Referenzhandbuch

AWS Verwaltung von Benutzerkonten

AWS Verwaltung von Benutzerkonten: Referenzhandbuch

Table of Contents

Willkommen 1
Brauche ich mehrereAWS-Konten? 2
Verwalten mehrererAWS-Konten 3
Erste Schritte: Sind Sie ein AWS Erstbenutzer? 3
Voraussetzungen 4
Schritt 1: Erstellen Sie Ihr AWS-Konto 5
Schritt 2: MFA für Ihren Root-Benutzer aktivieren 7
Schritt 3: Erstellen Sie einen Administratorbenutzer 7
Verwandte Themen 7
Den Root-Benutzer verwenden 8
Verwalten Ihrer Konten 9
Erstellen Sie in Ihrem Konto 9
Anzeigen Ihrer Konto-IDs 12
Suchen Ihrer AWS-Konto -ID 13
Ermitteln der kanonischen Benutzer-ID für Ihr AWS-Konto 16
Aktualisieren Ihrer Kontoeinstellungen 18
Verständnis der API-Betriebsmodi 20
Berechtigungen zum Aktualisieren von Kontoattributen gewähren 22
Aktualisieren Sie die Kontaktinformationen Ihres Kontos 24
Alternative Kontokontakte 24
Kontakt des primären Kontos 34
Aktualisieren Sie Ihre Sicherheitsfragen 41
Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann 42
Überlegungen vor dem Aktivieren und Deaktivieren von Regionen 44
Aktiviere oder deaktiviere eine Region für eigenständige Konten 46
Aktivieren oder deaktivieren Sie eine Region in Ihrer Organisation 49
Erstellen oder aktualisieren Sie Ihren Kontoalias 51
Abrechnung für IhreAWS-Konto 52
Konten in Indien verwalten 52
Ermitteln Sie, bei welchem Unternehmen Ihr Konto ist 53
Erstelle eineAWS-Kontomit AISPL 53
Verwalte dein AISPL-Konto 55
Schließe dein Konto 55
Was müssen Sie wissen, bevor Sie Ihr Konto schließen 56

Wie können Sie Ihr Konto schließen ... 58
Was erwartet Sie, nachdem Sie Ihr Konto geschlossen haben ... 61
Kontoverwaltung und AWS Organizations ... 63
Vertrauenswürdiger Zugriff ... 64
Delegiertes Administratorkonto ... 66
Beispiel-SCPs ... 67
Sicherheit ... 70
Datenschutz ... 71
AWS PrivateLink ... 72
Erstellen des Endpunkts ... 72
Amazon VPC-Endpunktrichtlinien ... 73
Endpunktrichtlinien ... 73
Identitäts- und Zugriffsverwaltung ... 74
Zielgruppe ... 75
Authentifizierung mit Identitäten ... 75
Verwalten des Zugriffs mit Richtlinien ... 79
AWS Kontoverwaltung und IAM ... 82
Beispiele für identitätsbasierte Richtlinien ... 91
Verwenden identitätsbasierter Richtlinien ... 95
Fehlerbehebung ... 97
Von AWS verwaltete Richtlinien ... 100
AWSAccountManagementReadOnlyAccess ... 100
AWSAccountManagementFullAccess ... 101
Richtlinienaktualisierungen ... 102
Compliance-Validierung ... 103
Ausfallsicherheit ... 104
Sicherheit der Infrastruktur ... 104
Überwachung ... 105
CloudTrail-Protokolle ... 105
Informationen zur Kontoverwaltung in CloudTrail ... 106
Verstehen der Logeinträge zur Kontoverwaltung ... 107
Überwachung von Kontoverwaltungsereignissen mit EventBridge ... 110
Ereignisse im Bereich Kontoverwaltung ... 111
API-Referenz ... 113
Aktionen ... 115
DeleteAlternateContact ... 116

DisableRegion ... 121
EnableRegion ... 125
GetAlternateContact ... 129
GetContactInformation ... 135
GetRegionOptStatus ... 139
ListRegions ... 143
PutAlternateContact ... 148
PutContactInformation ... 154
Zugehörige Aktionen ... 157
CreateAccount ... 157
createGovCloudAccount ... 157
DescribeAccount ... 157
Datentypen ... 158
AlternateContact ... 159
ContactInformation ... 161
Region ... 165
ValidationExceptionField ... 166
Geläufige Parameter ... 166
Häufige Fehler ... 169
Erstellen von HTTP-Abfrageanforderungen ... 171
Endpunkte ... 172
HTTPS erforderlich ... 172
SignierenAWSAPI-Anfragen zur Kontoverwaltung ... 172
Kontingente ... 173
Fehlerbehebung bei Ihrem AWS-Konto ... 175
Probleme bei der Kontoerstellung ... 175
Ich habe den Anruf von AWS zur Bestätigung meines neuen Kontos nicht erhalten ... 175
Ich erhalte die Fehlermeldung „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine Versuche AWS-Konto telefonisch zu verifizieren ... 176
Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert ... 177
Probleme mit der Kontoschließung ... 178
Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann ... 178
Ich sehe die Schaltfläche Konto schließen auf der Seite Konten nicht ... 179
Ich habe mein Konto geschlossen, aber immer noch keine E-Mail-Bestätigung erhalten ... 179
Ich erhalte die Fehlermeldung „ConstraintViolationException“, wenn ich versuche, mein Konto zu schließen ... 179

Ich erhalte die Fehlermeldung „CLOSE_ACCOUNT_QUOTA_EXCEED“, wenn ich versuche, ein Mitgliedskonto zu schließen 180
Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließen kann? 180
Sonstige Probleme 180
Ich muss die Kreditkarte für meine ändernAWS-Konto 180
Ich muss betrügerisch meldenAWS-KontoAktivität 181
Ich muss meine schließenAWS-Konto 181
Dokumentverlauf 182
AWS-Glossar 184
..... clxxxv

Willkommen im Referenzhandbuch zur AWS Kontoverwaltung

AWS-Kontensind ein grundlegender Bestandteil des Zugriffs auf AWS Dienste.

Und AWS-Konto erfüllt zwei grundlegende Funktionen:

- Container — An AWS-Konto ist der Basiscontainer für alle AWS Ressourcen, die Sie als AWS Kunde erstellen. Beispielsweise sind ein Amazon Simple Storage Service (Amazon S3) -Bucket, eine Amazon Relational Database Service (Amazon RDS) -Datenbank und eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance alles Ressourcen. Jede Ressource wird eindeutig durch einen Amazon-Ressourcennamen (ARN) identifiziert, der die Konto-ID des Kontos enthält, das die Ressource enthält oder besitzt.
- Sicherheitsgrenze — An AWS-Konto ist auch die grundlegende Sicherheitsgrenze für Ihre AWS Ressourcen. Ressourcen, die Sie in Ihrem Konto erstellen, stehen Benutzern zur Verfügung, die über Anmeldeinformationen für Ihr Konto verfügen.

  Zu den wichtigsten Ressourcen, die Sie in Ihrem Konto erstellen können, gehören Identitäten wie Benutzer und Rollen. Identitäten verfügen über Anmeldeinformationen, mit denen sich jemand anmelden (authentifizieren) kann. AWS Für Identitäten gibt es auch Berechtigungsrichtlinien, die festlegen, was ein Benutzer mit den Ressourcen im Konto tun kann (Autorisierung).

  Aus Sicherheitsgründen sollten Sie von Ihren Benutzern verlangen, dass sie beim Zugriff AWS temporäre Anmeldeinformationen verwenden. Um temporäre Anmeldeinformationen bereitzustellen, können Sie einen Verbund und einen Identitätsanbieter wie AWS IAM Identity Center(IAM Identity Center) verwenden. Wenn Ihr Unternehmen bereits einen Identitätsanbieter verwendet, verwenden Sie ihn zusammen mit einem Verbund, um den Zugriff auf die Ressourcen in Ihrem AWS-Konto System zu vereinfachen.

  Informationen zu bewährten Sicherheitsmethoden finden Sie unter Bewährte Sicherheitsmethoden in IAM im IAM-Benutzerhandbuch.

Themen

- Brauche ich mehrereAWS-Konten?
- Erste Schritte: Sind Sie ein AWS Erstbenutzer?
- Verwendung der Root-Benutzer des AWS-Kontos

Brauche ich mehrereAWS-Konten?

AWS-Kontendienen als grundlegende Sicherheitsgrenze inAWSaus. Sie dienen als Ressourcencontainer, der eine nützliche Isolationsstufe bietet. Die Fähigkeit, Ressourcen und Benutzer zu isolieren, ist eine wichtige Voraussetzung für die Schaffung einer sicheren, gut verwalteten Umgebung.

Trennen Sie Ihre Ressourcen in separateAWS-Kontenhilft Ihnen, die folgenden Prinzipien in Ihrer Cloud-Umgebung zu unterstützen:

- Sicherheitskontrolle- Verschiedene Anwendungen können unterschiedliche Sicherheitsprofile haben, die unterschiedliche Kontrollrichtlinien und -mechanismen erfordern. Zum Beispiel ist es viel einfacher, mit einem Auditor zu sprechen und auf einen einzigen verweisen zu könnenAWS-Kontodas alle Elemente Ihrer Workload hostet, die unterliegenSicherheitsstandards für Payment Card Industry (PCI)aus.
- ISOLATION— EinAWS-Kontoist eine Einheit des Sicherheitsschutzes. Potenzielle Risiken und Sicherheitsbedrohungen sollten in einemAWS-Kontoohne andere zu beeinflussen. Aufgrund verschiedener Teams oder verschiedener Sicherheitsprofile kann es unterschiedliche Sicherheitsbedürfnisse geben.
- Viele Teams- Verschiedene Teams haben ihre unterschiedlichen Verantwortlichkeiten und Ressourcenbedürfnisse. Sie können verhindern, dass sich Teams gegenseitig stören, indem Sie sie auf separateAWS-Kontenaus.
- Datenisolierung— Neben der Isolierung der Teams ist es wichtig, die Datenspeicher auf ein Konto zu isolieren. Dies kann dazu beitragen, die Anzahl der Personen zu begrenzen, die auf diesen Datenspeicher zugreifen und diese verwalten können. Dies trägt dazu bei, die Exposition gegenüber hochprivaten Daten einzudämmen und kann daher bei der Einhaltung der(DSGVO) der Europäischen Unionaus.
- Geschäftsprozess— Verschiedene Geschäftsbereiche oder Produkte können völlig unterschiedliche Zwecke und Prozesse haben. Mit mehrerenAWS-Kontenkönnen Sie die spezifischen Anforderungen einer Geschäftseinheit unterstützen.
- Fakturierung— Ein Konto ist die einzig wahre Möglichkeit, Artikel auf Abrechnungsebene zu trennen. Mehrere Konten helfen dabei, Elemente auf Abrechnungsebene zwischen Geschäftseinheiten, funktionalen Teams oder einzelnen Benutzern zu trennen. Sie können alle Ihre Rechnungen weiterhin auf einen einzelnen Zahler konsolidieren lassen (mitAWS Organizationsund konsolidierte Abrechnung), während Einzelposten getrennt durchAWS-Kontoaus.

- Kontingentzuweisung–AWSService-Kontingente werden für jeden separat durchgesetztAWS-Kontoaus. Aufteilen von Workloads in verschiedeneAWS-Kontenverhindert, dass sie Quoten füreinander konsumieren.

