBS und AWS Lambda hinzugefügt. Weitere Informationen finden Sie unter Melden Sie sich an, AWS Compute Optimizer um Trusted Advisor Schecks hinzuzufügen.	4. Mai 2022

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	27. April 2022
Aktualisierte Dokumentation für die Prüfung kompromittierter Zugriffsschlüssel	Diese Prüfung wird jetzt automatisch für Sie aktualisiert. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Schecks.	25. April 2022
Aktualisierte Dokumentation für Trusted Advisor	Die AWS Direct Connect Prüfungen in der Kategorie Fehlertoleranz wurden aktualisiert. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	29. März 2022

Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	14. März 2022
Dokumentation für Trusted Advisor Priority hinzugefügt	Sie können Trusted Advisor Priority verwenden, um eine Liste mit priorisierten Empfehlungen von Ihrem Technical Account Manager (TAM) einzusehen. Weitere Informationen finden Sie unter Erste Schritte mit Trusted Advisor Priority.	28. Februar 2022
Aktualisierte Dokumentation zur Nutzung von Amazon EventBridge für Trusted Advisor	Sie können eine EventBridge Regel erstellen, um Änderungen an Ihren Trusted Advisor Schecks zu überwachen. Weitere Informationen finden Sie unter AWS Trusted Advisor Prüfergebnisse überwachen mit EventBridge.	21. Februar 2022

Neue Dokumentation für die Verwendung von Amazon EventBridge zur Überwachung von AWS Support Fällen	Sie können eine EventBridge Regel erstellen, um Ihre Supportfälle zu überwachen und Benachrichtigungen darüber zu erhalten. Weitere Informationen finden Sie unter AWS Support Fälle überwachen mit EventBridge.	21. Februar 2022
Aktualisierte Dokumentation für `AWSSupportServiceRolePolicy`	Es wurden neue Berechtigungen hinzugefügt, um Fakturierungs-, Verwaltungs- und Supportservices für die servicegebundene Rolle bereitzustellen. Weitere Informationen finden Sie unter AWS managed policy: AWSSupportServiceRolePolicy (verwaltete Richtlinie).	17. Februar 2022
Dokumentation für die Integration mit hinzugefügt AWS Security Hub	In der Trusted Advisor Konsole können Sie jetzt die Ergebnisse für Ihre Security Hub-Steuerelemente einsehen, die Teil des Sicherheitsstandards AWS Foundation Security Best Practices sind. Weitere Informationen finden Sie unter AWS Security Hub Steuerelemente in der AWS Trusted Advisor Konsole anzeigen.	18. Januar 2022

Die Dokumentation für wurde aktualisiert Trusted Advisor	Es wurden drei neue Prüfungen für Amazon-EC 2-Instances hinzugefügt, auf denen Microsoft SQL Server ausgeführt wird. • Konsolidierung von Amazon-EC2-Instances für Microsoft SQL Server • Amazon-EC2-Instances für Microsoft SQL Server mit übermäßiger Bereitstellung • Amazon-EC2-Instances mit veraltetem Microsoft SQL Server (Ende des Supports) Weitere Informationen finden Sie unter der AWS Trusted Advisor -Überprüfungsreferenz.	20. Dezember 2021

Aktualisierte Dokumentation für Trusted Advisor	Trusted Advisor vier neue Schecks für hinzugefügt AWS Well-Architected • AWS Well-Architected-Probleme mit hohem Risiko für die Kostenoptimierung • AWS Well-Architected-Probleme mit hohem Risiko für die Leistung • AWS Well-Architected-Probleme mit hohem Risiko für die Sicherheit • AWS Well-Architected-Probleme mit hohem Risiko für die Zuverlässigkeit Weitere Informationen finden Sie unter der AWS Trusted Advisor -Überprüfungsreferenz.	20. Dezember 2021
Aktualisierte Dokumentation	Wenn Sie einen Enterprise On-Ramp Support-Plan haben, haben Sie Zugriff auf alle Trusted Advisor Checks und die AWS Support API.	24. November 2021
Aktualisierte Dokumentation für Trusted Advisor	Trusted Advisor zwei neue Prüfungen für Amazon Comprehend hinzugefügt. Weitere Informationen finden Sie unter der AWS Trusted Advisor -Überprüfungsreferenz.	29. September 2021