Alle in diesem Dokument beschriebenen Empfehlungen und Verfahren entsprechen demAWSWell-Architected Frameworkaus. Dieses Framework soll Ihnen dabei helfen, eine flexible, belastbare und skalierbare Cloud-Infrastruktur zu entwickeln. Auch wenn Sie klein anfangen, empfehlen wir Ihnen, diese Anleitung im Rahmen einzuhalten. Dies kann Ihnen helfen, Ihre Umgebung sicher und ohne Auswirkungen auf Ihren laufenden Betrieb zu beeinträchtigen, während Sie wachsen.

Verwalten mehrererAWS-Konten

Bevor Sie mit dem Hinzufügen mehrerer Konten beginnen, sollten Sie einen Plan entwickeln, um sie zu verwalten. Dafür empfehlen wir die Verwendung vonAWS Organizations, welches ist kostenlosAWSService zur Verwaltung allerAWS-Kontenin Ihrer Organisation.

AWSbietet auchAWS Control Tower, das Ebenen vonAWSverwaltete Automatisierung für Organizations und integriert sie automatisch mit anderenAWSDienstleistungen wieAWS CloudTrail,AWS Config, Amazon CloudWatchAWS Service Catalogund andere. Für diese Dienste können zusätzliche Kosten fallen. Weitere Informationen finden Sie unter AWS Control Tower Preise.

Erste Schritte: Sind Sie ein AWS Erstbenutzer?

Wenn Sie zum ersten Mal Benutzer von sindAWS, registrieren Sie sich zunächst für einenAWS-Konto. Wenn Sie sich anmelden, AWS erstellt eine AWS-Konto mit den von Ihnen angegebenen Daten und weist Ihnen das Konto zu. Nachdem Sie Ihren erstellt habenAWS-Konto, melden Sie sich als Root-Benutzer an, aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer und weisen Sie einem Benutzer Administratorzugriff zu.

Schritte

- Voraussetzungen
- Schritt 1: Erstellen Sie Ihr AWS-Konto
- Schritt 2: MFA für Ihren Root-Benutzer aktivieren
- Schritt 3: Erstellen Sie einen Administratorbenutzer
- Verwandte Themen

Voraussetzungen

Um sich für einen zu registrierenAWS-Konto, benötigen Sie die folgenden Informationen:

- Ein Kontoname — Der Name des Accounts erscheint an verschiedenen Stellen, z. B. auf Ihrer Rechnung und in Konsolen wie dem Billing and Cost Management-Dashboard und der AWS Organizations Konsole.

  Wir empfehlen Ihnen, für die Benennung Ihrer Konten eine Standardmethode zu verwenden, damit Sie Ihren Konten Namen geben können, die leicht zu erkennen sind. Erwägen Sie, für Unternehmenskonten einen Benennungsstandard wie Organisation — Zweck — Umgebung zu verwenden (z. B. AnyCompany— Audit — Produktion). Für Privatkonten sollten Sie in Erwägung ziehen, einen Benennungsstandard wie Vorname — Nachname — Zweck zu verwenden (z. B. paulo-santos-testaccount).

  Informationen zum Ändern eines Kontonamens finden Sie unter Wie ändere ich den Namen auf meinemAWS-Konto? .
- Adresse — Wenn sich Ihre Kontaktadresse in Indien befindet, wurde die Benutzervereinbarung für Ihr Konto mit Amazon Internet Services Private Limited (AISPL), einem lokalen AWS Verkäufer in Indien, abgeschlossen. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben. Abhängig von Ihrer Bank müssen Sie möglicherweise auch ein Einmalpasswort eingeben. AISPL berechnet Ihrer Zahlungsmethode im Rahmen des Überprüfungsprozesses 2 INR. AISPL erstattet die 2 INR nach Abschluss der Überprüfung zurück.
- Eine E-Mail-Adresse — Die E-Mail-Adresse wird als Anmeldename für den Root-Benutzer verwendet und ist für die Kontowiederherstellung erforderlich. Sie müssen in der Lage sein, E-Mail-Nachrichten zu empfangen, die an diese Adresse gesendet werden. Bevor Sie bestimmte Aufgaben ausführen können, müssen Sie sicherstellen, dass Sie Zugriff auf E-Mails haben, die an diese Adresse gesendet wurden.

> **Important**
>
> Wenn dieses Konto für ein Unternehmen bestimmt ist, verwenden Sie (z. B.`it.admins@example.com`) eine sichere Unternehmensverteilerliste, damit Ihr Unternehmen AWS-Konto auch dann Zugriff darauf hat, wenn ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt. Da die E-Mail-Adresse verwendet werden kann, um die Root-Benutzeranmeldeinformationen des Kontos zurückzusetzen, sollten Sie den Zugriff auf diese Verteilerliste oder Adresse schützen.

- Eine Telefonnummer — Diese Nummer kann verwendet werden, um die Inhaberschaft Ihres Kontos zu bestätigen. Sie müssen in der Lage sein, Anrufe unter dieser Telefonnummer entgegenzunehmen.

> **Important**
>
> Wenn dieses Konto für ein Unternehmen bestimmt ist, verwenden Sie eine Unternehmenstelefonnummer, damit Ihr Unternehmen AWS-Konto auch dann Zugriff darauf hat, wenn ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt.

Schritt 1: Erstellen Sie Ihr AWS-Konto

1. Öffnen Sie in Ihrem Browser die AWSStartseite.
2. Wählen Sie Create an AWS-Konto.

> **Note**
>
> Wenn Sie sich AWS vor Kurzem angemeldet haben, wählen Sie Anmelden. Wenn die Option Neues Konto erstellen AWS-Konto nicht sichtbar ist, wählen Sie zuerst Mit einem anderen Konto anmelden und dann Neues erstellen ausAWS-Konto.

3. Geben Sie Ihre Kontoinformationen ein und wählen Sie dann E-Mail-Adresse verifizieren aus. Dadurch wird ein Bestätigungscode an die von Ihnen angegebene E-Mail-Adresse gesendet.
4. Geben Sie Ihren Bestätigungscode ein und wählen Sie dann Verifizieren.
5. Geben Sie ein sicheres Passwort für Ihren Root-Benutzer ein, bestätigen Sie es und wählen Sie dann Weiter. AWSsetzt voraus, dass Ihr Passwort die folgenden Bedingungen erfüllt:
   - Es muss mindestens 8 Zeichen und darf maximal 128 Zeichen lang sein.
   - Es muss mindestens drei der folgenden Zeichentypen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und! @ # $% ^ & * () <> [] {} | _+-= Symbole.
   - Es darf nicht mit Ihrem AWS-Konto Namen oder Ihrer E-Mail-Adresse identisch sein.
6. Wählen Sie Geschäftlich oder Persönlich. Der Unterschied zwischen diesen Optionen besteht in den Informationen, nach denen wir Sie fragen. Beide Kontotypen haben dieselben Merkmale und Funktionen.

7. Geben Sie Ihre geschäftlichen oder persönlichen Daten ein. Informationen zur E-Mail-Adresse und Telefonnummer finden Sie in den Empfehlungen im Abschnitt Voraussetzungen.
8. Lesen und akzeptieren Sie die AWSKundenvereinbarung. Stellen Sie sicher, dass Sie die Bedingungen der AWS Kundenvereinbarung gelesen und verstanden haben.
9. Klicken Sie auf Weiter. Zu diesem Zeitpunkt erhalten Sie eine E-Mail-Nachricht, in der bestätigt wird, dass Ihr AWS-Konto Gerät einsatzbereit ist. Sie können sich mit der E-Mail-Adresse und dem Passwort, die Sie bei der Registrierung angegeben haben, bei Ihrem neuen Konto anmelden. Sie können jedoch keine AWS Dienste nutzen, bis Sie die Aktivierung Ihres Kontos abgeschlossen haben.
10. Geben Sie Informationen zu Ihrer Zahlungsmethode ein. Wenn Sie eine andere Adresse für Rechnungszwecke verwenden möchten, wählen Sie Neue Adresse verwenden.
11. Wählen Sie Überprüfen und fortfahren aus.
12. Geben Sie Ihren Landes- oder Regionalcode aus der Liste ein und geben Sie dann eine Telefonnummer ein, unter der Sie in den nächsten Minuten erreichbar sind. Geben Sie den CAPTCHA-Code ein und senden Sie ihn ab.
13. Wenn das automatisierte System Sie kontaktiert, geben Sie die PIN ein, die Sie erhalten haben, und senden Sie sie dann ab.
14. Wählen Sie Ihren AWS Support Plan aus. Eine Beschreibung der verfügbaren Tarife finden Sie unter AWS SupportTarife vergleichen.
15. Wählen Sie Registrierung abschließen aus. Eine Bestätigungsseite wird angezeigt, die darauf hinweist, dass Ihr Konto aktiviert wird.
16. Suchen Sie in Ihrem E-Mail- und Spam-Ordner nach einer E-Mail-Nachricht, die bestätigt, dass Ihr Konto aktiviert wurde. Die Aktivierung dauert normalerweise einige Minuten, kann aber manchmal bis zu 24 Stunden dauern.

    Nachdem Sie die Aktivierungsnachricht erhalten haben, haben Sie vollen Zugriff auf alle AWS Dienste.

> **Note**
>
> Falls Sie Probleme mit der Kontoaktivierung haben, finden Sie weitere Informationen unterthe section called “Probleme bei der Kontoerstellung”.

Schritt 2: MFA für Ihren Root-Benutzer aktivieren

Wir empfehlen dringend, MFA für Ihren Root-Benutzer zu aktivieren. MFA senkt das Risiko, dass jemand ohne Ihre Genehmigung auf Ihr Konto zugreift, erheblich.

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit Ihrem Root-Benutzer finden Sie unter AWS Management Console Als Root-Benutzer anmelden im AWS Anmelde-Benutzerhandbuch.
2. Schalten Sie MFA für Ihren Root-Benutzer ein.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto (Konsole) im IAM-Benutzerhandbuch.

Schritt 3: Erstellen Sie einen Administratorbenutzer

Da Sie nicht einschränken können, was ein Root-Benutzer tun kann, empfehlen wir dringend, Ihren Root-Benutzer nicht für Aufgaben zu verwenden, für die der Root-Benutzer nicht ausdrücklich erforderlich ist. Weisen Sie stattdessen einem Administratorbenutzer in IAM Identity Center Administratorzugriff zu und melden Sie sich als dieser Administratorbenutzer an, um Ihre täglichen Verwaltungsaufgaben auszuführen.

Anweisungen finden Sie unter AWS-KontoZugriff für einen IAM Identity Center-Administratorbenutzer einrichten im IAM Identity Center-Benutzerhandbuch.

Verwandte Themen

- Informationen zum Schutz Ihrer Root-Benutzeranmeldedaten finden Sie unter Sichern der Anmeldeinformationen für den Root-Benutzer im IAM-Benutzerhandbuch.
- Eine Liste der Aufgaben, für die der Root-Benutzer erforderlich ist, finden Sie im IAM-Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind.

Verwendung der Root-Benutzer des AWS-Kontos

> **Important**
>
> Jeder Benutzer, der Root-Benutzer-Anmeldeinformationen für Ihr AWS-Konto besitzt, hat uneingeschränkten Zugriff auf alle Ressourcen in Ihrem Konto, einschließlich Fakturierungsdaten.

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. 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.

Um zu vermeiden, dass der Root-Benutzer für alltägliche Aufgaben verwendet wird, erfahren Sie unter, wie Sie einen Administratorbenutzer einrichten AWS IAM Identity Center. Weitere Sicherheitsempfehlungen für Root-Benutzer finden Sie unter Bewährte Methoden für Root-Benutzer für Ihren AWS-Konto.

Sie können das Root-Benutzerkennwort ändern oder zurücksetzen und Zugriffsschlüssel (Zugriffsschlüssel-IDs und geheime Zugriffsschlüssel) für Ihren Root-Benutzer erstellen oder löschen. Hilfe bei der Anmeldung mit Ihrem Root-Benutzer finden Sie unter AWS Management Console Als Root-Benutzer anmelden im AWS Anmelde-Benutzerhandbuch.

Verwalte deineAWS-Konto

Dieser Abschnitt enthält Themen, in denen beschrieben wird, wie Sie IhrAWS-Konto.

> **Note**
>
> Wenn deinAWS-Kontowurde in Indien erstellt mitAmazon Internet Services Private Limited(AISPL), es gibt zusätzliche Überlegungen. Weitere Informationen finden Sie unter Konten in Indien verwalten.

Themen

- Erstellen Sie ein eigenständiges AWS-Konto
- Anzeigen von AWS-Konto Kennungen
- Aktualisieren des AWS-Konto Namens, der E-Mail-Adresse oder des Passworts für den Root-Benutzer
- Verständnis der API-Betriebsmodi
- Aktualisiere deineAWS-KontoKontaktinformationen
- Fragen zur Sicherheitsherausforderung aktualisieren
- Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann
- Erstelle oder aktualisiere deinen AWS-Konto Alias
- Abrechnung für IhreAWS-Konto
- Konten in Indien verwalten
- Schließe eine AWS-Konto

Erstellen Sie ein eigenständiges AWS-Konto

In diesem Thema wird beschrieben, wie Sie eine eigenständige Version erstellenAWS-Konto, die nicht von verwaltet wirdAWS Organizations. Wenn Sie ein Konto erstellen möchten, das Teil einer Organisation ist, die von verwaltet wirdAWS Organizations, finden Sie im AWS OrganizationsBenutzerhandbuch weitere Informationen unter Erstellen eines Mitgliedskontos in Ihrer Organisation.

Diese Anweisungen beziehen sich auf die Einrichtung eines AWS-Konto Kontos außerhalb Indiens. Informationen zum Erstellen eines Kontos in Indien finden Sie unterErstelle eineAWS-Kontomit AISPL.

AWS Management Console

So erstellen Sie ein AWS-Konto

1. Öffnen Sie die Amazon Web Services Services-Startseite.
2. Wählen Sie Create an AWS-Konto.

> **Note**
>
> Wenn Sie sich AWS vor Kurzem angemeldet haben, ist diese Option möglicherweise nicht verfügbar. Wählen Sie stattdessen Bei der Konsole anmelden aus. Wenn dann „Neues Konto erstellen“ AWS-Konto immer noch nicht angezeigt wird, wählen Sie zunächst Bei einem anderen Konto anmelden und dann Neues erstellen ausAWS-Konto.

3. Geben Sie Ihre Kontoinformationen ein und wählen Sie dann E-Mail-Adresse verifizieren aus. Dadurch wird ein Bestätigungscode an die von Ihnen angegebene E-Mail-Adresse gesendet.

> **Important**
>
> Aufgrund des kritischen Charakters des Root-Benutzers des Kontos empfehlen wir dringend, eine E-Mail-Adresse zu verwenden, auf die eine Gruppe und nicht nur eine Einzelperson zugreifen kann. Wenn die Person, für die sich angemeldet hat, das Unternehmen AWS-Konto verlässt, AWS-Konto kann sie auf diese Weise weiterhin verwendet werden, da die E-Mail-Adresse weiterhin zugänglich ist.
> Wenn Sie den Zugriff auf die mit dem verknüpfte E-Mail-Adresse verlierenAWS-Konto, können Sie den Zugriff auf das Konto nicht wiederherstellen, falls Sie jemals das Passwort verlieren.

4. Gib deinen Bestätigungscode ein und wähle dann Verifizieren.
5. Geben Sie ein sicheres Passwort für Ihren Root-Benutzer ein, bestätigen Sie es und wählen Sie dann Weiter. AWSsetzt voraus, dass Ihr Passwort die folgenden Bedingungen erfüllt:

   - Es muss mindestens 8 Zeichen und maximal 128 Zeichen lang sein.

- Es muss mindestens drei der folgenden Zeichentypen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und ! @ # $ % ^ & * () <> [] {} | _+-= Symbole.
- Es darf nicht identisch mit Ihrem AWS-Konto-Namen oder Ihrer E-Mail-Adresse sein.

6. Wählen Sie Geschäftlich oder Persönlich. Privatkonten und Geschäftskonten haben dieselben Merkmale und Funktionen.
7. Geben Sie Ihre Unternehmens- oder persönlichen Daten ein.

> **Important**
>
> Für Unternehmen AWS-Konten ist es eine bewährte Methode, Folgendes einzugeben:
>
> - Eine Firmentelefonnummer statt einer Nummer für ein Privattelefon.
> - Eine E-Mail-Adresse mit einem Domainnamen, der dem Unternehmen oder der Organisation gehört, die das Konto verwenden wird.
>
> Wenn Sie den Root-Benutzer des Kontos mit einer individuellen E-Mail-Adresse oder einer persönlichen Telefonnummer konfigurieren, kann Ihr Konto unsicher werden.

8. Lesen und akzeptieren Sie die AWSKundenvereinbarung. Stellen Sie sicher, dass Sie die Bedingungen der AWS Kundenvereinbarung gelesen und verstanden haben.
9. Klicken Sie auf Weiter. Zu diesem Zeitpunkt erhalten Sie eine E-Mail-Nachricht, in der bestätigt wird, dass Ihr AWS-Konto Gerät einsatzbereit ist. Sie können sich mit der E-Mail-Adresse und dem Passwort, die Sie bei der Registrierung angegeben haben, bei Ihrem neuen Konto anmelden. Sie können jedoch keine AWS Dienste nutzen, bis Sie die Aktivierung Ihres Kontos abgeschlossen haben.
10. Geben Sie die Informationen zu Ihrer Zahlungsmethode ein und wählen Sie dann Überprüfen und Fortfahren. Wenn Sie eine andere Rechnungsadresse für Ihre AWS Rechnungsinformationen verwenden möchten, wählen Sie Neue Adresse verwenden aus.

    Sie können mit dem Anmeldevorgang erst fortfahren, wenn Sie eine gültige Zahlungsmethode hinzugefügt haben.
11. Geben Sie Ihren Landes- oder Regionalcode aus der Liste ein und geben Sie dann eine Telefonnummer ein, unter der Sie in den nächsten Minuten erreichbar sind.
12. Geben Sie den im CAPTCHA angezeigten Code ein und senden Sie ihn ab.

13. Wenn das automatisierte System Sie kontaktiert, geben Sie die PIN ein, die Sie erhalten haben, und senden Sie sie dann ab.
14. Wählen Sie einen der verfügbaren AWS Support Pläne aus. Eine Beschreibung der verfügbaren Support-Pläne und ihrer Vorteile finden Sie unter AWS SupportTarife vergleichen.
15. Wählen Sie Registrierung abschließen aus. Eine Bestätigungsseite wird angezeigt, die darauf hinweist, dass Ihr Konto aktiviert wird.
16. Suchen Sie in Ihrem E-Mail- und Spam-Ordner nach einer E-Mail-Nachricht, die bestätigt, dass Ihr Konto aktiviert wurde. Die Aktivierung dauert normalerweise einige Minuten, kann aber manchmal bis zu 24 Stunden dauern.

    Nachdem Sie die Aktivierungsnachricht erhalten haben, haben Sie vollen Zugriff auf alle AWS Dienste.

AWS CLI & SDKs

Sie können Mitgliedskonten in einer Organisation erstellen, die von verwaltet wird, AWS Organizations indem Sie den CreateAccountVorgang ausführen, während Sie beim Verwaltungskonto der Organisation angemeldet sind.

Sie können kein eigenständiges Konto AWS-Konto außerhalb einer Organisation erstellen, indem Sie eine AWS Command Line Interface (AWS CLI) - oder AWS API-Operation verwenden.

Anzeigen von AWS-Konto Kennungen

AWS weist jedem die folgenden eindeutigen Kennungen zu AWS-Konto:

AWS-Konto ID (ID)

Eine 12-stellige Zahl, z. B. 012345678901, die ein eindeutig identifiziert AWS-Konto. Viele AWS Ressourcen enthalten die Konto-ID in ihren Amazon-Ressourcennamen (ARNs). Im Abschnitt „Konto-ID“ werden Ressourcen in einem Konto von den Ressourcen in einem anderen Konto unterschieden. Wenn Sie ein AWS Identity and Access Management (IAM)-Benutzer sind, können Sie sich entweder AWS Management Console mit der Konto-ID oder dem Kontoalias bei der anmelden. Konto-IDs sollten zwar wie alle identifizierenden Informationen verwendet und sorgfältig weitergegeben werden, sie gelten jedoch nicht als geheime, sensible oder vertrauliche Informationen.

Kanonische Benutzer-ID

Eine alphanumerische Kennung, z. B. `79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`, die eine verschleierte Form der AWS-Konto ID darstellt. Sie können diese ID verwenden, um ein zu identifizieren, AWS-Konto wenn Sie mit Amazon Simple Storage Service (Amazon S3) kontoübergreifenden Zugriff auf Buckets und Objekte gewähren. Sie können die kanonische Benutzer-ID für Ihr entweder AWS-Konto als Stammbenutzer oder als IAM-Benutzer abrufen.

Sie müssen bei authentifiziert sein AWS , um diese Kennungen anzeigen zu können.

> **Warning**
>
> Geben Sie Ihre - AWS Anmeldeinformationen (einschließlich Passwörtern und Zugriffsschlüsseln) nicht an Dritte weiter, die Ihre AWS-Konto Kennungen benötigen, um AWS Ressourcen für Sie freizugeben. Dies würde ihnen denselben Zugriff auf die gewähren AWS-Konto , die Sie haben.

Suchen Ihrer AWS-Konto -ID

Sie finden die AWS-Konto ID entweder mit der AWS Management Console oder der AWS Command Line Interface (AWS CLI). In der Konsole hängt der Speicherort der Konto-ID davon ab, ob Sie als Stammbenutzer oder als IAM-Benutzer angemeldet sind. Die Konto-ID ist identisch, unabhängig davon, ob Sie als Stammbenutzer oder als IAM-Benutzer angemeldet sind.

Suchen Ihrer Konto-ID als Root-Benutzer

AWS Management Console

So finden Sie Ihre AWS-Konto -ID, wenn Sie als Root-Benutzer angemeldet sind

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - Wenn Sie sich als Root-Benutzer anmelden, benötigen Sie keine IAM-Berechtigungen.

1. Wählen Sie in der Navigationsleiste oben rechts Ihren Kontonamen oder Ihre Kontonummer und dann Sicherheitsanmeldeinformationen aus.

   > **Tip**
   >
   > Wenn die Option Sicherheitsanmeldeinformationen nicht angezeigt wird, sind Sie möglicherweise als Verbundbenutzer mit einer IAM-Rolle und nicht als IAM-Benutzer angemeldet. Suchen Sie in diesem Fall nach dem Eintrag Konto und der Konto-ID-Nummer daneben.

2. Im Abschnitt Kontodetails wird die Kontonummer neben AWS-Konto ID angezeigt.

AWS CLI & SDKs

So finden Sie Ihre AWS-Konto -ID mithilfe der AWS CLI

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - Wenn Sie den Befehl als Root-Benutzer ausführen, benötigen Sie keine IAM-Berechtigungen.

Verwenden Sie den get-caller-identity-Befehl wie folgt:

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Suchen Ihrer Konto-ID als IAM-Benutzer

AWS Management Console

So finden Sie Ihre AWS-Konto -ID, wenn Sie als IAM-Benutzer angemeldet sind

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - `account:GetAccountInformation`

1. Wählen Sie auf der Navigationsleiste rechts oben Ihren Benutzernamen und dann Security Credentials (Sicherheitsanmeldeinformationen) aus.