Aktualisierte Dokumentation für Trusted Advisor	Der Prüfungsname für Amazon OpenSearch Service Reserved Instance Optimization wurde aktualisiert. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Schecks.	8. September 2021
Die Dokumentation für Trusted Advisor Schecks wurde aktualisiert	Es wurde ein Referenzschema für alle Trusted Advisor Prüfungen hinzugefügt. Weitere Informationen finden Sie unter dem AWS Trusted Advisor Referenz-Prüfung.	1. September 2021
Die Dokumentation für Trusted Advisor verwaltete Richtlinien wurde aktualisiert	Die Dokumentation für die Trusted Advisor verwalteten Richtlinien wurde aktualisiert. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für AWS Support und AWS Trusted Advisor.	10. August 2021
Aktualisierte Dokumentation für Trusted Advisor	Die Dokumentation für die Trusted Advisor Konsole wurde aktualisiert. Weitere Informationen finden Sie unter Erste Schritte mit AWS Trusted Advisor.	16. Juli 2021

Die Dokumentation zum Erstellen von AWS Support Fällen wurde aktualisiert	Es wurde eine Dokumentation darüber hinzugefügt, wie ein zugehöriger Support-Fall für dauerhaft geschlossene Fälle erstellt werden kann. Weitere Informationen finden Sie unter Wiederaufnahme eines abgeschlossenen Falls und Erstellen eines zugehörigen Falls.	8. Juni 2021
Aktualisierte Dokumentation für Trusted Advisor	Trusted Advisor hat zwei neue Prüfungen für den Amazon Elastic Block Store (Amazon EBS) -Volumenspeicher hinzugefügt. Weitere Informationen finden Sie unter Änderungsprotokoll für AWS Trusted Advisor Prüfungen.	8. Juni 2021
Aktualisierte Dokumentation	Die folgenden Themen werden aktualisiert: • Aktualisierte Verfahren und zusätzliche Inhalte zum Thema CloudWatch Amazon-Alarme zur Überwachung von AWS Trusted Advisor Messwerten erstellen • Die Service-Kontingente für den AWS Support API-Bereich wurden hinzugefügt	12. Mai 2021

Frühere Aktualisierungen

Änderung	Beschreibung	Datum
Aktualisierte Dokumentation für Trusted Advisor	Dokumentation zum Filtern, Aktualisieren und Download von Prüfungsergebnissen hinzugefügt. Weitere Informationen finden Sie in den folgenden Abschnitten: • Ihre Prüfungen filter • Ergebnisse der Prüfung aktualisieren • Herunterladen der Prüfungsergebnisse	16. März 2021
Die Dokumentation zu AWS verwaltet en Richtlinien wurde aktualisiert	Es wurden Informationen zur `AWSSuppor tServiceRolePolicy` AWS verwalteten Richtlinie hinzugefügt. Weitere Informationen finden Sie unter Verwenden von serviceve rknüpften Rollen für AWS Support.	16. März 2021
Es wurden Prüfungen für hinzugefügt AWS Lambda	Vier AWS Trusted Advisor Prüfungen für Lambda wurden hinzugefügt. Protokoll ändern für AWS Trusted Advisor	8. März 2021
Aktualisierte Prüfungen der Servicegrenzen für Amazon Elastic Block Store	Fünf AWS Trusted Advisor Prüfungen für Amazon EBS wurden in der Protokoll ändern für AWS Trusted Advisor aktualisiert.	5. März 2021
Die Dokumentation für CloudTrail die Protokollierung wurde aktualisiert	CloudTrail unterstützt die Protokollierung von Konsolenaktionen, wenn Sie Ihren AWS Support Plan ändern. Weitere Informationen finden Sie unter Protokollieren von Änderungen an Ihrem AWS Support Plan.	9. Februar 2021