   > **Tip**
   >
   > Wenn die Option Sicherheitsanmeldeinformationen nicht angezeigt wird, sind Sie möglicherweise als Verbundbenutzer mit einer IAM-Rolle und nicht als IAM-Benutzer angemeldet. Suchen Sie in diesem Fall nach dem Eintrag Konto und der Konto-ID-Nummer daneben.

2. Oben auf der Seite wird unter Kontodetails die Kontonummer neben AWS-Konto ID angezeigt.

AWS CLI & SDKs

So finden Sie Ihre AWS-Konto -ID mithilfe der AWS CLI

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - Wenn Sie den Befehl als IAM-Benutzer oder -Rolle ausführen, benötigen Sie Folgendes:
>   - `sts:GetCallerIdentity`

Verwenden Sie den get-caller-identity-Befehl wie folgt:

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Ermitteln der kanonischen Benutzer-ID für Ihr AWS-Konto

Sie finden die kanonische Benutzer-ID für Ihr AWS-Konto mithilfe der AWS Management Console oder der AWS CLI. Die kanonische Benutzer-ID für einen AWS-Konto ist für dieses Konto spezifisch. Sie können die kanonische Benutzer-ID für Ihr AWS-Konto als Stammbenutzer, Verbundbenutzer oder IAM-Benutzer abrufen.

Die kanonische ID als Stammbenutzer oder IAM-Benutzer finden

AWS Management Console

So finden Sie die kanonische Benutzer-ID für Ihr Konto, wenn Sie als Stammbenutzer oder IAM-Benutzer bei der Konsole angemeldet sind

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - Wenn Sie den Befehl als Root-Benutzer ausführen, benötigen Sie keine IAM-Berechtigungen.
> - Wenn Sie sich als IAM-Benutzer anmelden, benötigen Sie:
>   - `account:GetAccountInformation`

1. Melden Sie sich bei der AWS Management Console als Stammbenutzer oder IAM-Benutzer an.
2. Wählen Sie in der Navigationsleiste oben rechts Ihren Kontonamen oder Ihre Kontonummer und dann Sicherheitsanmeldeinformationen aus.

> **Tip**
>
> Wenn Sie die Option Sicherheitsanmeldeinformationen nicht sehen, sind Sie möglicherweise als Verbundbenutzer mit einer IAM-Rolle und nicht als IAM-Benutzer angemeldet. Suchen Sie in diesem Fall nach dem Eintrag Konto und der Konto-ID-Nummer daneben.

3. Im Abschnitt Kontodetails wird die kanonische Benutzer-ID neben Kanonische Benutzer-ID angezeigt. Sie können Ihre kanonische Benutzer-ID verwenden, um Amazon S3-Zugriffskontrolllisten (ACLs) zu konfigurieren.

AWS CLI & SDKs

So finden Sie die kanonische Benutzer-ID mithilfe der AWS CLI

Derselbe - AWS CLI und -API-Befehl funktioniert für die , Root-Benutzer des AWS-KontosIAM-Benutzer oder IAM-Rollen.

Verwenden Sie den Befehl list-buckets wie folgt.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Die kanonische ID als Verbundbenutzer mit einer IAM-Rolle finden

AWS Management Console

So finden Sie die kanonische ID für Ihr Konto, wenn Sie bei der Konsole als Verbundbenutzer mit einer IAM-Rolle angemeldet sind

> **Mindestberechtigungen**
>
> - Sie müssen über die Berechtigung zum Auflisten und Anzeigen eines Amazon S3-Buckets verfügen.

1. Melden Sie sich bei AWS Management Console als Verbundbenutzer mit einer IAM-Rolle an.
2. Wählen Sie in der Amazon S3-Konsole einen Bucket-Namen aus, um Details zu einem Bucket anzuzeigen.
3. Wählen Sie die Registerkarte Berechtigungen.
4. Im Abschnitt Zugriffskontrollliste wird unter Bucket-Eigentümer die kanonische ID für Ihr AWS-Konto angezeigt.

AWS CLI & SDKs

So finden Sie die kanonische Benutzer-ID mithilfe der AWS CLI

Derselbe - AWS CLI und -API-Befehl funktioniert für die , Root-Benutzer des AWS-KontosIAM-Benutzer oder IAM-Rollen.

Verwenden Sie den Befehl list-buckets wie folgt.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Aktualisieren des AWS-Konto Namens, der E-Mail-Adresse oder des Passworts für den Root-Benutzer

Um AWS-Kontoden Namen Ihres zu bearbeiten oder das Passwort oder die E-Mail-Adresse des Stammbenutzers zu ändern, führen Sie die folgenden Schritte aus. Diese E-Mail-Adresse und dieses Passwort sind die Anmeldeinformationen, mit denen Sie sich als anmeldenRoot-Benutzer des AWS-Kontos.

> **Note**
>
> Es AWS-Konto kann bis zu vier Stunden dauern, bis Änderungen an einem überall verbreitet sind.

AWS Management Console

So bearbeiten Sie Ihren AWS-Konto Namen, Ihr Stammbenutzerpasswort oder Ihre Stammbenutzer-E-Mail-Adresse

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - Sie müssen sich als anmeldenRoot-Benutzer des AWS-Kontos, was keine zusätzlichen IAM-Berechtigungen erfordert. Sie können diese Schritte nicht als IAM-Benutzer oder -Rolle ausführen.

1. Verwenden Sie die E-Mail-Adresse und AWS-Kontodas Passwort Ihres , um sich bei der AWS Management Console als Ihr anzumeldenRoot-Benutzer des AWS-Kontos.
2. Wählen Sie oben rechts in der Konsole Ihren Kontonamen oder Ihre Kontonummer und dann Account (Konto) aus.
3. Wählen Sie auf der Seite Konto, neben den Kontoeinstellungen, Bearbeiten aus. Aus Sicherheitsgründen werden Sie aufgefordert, sich erneut zu authentifizieren.

   > **Note**
   >
   > Wenn die Option Bearbeiten nicht angezeigt wird, sind Sie wahrscheinlich nicht als Root-Benutzer für Ihr Konto angemeldet. Sie können die Kontoeinstellungen nicht ändern, wenn Sie als IAM-Benutzer oder als IAM-Rolle angemeldet sind.

4. Wählen Sie auf der Seite Kontoeinstellungen aktualisieren neben dem Feld, das Sie aktualisieren möchten, die Option Bearbeiten aus.

   a. Geben Sie unter Name – Geben Sie auf der Seite Kontoname aktualisieren unter Neuer Kontoname den neuen Kontonamen ein und wählen Sie dann Änderungen speichern aus.

      > **Note**
      >
      > Wenn Sie den AWS-Konto Namen nicht ändern können, überprüfen Sie, ob eine Service-Kontrollrichtlinie (SCP) in vorhanden istAWS Organizations,

die den Zugriff auf einschränkt `account` oder so eingestellt ist, dass die `iam:UpdateAccountName` Aktion verweigert wird.

b. Für E-Mail – Füllen Sie auf der Seite Ihre E-Mail-Adresse aktualisieren die Felder Neue E-Mail-Adresse , Neue E-Mail-Adresse bestätigen aus und bestätigen Sie Ihr aktuelles Passwort . Dann wählen Sie Save changes (Änderungen speichern) aus. Ein Verifizierungscode wird von an Ihre neue E-Mail-Adresse gesendetno-`reply@verify.signin.aws`. Geben Sie auf der Seite Verifizieren Ihrer neuen E-Mail-Adresse unter Verifizierungscode den Code ein, den Sie von Ihrer E-Mail erhalten haben, und wählen Sie dann Änderungen speichern aus.

> **Note**
>
> Es kann bis zu 5 Minuten dauern, bis der Verifizierungscode eintrifft. Wenn Sie die E-Mail nicht in Ihrem Posteingang sehen, überprüfen Sie Ihre Spam- und Junk-Ordner.

c. Für Passwort – Füllen Sie auf der Seite Passwort aktualisieren die Felder Aktuelles Passwort , Neues Passwort und Neues Passwort bestätigen aus. Dann wählen Sie Save changes (Änderungen speichern) aus. Weitere Hinweise, einschließlich bewährter Methoden zum Festlegen von Root-Benutzerpasswörtern, finden Sie unter Ändern des Passworts für Root-Benutzer des AWS-Kontos im IAM-Benutzerhandbuch.

5. Nachdem Sie alle Änderungen durchgeführt haben, wählen Sie Fertig aus.

AWS CLI & SDKs

Diese Aufgabe wird in der AWS CLI oder durch eine API-Operation von einem der AWS-SDKs nicht unterstützt. Diese Aufgabe können Sie nur mit der AWS Management Console ausführen.

Verständnis der API-Betriebsmodi

Die API-Operationen, die mit einemAWS-Kontos Attribute funktionieren immer in einer von zwei Betriebsarten:

- Standalone-Kontext— Dieser Modus wird verwendet, wenn ein Benutzer oder eine Rolle in einem Konto auf ein Kontoattribut imgleiches -Kontoaus. Der eigenständige Kontextmodus wird

automatisch verwendet, wenn SieDon't (Nichtschließe das mit ein`AccountId`Parameter, wenn Sie eine der Account Management aufrufenAWS CLIoderAWSSDK-Operationen.

- Organisationskontext— Dieser Modus wird verwendet, wenn ein Benutzer oder eine Rolle in einem Konto in einer Organisation auf ein Kontoattribut in einem anderen Mitgliedskonto in derselben Organisation zugreift oder es ändert. Der Organisationskontextmodus wird automatisch verwendet, wenn Sietunschließe das mit ein`AccountId`Parameter, wenn Sie eine der Account Management aufrufenAWS CLIoderAWSSDK-Betrieb. Sie können die Vorgänge in diesem Modus nur über das Verwaltungskonto der Organisation oder das delegierte Administratorkonto für die Kontoverwaltung aufrufen.

DieAWS CLIundAWSSDK-Vorgänge können entweder im eigenständigen Kontext oder im Unternehmenskontext funktionieren.

- Wenn SieDon't (Nichtschließe das mit ein`AccountId`-Parameter, dann wird der Vorgang im eigenständigen Kontext ausgeführt und wendet die Anfrage automatisch auf das Konto an, mit dem Sie die Anfrage gestellt haben. Dies gilt unabhängig davon, ob das Konto Mitglied einer Organisation ist oder nicht.
- Wenn Sie das einbeziehen`AccountId`-Parameter, dann wird der Vorgang im Organisationskontext ausgeführt, und der Vorgang funktioniert mit dem angegebenen Organisationskonto.
  - Wenn das Konto, das den Vorgang aufruft, das Verwaltungskonto oder das delegierte Administratorkonto für den Account Management Service ist, können Sie ein beliebiges Mitgliedskonto dieser Organisation in der`AccountId`, um das angegebene -Konto zu aktualisieren.
  - Das einzige Konto in einer Organisation, das eine der alternativen Kontaktoperationen anrufen und seine eigene Kontonummer in der`AccountId`-Parameter ist das Konto, das alsdelegiertes Administratorkontofür den Account Management Service. Jedes andere Konto, einschließlich des Verwaltungskontos, erhält eine`AccessDenied`Ausnahme.
- Wenn Sie einen Vorgang im eigenständigen Modus ausführen, müssen Sie berechtigt sein, den Vorgang mit einer IAM-Richtlinie auszuführen, die eine`Resource`Element von entweder"*"um alle Ressourcen zuzulassen, oder einARN, der die Syntax für ein eigenständiges Konto verwendetaus.
- Wenn Sie einen Vorgang im Organisationsmodus ausführen, müssen Sie berechtigt sein, den Vorgang mit einer IAM-Richtlinie auszuführen, die eine`Resource`Element von entweder"*"um alle Ressourcen zuzulassen, oder einARN, der die Syntax für ein Mitgliedskonto in einer Organisation verwendetaus.

Berechtigungen zum Aktualisieren von Kontoattributen gewähren

Wie bei den meistenAWS-Vorgängen gewähren Sie Berechtigungen zum Hinzufügen, Aktualisieren oder Löschen von Kontoattributen fürAWS-Kontendurch Verwendung von-IAM-Berechtigungsrichtlinienaus. Wenn Sie eine IAM-Berechtigungsrichtlinie an einen IAM-Prinzipal (entweder einen Benutzer oder eine Rolle) anhängen, geben Sie an, welche Aktionen dieser Prinzipal für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Im Folgenden finden Sie einige spezifische Überlegungen zur Kontoverwaltung beim Erstellen einer Berechtigungsrichtlinie.

Format des Amazon-Ressourcennamens fürAWS-Konten

- DieAmazon Resource Name (ARN, Amazon-Ressourcenname)für einAWS-Kontodie Sie in die`resource`-Element einer Richtlinienerklärung ist unterschiedlich aufgebaut, je nachdem, ob es sich bei dem Konto, auf das Sie verweisen möchten, um ein eigenständiges Konto oder um ein Konto handelt, das sich in einer Organisation befindet. Informationen finden Sie im vorherigen Abschnitt überVerständnis der API-Betriebsmodiaus.

  - Ein Konto-ARN für ein eigenständiges Konto:

    ```
    arn:aws:account::{AccountId}:account
    ```

    Sie müssen dieses Format verwenden, wenn Sie einen Vorgang mit Kontoattributen im Standalone-Modus ausführen, indem Sie das`AccountID`-Parameter.

  - Ein Konto-ARN für ein Mitgliedskonto in einer Organisation:

    ```
    arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
    ```

    Sie müssen dieses Format verwenden, wenn Sie einen Vorgang mit Kontoattributen im Organisationsmodus ausführen, indem Sie das`AccountID`-Parameter.

Kontextschlüssel für IAM-Richtlinien

Der Account Management Service bietet auch mehrereService-spezifische Bedingungsschlüssel für die Kontoverwaltungdie eine genaue Kontrolle über die von Ihnen erteilten Berechtigungen bieten.

`account:AccountResourceOrgPaths`

Der Kontext-Schlüssel`account:AccountResourceOrgPaths`können Sie einen Pfad durch die Hierarchie Ihrer Organisation zu einer bestimmten Organisationseinheit (OU) angeben. Nur Mitgliedskonten, die in dieser OU enthalten sind, erfüllen die Bedingung. Das folgende Beispiel-Snippet schränkt die Richtlinie so ein, dass sie nur für Konten gilt, die sich in einer von zwei angegebenen Organisationseinheiten befinden.

Da es sich bei`account:AccountResourceOrgPaths`ist ein mehrwertiger String-Typ, müssen Sie den`ForAnyValue`oder`ForAllValues`String-Operatoren mit mehreren aus. Beachten Sie außerdem, dass das Präfix für den Bedingungsschlüssel`account`, obwohl Sie Pfade zu Organisationseinheiten in einer Organisation referenzieren.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

`account:AccountResourceOrgTags`

Der Kontext-Schlüssel`account:AccountResourceOrgTags`können Sie auf die Tags verweisen, die an ein Konto in einer Organisation angehängt werden können. Ein Tag ist ein Schlüssel/Wert-Zeichenfolgenpaar, das Sie verwenden können, um die Ressourcen in Ihrem Konto zu kategorisieren und zu kennzeichnen. Weitere Informationen über das Markieren mit Tags finden Sie unter Tag-Editor im AWS Resource Groups Benutzerhandbuch aus. Informationen zur Verwendung von Tags als Teil einer attributbasierten Zugriffskontrollstrategie finden Sie unter Wofür wird ABAC in verwendet AWS im IAM User Guide aus. Das folgende Beispiel-Snippet schränkt die Richtlinie so ein, dass sie nur für Konten in einer Organisation gilt, die das Tag mit dem Schlüssel haben`project`und ein Wert von`blue`oder`red`aus.