Änderung	Beschreibung	Datum
Aktualisierte Dokumentation für Trusted Advisor	Das Thema Erste Schritte mit Trusted Advisor - Empfehlungen wurde aktualisiert.	29. Januar 2021
Aktualisierte Dokumentation für Trusted Advisor Berichte	Es wurde ein Fehlerbehebung Abschnitt für die Verwendung von Trusted Advisor Berichten mit anderen AWS Diensten hinzugefügt.	4. Dezember 2020
AWS Trusted Advisor Unterstützung für die AWS CloudTrail Protokollierung hinzugefügt	CloudTrail unterstützt die Protokollierung für eine Teilmenge von Trusted Advisor Konsolenaktionen. Weitere Informationen finden Sie unter AWS Trusted Advisor Konsolenaktionen protokollieren mit AWS CloudTrail.	23. November 2020
Ein Thema für das Änderungsprotokoll hinzugefügt	Änderungen an AWS Trusted Advisor Prüfungen und Kategorien finden Sie in derProtokoll ändern für AWS Trusted Advisor.	18. November 2020
Zusätzliche Unterstützung für Organisationseinheiten	Sie können jetzt Berichte für Trusted Advisor Prüfungen für Organisationseinheiten (OUs) erstellen. Weitere Informationen finden Sie unter Berichte für die Organisationsansicht erstellen.	17. November 2020
Die Protokollierung mit dem AWS CloudTrail Thema wurde aktualisiert	Ein Beispielprotokolleintrag für einen Trusted Advisor API-Vorgang wurde hinzugefügt. Siehe AWS Trusted Advisor-Informationen in der CloudTrail Protokollierung.	22. Oktober 2020
AWS Support Kontingente hinzugefügt	Es wurden Informationen über die aktuellen Kontingente und Beschränkungen für AWS Support. Weitere Informationen finden Sie unter AWS Support -Endpunkte und -Kontingente im Allgemeine AWS-Referenz.	4. August 2020

Änderung	Beschreibung	Datum
Organisatorische Ansicht für AWS Trusted Advisor	Sie können jetzt Berichte für Trusted Advisor Schecks für Konten erstellen, die Teil von sind AWS Organizations. Siehe Organisationsansicht für AWS Trusted Advisor.	17. Juli 2020
Sicherheit und AWS Support	Es wurden Informationen zu Sicherheitsüberlegungen bei der Verwendung von AWS Support und Trusted Advisor aktualisiert. Siehe Sicherheit in AWS Support.	5. Mai 2020
Sicherheit und AWS Support	Es wurden Informationen zu Sicherheitsüberlegungen bei der Verwendung von AWS Support hinzugefügt.	10. Januar 2020
Verwendung Trusted Advisor als Webservice	Es wurden aktualisierte Anweisungen hinzugefügt, um Trusted Advisor Daten zu aktualisieren, nachdem die Liste der Trusted Advisor Prüfungen abgerufen wurde.	1. November 2018
Verwenden von serviceverknüpften Rollen	Neuer Abschnitt hinzugefügt.	11. Juli 2018
Erste Schritte: Fehlerbehebung	Links zur Fehlerbehebung für Route 53 und AWS Certificate Manager.	1. September 2017
Beispiel eines Fallmanagements: Erstellen eines Falls	Eine Notiz zu dem Feld CC für Benutzer hinzugefügt, die über den „Basic“-Support-Plan verfügen.	1. August 2017
Trusted Advisor Prüfergebnisse anhand von CloudWatch Ereignissen überwachen	Neuer Abschnitt hinzugefügt.	18. November 2016

Änderung	Beschreibung	Datum
Fallmanagement	Die Namen der Falldringlichkeitsstufen aktualisiert.	27. Oktober 2016
AWS Support Anrufe protokollieren mit AWS CloudTrail	Neuer Abschnitt hinzugefügt.	21. April 2016
Erste Schritte: Fehlerbehebung	Weitere Links zur Fehlerbehebung hinzugefügt.	19. Mai 2015
Erste Schritte: Fehlerbehebung	Weitere Links zur Fehlerbehebung hinzugefügt.	18. November 2014
Erste Schritte: Fallmanagement	Aktualisiert, um Service Catalog in der AWS Management Console wiederzugeben.	30. Oktober 2014
Den Ablauf eines AWS Support Falls programmieren	Informationen über neue API-Elemente für das Hinzufügen von Anlagen in Fällen und für das Weglassen von Fallkommunikation, wenn der Fallverlauf abgerufen wird, hinzugefügt.	16. Juli 2014
Zugreifen AWS Support	Angegebene Support-Kontakte als Zugriffsmethode entfernt.	28. Mai 2014
Erste Schritte	Den Abschnitt mit den ersten Schritten hinzugefügt.	13. Dezember 2013
Erste Veröffentlichung	Neuer AWS Support Dienst veröffentlicht.	30. April 2013

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.