Da es sich bei`account:AccountResourceOrgTags`ist ein mehrwertiger String-Typ, müssen Sie den`ForAnyValue`oder`ForAllValues`String-Operatoren mit mehreren aus. Beachten Sie außerdem, dass das Präfix für den Bedingungsschlüssel`account`, obwohl Sie auf die Tags im Mitgliedskonto einer Organisation verweisen.

```
"Condition": {
```

```
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> Sie können Tags nur an ein Konto in einer Organisation anhängen. Sie können keine Tags an ein Standalone anhängenAWS-Kontoaus.

Aktualisiere deineAWS-KontoKontaktinformationen

Sie können Kontaktinformationen über die speichernprimärer Kontokontaktfür deinAWS-Konto. Sie können auch Kontaktinformationen für Folgendes hinzufügen oder bearbeitenalternative Kontokontakte:

- Abrechnung— Der alternative Ansprechpartner für die Rechnungsstellung erhält Benachrichtigungen im Zusammenhang mit der Rechnungsstellung, z. B. Benachrichtigungen zur Verfügbarkeit von Rechnungen.
- Operationen— Der alternative Ansprechpartner für den Betrieb erhält betriebliche Benachrichtigungen.
- Sicherheit— Der alternative Sicherheitskontakt erhält sicherheitsrelevante Benachrichtigungen, einschließlich Benachrichtigungen von derAWSMissbrauchsteam.

Themen

- Aktualisieren Sie die alternativen Kontakte für Ihr AWS-Konto
- Aktualisieren des primären Kontakts für Ihr AWS-Konto

Aktualisieren Sie die alternativen Kontakte für Ihr AWS-Konto

Alternative Kontakte ermöglichen es AWS , bis zu drei alternative Kontakte zu kontaktieren, die dem Konto zugeordnet sind. Ein alternativer Kontakt muss keine bestimmte Person sein. Sie können stattdessen eine E-Mail-Verteilerliste hinzufügen, wenn Sie über ein Team verfügen, das

Abrechnungs-, Betriebs- und Sicherheitsprobleme verwaltet. Diese gelten zusätzlich zu der E-Mail-Adresse, die dem Root-Benutzer des Kontos zugeordnet ist. Der primäre Kontokontakt erhält weiterhin alle E-Mail-Kommunikationen, die an die E-Mail des Stammkontos gesendet werden.

Sie können nur einen der folgenden Kontakttypen angeben, die einem Konto zugeordnet sind.

- Fakturierungskontakt
- Betriebskontakt
- Sicherheitskontakt

Sie können alternative Kontakte unterschiedlich hinzufügen oder bearbeiten, je nachdem, ob die Konten eigenständig oder Teil einer Organisation sind oder nicht:

- Eigenständig AWS-Konten – Wenn Sie AWS-Konten keiner Organisation zugeordnet sind, können Sie Ihre eigenen alternativen Kontakte mithilfe der -AWSManagementkonsole oder über AWS CLI und SDKs aktualisieren. Informationen dazu finden Sie unter Aktualisieren eigenständiger AWS-Konto alternativer Kontakte.
- AWS-Konten innerhalb einer Organisation – Für Mitgliedskonten, die Teil einer AWS Organisation sind, kann ein Benutzer im Verwaltungskonto oder im Konto eines delegierten Administrators jedes Mitgliedskonto in der Organisation zentral über die AWS OrganizationsKonsole oder programmgesteuert über die AWS CLI und SDKs aktualisieren. Informationen dazu finden Sie unter Aktualisieren AWS-Konto alternativer Kontakte in Ihrer Organisation.

Themen

- Anforderungen an Telefonnummern und E-Mail-Adressen
- Aktualisieren der alternativen Kontakte für ein eigenständiges AWS-Konto
- Aktualisieren Sie die alternativen Kontakte für alle AWS-Konto in Ihrer Organisation
- Konto:AlternateContactTypes Kontextschlüssel

Anforderungen an Telefonnummern und E-Mail-Adressen

Bevor Sie mit der Aktualisierung der alternativen Kontaktinformationen Ihres Kontos fortfahren, empfehlen wir Ihnen, bei der Eingabe von Telefonnummern und E-Mail-Adressen zunächst die folgenden Anforderungen zu überprüfen.

- Telefonnummern dürfen nur Zahlen, Leerzeichen und die folgenden Zeichen enthalten: „+ - ( )“.

- E-Mail-Adressen können bis zu 254 Zeichen lang sein und zusätzlich zu den standardmäßigen alphanumerischen Zeichen die folgenden Sonderzeichen im lokalen Teil der E-Mail-Adresse enthalten: „+=.#|!&-_“.

Aktualisieren der alternativen Kontakte für ein eigenständiges AWS-Konto

Um die alternativen Kontakte für ein eigenständiges hinzuzufügen oder zu bearbeitenAWS-Konto, führen Sie die Schritte im folgenden Verfahren aus. Das folgende AWS Management Console Verfahren funktioniert immer nur im eigenständigen Kontext. Sie können die verwendenAWS Management Console, um nur auf die alternativen Kontakte in dem Konto zuzugreifen oder diese zu ändern, mit dem Sie die Operation aufgerufen haben.

AWS Management Console

So fügen Sie alternative Kontakte für ein eigenständiges hinzu oder bearbeiten sie AWS-Konto

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - `account:GetAlternateContact` (um die alternativen Kontaktdaten anzuzeigen)
> - `account:PutAlternateContact` (um einen alternativen Kontakt festzulegen oder zu aktualisieren)
> - `account:DeleteAlternateContact` (um einen alternativen Kontakt zu löschen)

1. Melden Sie sich bei AWS Management Console als IAM-Benutzer oder -Rolle an, die über die Mindestberechtigungen verfügt.
2. Wählen Sie oben rechts im Fenster Ihren Kontonamen und dann Konto aus.
3. Scrollen Sie auf der Seite Konto nach unten zu Alternative Kontakte und wählen Sie rechts neben dem Titel Bearbeiten aus.

> **Note**
>
> Wenn Sie die Option Bearbeiten nicht sehen, sind Sie wahrscheinlich nicht als Root-Benutzer für Ihr Konto oder als jemand angemeldet, der über die oben angegebenen Mindestberechtigungen verfügt.

4. Ändern Sie die Werte in einem der verfügbaren Felder.

> **Important**
>
> Für Unternehmen ist es eine bewährte MethodeAWS-Konten, eine Unternehmenstelefonnummer und E-Mail-Adresse einzugeben, nicht eine, die zu einer Person gehört.

5. Nachdem Sie alle Ihre Änderungen vorgenommen haben, wählen Sie Aktualisieren aus.

AWS CLI & SDKs

Sie können die alternativen Kontaktinformationen mithilfe der folgenden AWS CLI Befehle oder ihrer entsprechenden AWS SDK-Operationen abrufen, aktualisieren oder löschen:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Hinweise**
>
> - Um diese Vorgänge über das Verwaltungskonto oder ein delegiertes Administratorkonto in einer Organisation für Mitgliedskonten auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoservice aktivieren.

> **Mindestberechtigungen**
>
> Für jede Operation benötigen Sie die -Berechtigung, die dieser Operation zugeordnet ist:

- `GetAlternateContact` (um die alternativen Kontaktdaten anzuzeigen)
- `PutAlternateContact` (um einen alternativen Kontakt festzulegen oder zu aktualisieren)
- `DeleteAlternateContact` (um einen alternativen Kontakt zu löschen)

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern die Möglichkeit geben, nur die Kontaktinformationen zu lesen, und anderen die Möglichkeit geben, sowohl zu lesen als auch zu schreiben.

Example

Im folgenden Beispiel wird der aktuelle alternative Fakturierungskontakt für das Konto des Anrufers abgerufen.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Im folgenden Beispiel wird ein neuer alternativer Operations-Kontakt für das Konto des Anrufers eingerichtet.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
```

```
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Example

> **Note**
>
> Wenn Sie mehrere `PutAlternateContact` Operationen für denselben AWS-Konto und denselben Kontakttyp ausführen, fügt der erste den neuen Kontakt hinzu, und alle aufeinanderfolgenden Aufrufe desselben AWS-Konto und desselben Kontakttyps aktualisieren den vorhandenen Kontakt.

Example

Im folgenden Beispiel wird der alternative Sicherheitskontakt für das Konto des Anrufers gelöscht.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

> **Note**
>
> Wenn Sie versuchen, denselben Kontakt mehr als einmal zu löschen, ist der erste im Hintergrund erfolgreich. Alle späteren Versuche erzeugen eine `ResourceNotFound` Ausnahme.

Aktualisieren Sie die alternativen Kontakte für alle AWS-Konto in Ihrer Organisation

Um die alternativen Kontaktdaten für einen AWS-Konto in Ihrer Organisation hinzuzufügen oder zu bearbeiten, führen Sie die Schritte im folgenden Verfahren aus.

Voraussetzungen

Um alternative Kontakte mit der AWS Organizations Konsole zu aktualisieren, müssen Sie einige vorbereitende Einstellungen vornehmen:

- Ihre Organisation muss alle Funktionen aktivieren, um Einstellungen für Ihre Mitgliedskonten zu verwalten. Dies ermöglicht die Admin-Kontrolle über die Mitgliedskonten. Dies wird standardmäßig festgelegt, wenn Sie Ihre Organisation erstellen. Wenn Ihre Organisation nur auf konsolidierte Fakturierung eingestellt ist und Sie alle Funktionen aktivieren möchten, finden Sie weitere Informationen unter Aktivieren aller Funktionen in Ihrer Organisation.
- Sie müssen den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsservice aktivieren. Informationen zum Einrichten finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs für die AWS Kontoverwaltung.

> **Note**
>
> Die AWS Organizations verwalteten Richtlinien `AWSOrganizationsReadOnlyAccess` oder `AWSOrganizationsFullAccess` werden aktualisiert, um die Berechtigung für den Zugriff auf die AWS Kontoverwaltungs-APIs zu erteilen, sodass Sie über die AWS Organizations Konsole auf Kontodaten zugreifen können. Informationen zum Anzeigen der aktualisierten verwalteten Richtlinien finden Sie unter Aktualisierungen der von Organizations AWS verwalteten Richtlinien.

AWS Management Console

So fügen Sie alternative Kontakte für AWS-Konto in Ihrer Organisation hinzu oder bearbeiten sie

1. Melden Sie sich bei der -AWS OrganizationsKonsole mit den Anmeldeinformationen des Verwaltungskontos der Organisation an.
2. Wählen Sie unter das Konto AWS-Kontenaus, das Sie aktualisieren möchten.
3. Wählen Sie Kontaktinformationen aus und suchen Sie unter Alternative Kontakte nach der Art des Kontakts: Fakturierungskontakt, Sicherheitskontakt oder Betriebskontakt.
4. Um einen neuen Kontakt hinzuzufügen, wählen Sie Hinzufügen aus, oder um einen vorhandenen Kontakt zu aktualisieren, wählen Sie Bearbeiten aus.
5. Ändern Sie die Werte in einem der verfügbaren Felder.

> **Important**
>
> Für Unternehmen ist es eine bewährte MethodeAWS-Konten, eine Unternehmenstelefonnummer und E-Mail-Adresse einzugeben, nicht eine, die zu einer Person gehört.

6. Nachdem Sie alle Ihre Änderungen vorgenommen haben, wählen Sie Aktualisieren aus.

AWS CLI & SDKs

Sie können die alternativen Kontaktinformationen mithilfe der folgenden AWS CLI Befehle oder ihrer entsprechenden AWS SDK-Operationen abrufen, aktualisieren oder löschen:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Hinweise**
>
> - Um diese Vorgänge vom Verwaltungskonto oder einem delegierten Administratorkonto in einer Organisation anhand von Mitgliedskonten aus auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoservice aktivieren.
> - Sie können nicht auf ein Konto in einer anderen Organisation als das zugreifen, das Sie zum Aufrufen der -Operation verwenden.

> **Mindestberechtigungen**
>
> Für jede Operation benötigen Sie die -Berechtigung, die dieser Operation zugeordnet ist:
>
> - `GetAlternateContact` (um die alternativen Kontaktdaten anzuzeigen)
> - `PutAlternateContact` (um einen alternativen Kontakt festzulegen oder zu aktualisieren)

- `DeleteAlternateContact` (um einen alternativen Kontakt zu löschen)

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern die Möglichkeit geben, nur die Kontaktinformationen zu lesen, und anderen die Möglichkeit geben, sowohl zu lesen als auch zu schreiben.

Example

Im folgenden Beispiel wird der aktuelle alternative Fakturierungskontakt für das Konto des Anrufers in einer Organisation abgerufen. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

Im folgenden Beispiel wird der alternative Operations-Kontakt für das angegebene Mitgliedskonto in einer Organisation festgelegt. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
```

```
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

> **Note**
>
> Wenn Sie mehrere `PutAlternateContact` Operationen für denselben AWS-Konto und denselben Kontakttyp ausführen, fügt der erste den neuen Kontakt hinzu, und alle aufeinanderfolgenden Aufrufe desselben AWS-Konto und desselben Kontakttyps aktualisieren den vorhandenen Kontakt.

Example

Im folgenden Beispiel wird der alternative Sicherheitskontakt für das angegebene Mitgliedskonto in einer Organisation gelöscht. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Example

> **Note**
>
> Wenn Sie versuchen, denselben Kontakt mehr als einmal zu löschen, ist der erste im Hintergrund erfolgreich. Alle späteren Versuche erzeugen eine `ResourceNotFound` Ausnahme.

Konto:AlternateContactTypes Kontextschlüssel

Sie können den Kontextschlüssel verwenden, `account:AlternateContactTypes` um anzugeben, welche der drei Fakturierungstypen von der IAM-Richtlinie zugelassen (oder abgelehnt)

wird. Die folgende Beispiel-IAM-Berechtigungsrichtlinie verwendet diesen Bedingungsschlüssel, um es den angefügten Prinzipalen zu ermöglichen, nur den `BILLING` alternativen Kontakt für ein bestimmtes Konto in einer Organisation abzurufen, aber nicht zu ändern.

Da es sich um einen mehrwertigen Zeichenfolgentyp `account:AlternateContactTypes` handelt, müssen Sie die `ForAnyValue` Zeichenfolgenoperatoren oder mit `ForAllValues` mehreren Werten verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

Aktualisieren des primären Kontakts für Ihr AWS-Konto

Sie können die mit Ihrem Konto verknüpften primären Kontaktinformationen aktualisieren, einschließlich des vollständigen Namens, des Unternehmensnamens, der E-Mail-Adresse, der Telefonnummer und der Website-Adresse.

Sie bearbeiten den primären Kontokontakt unterschiedlich, je nachdem, ob die Konten eigenständig oder Teil einer Organisation sind oder nicht:

- Eigenständig AWS-Konten – Wenn Sie AWS-Konten keiner Organisation zugeordnet sind, können Sie Ihren eigenen primären Kontokontakt mithilfe der -AWSManagementkonsole oder

über AWS CLI und SDKs aktualisieren. Informationen dazu finden Sie unter Aktualisieren eines eigenständigen AWS-Konto primären Kontakts.

- AWS-Konten innerhalb einer Organisation – Für Mitgliedskonten, die Teil einer AWS Organisation sind, kann ein Benutzer im Verwaltungskonto oder im Konto eines delegierten Administrators jedes Mitgliedskonto in der Organisation zentral über die AWS OrganizationsKonsole oder programmgesteuert über die AWS CLI und SDKs aktualisieren. Informationen dazu finden Sie unter Aktualisieren des AWS-Konto primären Kontakts in Ihrer Organisation.

Themen

- Anforderungen an Telefonnummern und E-Mail-Adressen
- Aktualisieren des primären Kontakts für ein eigenständiges AWS-Konto
- Aktualisieren des primären Kontakts für alle AWS-Konto in Ihrer Organisation

Anforderungen an Telefonnummern und E-Mail-Adressen

Bevor Sie mit der Aktualisierung der primären Kontaktinformationen Ihres Kontos fortfahren, empfehlen wir Ihnen, bei der Eingabe von Telefonnummern und E-Mail-Adressen zunächst die folgenden Anforderungen zu überprüfen.

- Telefonnummern dürfen nur Zahlen, Leerzeichen und die folgenden Zeichen enthalten: „+ - ( )“.
- Telefonnummern müssen mit einem + und einer Landesvorwahl beginnen und dürfen nach der Landesvorwahl keine führenden Nullen oder zusätzlichen Leerzeichen aufweisen. Zum Beispiel +1 (USA/Kanada) oder +44 (UK).
- Telefonnummern sollten Bindestriche „-“ zwischen der Vorwahl, der Austauschvorwahl und der lokalen Vorwahl enthalten. Zum Beispiel +1 202-555-0179.

> **Note**
>
> Telefonnummern, die ohne Bindestriche eingegeben wurden, können dazu führen, dass während des Verifizierungsprozesses für Telefonnummern beim Zurücksetzen eines MFA-Geräts für den Root-Benutzer keine Anrufe empfangen werden können. Weitere Informationen finden Sie unter Wie setze ich mein MFA-Gerät für das AWS Stammbenutzerkonto zurück?.

- Aus Sicherheitsgründen müssen Telefonnummern in der Lage sein, SMS von zu empfangenAWS. Gebührenfreie Nummern werden nicht akzeptiert, da die meisten SMS nicht unterstützen.

- Für Unternehmen ist es eine bewährte MethodeAWS-Konten, eine Unternehmenstelefonnummer und E-Mail-Adresse einzugeben, anstatt eine Adresse einer Person einzugeben. Die Konfiguration des Stammbenutzers des Kontos mit der E-Mail-Adresse oder Telefonnummer einer Person kann die Wiederherstellung Ihres Kontos erschweren, wenn diese Person das Unternehmen verlässt.

Aktualisieren des primären Kontakts für ein eigenständiges AWS-Konto

Führen Sie die folgenden Schritte ausAWS-Konto, um Ihre primären Kontaktdaten für ein eigenständiges zu bearbeiten. Das folgende AWS Management Console Verfahren funktioniert immer nur im eigenständigen Kontext. Sie können die verwendenAWS Management Console, um nur auf die primären Kontaktinformationen des Kontos zuzugreifen oder diese zu ändern, das Sie zum Aufrufen der -Operation verwendet haben.

AWS Management Console

So bearbeiten Sie Ihren primären Kontakt für ein eigenständiges AWS-Konto

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - `account:GetContactInformation` (um die primären Kontaktdaten anzuzeigen)
> - `account:PutContactInformation` (um die primären Kontaktdaten zu aktualisieren)

1. Melden Sie sich bei AWS Management Console als IAM-Benutzer oder -Rolle an, die über die Mindestberechtigungen verfügt.
2. Wählen Sie oben rechts im Fenster Ihren Kontonamen und dann Konto aus.
3. Scrollen Sie nach unten zum Abschnitt Kontaktinformationen und wählen Sie dann Bearbeiten aus.
4. Ändern Sie die Werte in einem der verfügbaren Felder.
5. Nachdem Sie alle Ihre Änderungen vorgenommen haben, wählen Sie Aktualisieren aus.

AWS CLI & SDKs

Sie können die primären Kontaktinformationen mithilfe der folgenden AWS CLI Befehle oder ihrer entsprechenden AWS SDK-Operationen abrufen, aktualisieren oder löschen:

- GetContactInformation
- PutContactInformation

> **Hinweise**
>
> - Um diese Vorgänge vom Verwaltungskonto oder einem delegierten Administratorkonto in einer Organisation anhand von Mitgliedskonten aus auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoservice aktivieren.

> **Mindestberechtigungen**
>
> Für jede Operation benötigen Sie die -Berechtigung, die dieser Operation zugeordnet ist:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern die Möglichkeit geben, nur die Kontaktinformationen zu lesen, und anderen die Möglichkeit geben, sowohl zu lesen als auch zu schreiben.

Example

Im folgenden Beispiel werden die aktuellen primären Kontaktinformationen für das Konto des Anrufers abgerufen.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
```

```
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Im folgenden Beispiel werden neue primäre Kontaktinformationen für das Konto des Anrufers festgelegt.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Aktualisieren des primären Kontakts für alle AWS-Konto in Ihrer Organisation

Um Ihre primären Kontaktdaten in einer AWS-Konto in Ihrer Organisation zu bearbeiten, führen Sie die Schritte im folgenden Verfahren aus.

Zusätzliche Anforderungen

Um den primären Kontakt mit der AWS Organizations Konsole zu aktualisieren, müssen Sie einige vorbereitende Einstellungen vornehmen:

- Ihre Organisation muss alle Funktionen aktivieren, um Einstellungen für Ihre Mitgliedskonten zu verwalten. Dies ermöglicht die Admin-Kontrolle über die Mitgliedskonten. Dies wird standardmäßig festgelegt, wenn Sie Ihre Organisation erstellen. Wenn Ihre Organisation nur auf konsolidierte Fakturierung eingestellt ist und Sie alle Funktionen aktivieren möchten, finden Sie weitere Informationen unter Aktivieren aller Funktionen in Ihrer Organisation.

- Sie müssen den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsservice aktivieren. Informationen zum Einrichten finden Sie unter Aktivieren des vertrauenswürdigen Zugriffs für die AWS Kontoverwaltung.

AWS Management Console

So bearbeiten Sie Ihren primären Kontakt für einen AWS-Konto in Ihrer Organisation

1. Melden Sie sich bei der -AWS OrganizationsKonsole mit den Anmeldeinformationen des Verwaltungskontos der Organisation an.
2. Wählen Sie unter das Konto AWS-Kontenaus, das Sie aktualisieren möchten.
3. Wählen Sie Kontaktinformationen und suchen Sie nach Primärer Kontakt ,
4. Wählen Sie Bearbeiten aus.
5. Ändern Sie die Werte in einem der verfügbaren Felder.
6. Nachdem Sie alle Ihre Änderungen vorgenommen haben, wählen Sie Aktualisieren aus.

AWS CLI & SDKs

Sie können die primären Kontaktinformationen mithilfe der folgenden AWS CLI Befehle oder ihrer entsprechenden AWS SDK-Operationen abrufen, aktualisieren oder löschen:

- GetContactInformation
- PutContactInformation

> **Hinweise**
>
> - Um diese Vorgänge vom Verwaltungskonto oder einem delegierten Administratorkonto in einer Organisation anhand von Mitgliedskonten aus auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoservice aktivieren.
> - Sie können nicht auf ein Konto in einer anderen Organisation als dem zugreifen, das Sie zum Aufrufen der -Operation verwenden.

Mindestberechtigungen

Für jede Operation benötigen Sie die -Berechtigung, die dieser Operation zugeordnet ist:

- `account:GetContactInformation`
- `account:PutContactInformation`

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern die Möglichkeit geben, nur die Kontaktinformationen zu lesen, und anderen die Möglichkeit geben, sowohl zu lesen als auch zu schreiben.

Example

Im folgenden Beispiel werden die aktuellen primären Kontaktinformationen für das angegebene Mitgliedskonto in einer Organisation abgerufen. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account get-contact-information --account-id 123456789012
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

Im folgenden Beispiel werden die primären Kontaktinformationen für das angegebene Mitgliedskonto in einer Organisation festgelegt. Die verwendeten Anmeldeinformationen müssen

entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Fragen zur Sicherheitsherausforderung aktualisieren

Sicherheitsabfragen sind zuvor eine Überprüfungsmethode zur Überprüfung einer Identität in Szenarien zur Kontowiederherstellung. Sie sind weniger sicher als moderne Formen der Verifizierung, z. B. Multi-Faktor-Authentifizierung (MFA). Wenn derzeit Sicherheitsfragen auf Ihrem aktiv sindAWS-Konto, AWS Support kann diese verwenden, um Sie als Besitzer des Kontos zu authentifizieren.

> **Important**
>
> Ab dem 5. Januar 2024 unterstützt AWS keine Sicherheitsfragen mehr für Konten, die sie noch nicht aktiviert und verwendet haben. Dadurch wird die Option entfernt, neue Sicherheitsabfragen von der Seite Konten im hinzufügenAWS Management Console. Wenn Sie bereits Fragen zur Sicherheitsherausforderung oder zum Verwaltungskonto in Ihrer AWS Organisation festgelegt haben, können Sie diese weiterhin verwenden. Nach dem 6. Januar 2025 unterstützt AWS keine Sicherheitsfragen mehr für alle verbleibenden Kunden. Wir empfehlen Ihnen, stattdessen MFA hinzuzufügen. Weitere Informationen finden Sie unter AWS Konten beendet die Verwendung von Sicherheitsabfragen.

Führen Sie die Schritte im folgenden Verfahren aus, um bestehende Sicherheitsabfragen zu bearbeiten und Antworten bereitzustellen.

AWS Management Console

So bearbeiten Sie Sicherheitsfragen für Ihr AWS-Konto

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - `account:GetChallengeQuestions` (um die Sicherheitsfragen anzuzeigen)
> - `account:PutChallangeQuestions` (um die Sicherheitsabfragen festzulegen oder zu aktualisieren)

1. Melden Sie sich bei der AWS Management Console als Root-Benutzer des AWS-Kontos oder als IAM-Benutzer oder -Rolle an, die über die Mindestberechtigungen verfügt.
2. Wählen Sie oben rechts im Fenster Ihren Kontonamen und dann Konto aus.
3. Scrollen Sie nach unten zum Abschnitt Sicherheitsabfragen und wählen Sie Bearbeiten aus.

   > **Note**
   >
   > Wenn Sie die Option Bearbeiten nicht sehen, sind Sie wahrscheinlich nicht als Stammbenutzer für Ihr Konto oder als jemand angemeldet, der über die oben angegebenen Mindestberechtigungen verfügt.

4. Ändern Sie die Werte in einem der verfügbaren Felder. Sie können eine der bereitgestellten Fragen auswählen und dann die entsprechende Antwort eingeben.
5. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie Aktualisieren aus.

AWS CLI & SDKs

Diese Aufgabe wird in der AWS CLI oder durch eine API-Operation von einem der AWS-SDKs nicht unterstützt. Diese Aufgabe können Sie nur mit der AWS Management Console ausführen.

Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann

An AWS-Regionist ein physischer Standort auf der Welt, an dem wir mehrere Availability Zones haben. Availability Zones bestehen aus einem oder mehreren diskreten AWS Rechenzentren, die

jeweils über redundante Stromversorgung, Netzwerke und Konnektivität verfügen und in separaten Einrichtungen untergebracht sind. Das bedeutet, AWS-Region dass jede Region physisch isoliert und unabhängig von den anderen Regionen ist. Regionen bieten Fehlertoleranz, Stabilität und Ausfallsicherheit und können auch die Latenz verkürzen. Eine Karte der aktuell und demnächst verfügbaren Regionen finden Sie unter Regionen und Availability Zones.

Die Ressourcen, die Sie in einer Region erstellen, sind in keiner anderen Region vorhanden, es sei denn, Sie verwenden ausdrücklich eine von einem AWS Dienst angebotene Replikationsfunktion. Beispielsweise unterstützen Amazon S3 und Amazon EC2 die regionsübergreifende Replikation. Einige Dienste, wie z. B. AWS Identity and Access Management (IAM), verfügen nicht über regionale Ressourcen.

Ihr Konto bestimmt die Regionen, die für Sie verfügbar sind.

- An AWS-Konto stellt mehrere Regionen bereit, sodass Sie AWS Ressourcen an Standorten einsetzen können, die Ihren Anforderungen entsprechen. Möglicherweise möchten Sie Amazon EC2 EC2-Instances in Europa starten, um näher an Ihren europäischen Kunden zu sein oder um gesetzliche Anforderungen zu erfüllen.
- Ein Konto AWS GovCloud (USA West) bietet Zugriff auf die Regionen AWS GovCloud (USA West) und die Region AWS GovCloud (USA Ost). Weitere Informationen finden Sie unter AWS GovCloud (US).
- Ein Amazon-Konto AWS (China) bietet nur Zugriff auf die Regionen Peking und Ningxia. Weitere Informationen finden Sie unter Amazon Web Services in China.

Eine Liste der Regionsnamen und der entsprechenden Codes finden Sie unter Regionale Endpunkte im AWS Allgemeinen Referenzhandbuch. Eine Liste der in den einzelnen Regionen unterstützten AWS Dienste (ohne Endpunkte) finden Sie in der Liste der AWS regionalen Dienste.

> **Important**
>
> AWS empfiehlt, regionale AWS Security Token Service (AWS STS) Endpunkte anstelle des globalen Endpunkts zu verwenden, um die Latenz zu reduzieren. Sitzungstoken von regionalen AWS STS Endpunkten sind in allen AWS Regionen gültig. Wenn Sie regionale AWS STS Endpunkte verwenden, müssen Sie keine Änderungen vornehmen. Sitzungstoken vom globalen AWS STS Endpunkt (https://sts.amazonaws.com) sind jedoch nur gültig AWS-Regionen , wenn Sie sie aktivieren oder die standardmäßig aktiviert sind. Wenn Sie beabsichtigen, eine neue Region für Ihr Konto zu aktivieren, können Sie entweder Sitzungstoken von regionalen AWS STS Endpunkten verwenden oder den globalen

AWS STS Endpunkt aktivieren, um Sitzungstoken auszugeben, die insgesamt AWS-Regionen gültig sind. Sitzungstoken, die in allen Regionen gültig sind, sind größer. Wenn Sie Sitzungstoken speichern, können sich diese größeren Token auf Ihre Systeme auswirken. Weitere Informationen zur Funktionsweise von AWS STS Endpunkten mit AWS Regionen finden Sie unter Verwaltung AWS STS in einer AWS Region.

Themen

- Überlegungen vor dem Aktivieren und Deaktivieren von Regionen
- Aktiviere oder deaktiviere eine Region für eigenständige Konten
- Aktivieren oder deaktivieren Sie eine Region in Ihrer Organisation

Überlegungen vor dem Aktivieren und Deaktivieren von Regionen

Bevor Sie eine Region aktivieren oder deaktivieren, sollten Sie Folgendes beachten:

- Regionen, die vor dem 20. März 2019 eingeführt wurden, sind standardmäßig aktiviert. AWS Ursprünglich waren alle neu AWS-Regionen standardmäßig aktiviert, sodass Sie sofort mit der Erstellung und Verwaltung von Ressourcen in diesen Regionen beginnen können. Standardmäßig aktivierte Regionen können weder aktiviert noch deaktiviert werden. Wenn heute eine Region AWS hinzugefügt wird, ist die neue Region standardmäßig deaktiviert. Wenn Sie möchten, dass Ihre Benutzer Ressourcen in einer neuen Region erstellen und verwalten können, müssen Sie zuerst diese Region aktivieren. Die folgenden Regionen sind standardmäßig deaktiviert.

Name	Code
Afrika (Kapstadt)	`af-south-1`
Asien-Pazifik (Hongkong)	`ap-east-1`
Asien-Pazifik (Hyderabad)	`ap-south-2`
Asien-Pazifik (Jakarta)	`ap-southeast-3`
Asien-Pazifik (Melbourne)	`ap-southeast-4`
Kanada (Calgary)	`ca-west-1`

Name	Code
Europa (Milan)	`eu-south-1`
Europa (Spain)	`eu-south-2`
Europa (Zürich)	`eu-central-2`
Israel (Tel Aviv)	`il-central-1`
Naher Osten (Bahrain)	`me-south-1`
Naher Osten (VAE)	`me-central-1`

- Sie können IAM-Berechtigungen verwenden, um den Zugriff auf Regionen zu steuern. AWS Identity and Access Management (IAM) umfasst vier Berechtigungen, mit denen Sie steuern können, welche Benutzer Regionen aktivieren, deaktivieren, abrufen und auflisten können. Weitere Informationen finden Sie im AWS Billing and Cost Management Benutzerhandbuch unter Aktionsrichtlinien für Billing and Cost Management. Sie können auch den `aws:RequestedRegion`Bedingungsschlüssel verwenden, um den Zugriff AWS-Services auf eine zu steuern AWS-Region.
- Die Aktivierung einer Region ist kostenlos — Die Aktivierung einer Region ist kostenlos. Ihnen werden nur Ressourcen in Rechnung gestellt, die Sie in der neuen Region erstellen.
- Durch das Deaktivieren einer Region wird der IAM-Zugriff auf Ressourcen in der Region deaktiviert — Wenn Sie eine Region deaktivieren, die noch AWS Ressourcen enthält, z. B. Amazon Elastic Compute Cloud (Amazon EC2) -Instances, verlieren Sie den IAM-Zugriff auf die Ressourcen in dieser Region. Sie können den beispielsweise nicht verwenden, AWS Management Console um die Konfiguration von EC2-Instances in einer deaktivierten Region anzuzeigen oder zu ändern.
- Gebühren für aktive Ressourcen bleiben bestehen, wenn Sie eine Region deaktivieren — Wenn Sie eine Region deaktivieren, die noch AWS Ressourcen enthält, fallen Gebühren für diese Ressourcen (falls vorhanden) weiterhin zum Standardsatz an. Beispiel: Falls Sie eine Region deaktivieren, die Amazon-EC2-Instances enthält, müssen Sie dennoch Gebühren für diese Instances bezahlen, auch wenn diese Instances nicht mehr aufgerufen werden können.
- Das Deaktivieren einer Region ist nicht immer sofort sichtbar — Dienste und Konsolen sind nach dem Deaktivieren einer Region möglicherweise vorübergehend sichtbar. Es kann einige Minuten bis mehrere Stunden dauern, bis die Deaktivierung einer Region wirksam wird.

- Die Aktivierung einer Region dauert in einigen Fällen einige Minuten bis mehrere Stunden. Wenn Sie eine Region aktivieren, werden Aktionen AWS zur Vorbereitung Ihres Kontos in dieser Region durchgeführt, z. B. die Verteilung Ihrer IAM-Ressourcen an die Region. Dieser Vorgang dauert bei den meisten Konten einige Minuten, kann aber manchmal mehrere Stunden dauern. Sie können eine Region erst verwenden, wenn dieser Vorgang abgeschlossen ist.
- Organizations können innerhalb einer AWS Organisation zu einem bestimmten Zeitpunkt 50 Region-Opt-Anfragen offen haben — Das Verwaltungskonto kann zu jedem Zeitpunkt 50 offene Anfragen haben, deren Abschluss für die Organisation noch aussteht. Eine Anfrage entspricht entweder der Aktivierung oder Deaktivierung einer bestimmten Region für ein Konto.
- Für ein einzelnes Konto können zu einem bestimmten Zeitpunkt 6 Region-Opt-Anfragen bearbeitet werden. Eine Anfrage entspricht entweder der Aktivierung oder Deaktivierung einer bestimmten Region für ein Konto.
- EventBridge Amazon-Integration — Kunden können in Region-Opt-Statusaktualisierungen Benachrichtigungen abonnieren. EventBridge Für jede Statusänderung wird eine EventBridge Benachrichtigung erstellt, sodass Kunden Arbeitsabläufe automatisieren können.
- Ausdrucksstarker Region-Opt-Status — Aufgrund der asynchronen Art der Aktivierung/Deaktivierung einer Opt-in-Region gibt es vier mögliche Statusarten für eine Region-Opt-Anfrage:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

  Sie können ein Opt-In oder Opt-Out nicht stornieren, wenn es sich in einem der beiden Status befindet. `ENABLING` `DISABLING` Andernfalls `ConflictException` wird a ausgelöst. Eine abgeschlossene (aktivierte/deaktivierte) Region-Opt-Anfrage hängt von der Bereitstellung der wichtigsten zugrunde liegenden Dienste ab. AWS Möglicherweise gibt es einige AWS Dienste, die trotz des Status nicht sofort nutzbar sind. `ENABLED`
- Vollständige Integration mit AWS Organizations — Ein Verwaltungskonto kann Region-Opt für jedes Mitgliedskonto dieser AWS Organisation ändern oder lesen. Ein Mitgliedskonto kann auch den Bundesstaat seiner Region lesen/schreiben.

Aktiviere oder deaktiviere eine Region für eigenständige Konten

Gehen Sie AWS-Konto wie folgt vor, um zu aktualisieren, auf welche Regionen Sie Zugriff haben. Das unten stehende AWS Management Console Verfahren funktioniert immer nur im eigenständigen

Kontext. Sie können den verwenden AWS Management Console , um nur die verfügbaren Regionen in dem Konto anzuzeigen oder zu aktualisieren, mit dem Sie den Vorgang aufgerufen haben.

AWS Management Console

Um eine Region für eine eigenständige Version zu aktivieren oder zu deaktivieren AWS-Konto

> **Mindestberechtigungen**
>
> Um die Schritte im folgenden Verfahren ausführen zu können, muss ein IAM-Benutzer oder eine IAM-Rolle über die folgenden Berechtigungen verfügen:
>
> - `account:ListRegions`(wird benötigt, um die Liste der AWS-Regionen aktuell aktivierten oder deaktivierten Benutzer einzusehen).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Melden Sie sich entweder AWS Management Consoleals oder als IAM-Benutzer Root-Benutzer des AWS-Kontos oder als Rolle an, die über die Mindestberechtigungen verfügt.
2. Wählen Sie oben rechts im Fenster Ihren Kontonamen und dann Konto aus.
3. Scrollen Sie auf der Kontoseite nach unten zum Abschnitt AWS-Regionen.

   > **Note**
   >
   > Möglicherweise werden Sie aufgefordert, Ihren Zugriff auf diese Informationen zu genehmigen. AWS sendet eine Anfrage an die mit dem Konto verknüpfte E-Mail-Adresse und an die primäre Kontakttelefonnummer. Wählen Sie den Link in der Anfrage, um sie in Ihrem Browser zu öffnen, und genehmigen Sie den Zugriff.

4. Wählen Sie neben jeder AWS-Region Option in der Spalte Aktion entweder Aktivieren oder Deaktivieren aus, je nachdem, ob Sie möchten, dass die Benutzer in Ihrem Konto Ressourcen in dieser Region erstellen und darauf zugreifen können.
5. Bestätigen Sie Ihre Auswahl, wenn Sie dazu aufgefordert werden.
6. Nachdem Sie alle Änderungen vorgenommen haben, wählen Sie Aktualisieren.

AWS CLI & SDKs

Sie können den Opt-Status der Region aktivieren, deaktivieren, lesen und auflisten, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Mindestberechtigungen**
>
> Um die folgenden Schritte ausführen zu können, benötigen Sie die entsprechende Berechtigung für diesen Vorgang:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern nur das Lesen von Opt-Informationen für Regionen gewähren und anderen Benutzern Lese- und Schreibberechtigungen gewähren.

Im folgenden Beispiel wird eine Region für das angegebene Mitgliedskonto in einer Organisation aktiviert. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

Beachten Sie, dass Sie eine Region auch mit demselben Befehl deaktivieren und dann durch `enable-region` ersetzen `disable-region` können.

```
aws account enable-region --region-name af-south-1
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Der Vorgang ist asynchron. Mit dem folgenden Befehl können Sie den aktuellen Status der Anfrage anzeigen.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Aktivieren oder deaktivieren Sie eine Region in Ihrer Organisation

Gehen Sie wie folgt vor AWS Organizations, um die aktivierten Regionen für Ihre Mitgliedskonten zu aktualisieren.

> **Note**
>
> Die AWS Organizations verwalteten Richtlinien `AWSOrganizationsReadOnlyAccess` wurden aktualisiert, sodass Sie Zugriff auf die AWS Kontoverwaltungs-APIs erhalten, sodass Sie von der AWS Organizations Konsole aus auf Kontodaten zugreifen können. `AWSOrganizationsFullAccess` Informationen zu den aktualisierten verwalteten Richtlinien finden Sie unter Aktualisierungen der AWS verwalteten Richtlinien von Organizations.

> **Note**
>
> Bevor Sie diese Vorgänge über das Verwaltungskonto oder ein delegiertes Administratorkonto in einer Organisation zur Verwendung mit Mitgliedskonten ausführen können, müssen Sie:
>
> - Aktivieren Sie alle Funktionen in Ihrer Organisation, um die Einstellungen Ihrer Mitgliedskonten zu verwalten. Dies ermöglicht dem Administrator die Kontrolle über die Mitgliedskonten. Dies ist standardmäßig festgelegt, wenn Sie Ihre Organisation erstellen. Wenn in Ihrer Organisation nur die konsolidierte Fakturierung aktiviert ist und Sie alle Funktionen aktivieren möchten, finden Sie weitere Informationen unter Alle Funktionen in Ihrer Organisation aktivieren.
> - Aktivieren Sie den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsdienst. Informationen zur Einrichtung finden Sie unterVertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

AWS Management Console

So aktivieren oder deaktivieren Sie eine Region in Ihrer Organisation

1. Melden Sie sich mit den Anmeldeinformationen für das Verwaltungskonto Ihrer Organisation an der AWS Organizations Konsole an.
2. Wählen Sie auf der AWS-KontenSeite das Konto aus, das Sie aktualisieren möchten.
3. Wählen Sie den Tab Kontoeinstellungen.
4. Wählen Sie unter Regionen die Region aus, die Sie aktivieren oder deaktivieren möchten.
5. Wählen Sie Aktionen und dann entweder die Option Aktivieren oder Deaktivieren.
6. Wenn Sie die Option Aktivieren ausgewählt haben, überprüfen Sie den angezeigten Text und wählen Sie dann Region aktivieren.
7. Wenn Sie die Option „Deaktivieren“ ausgewählt haben, überprüfen Sie den angezeigten Text, geben Sie zur Bestätigung „Deaktivieren“ ein und wählen Sie dann „Region deaktivieren“.

AWS CLI & SDKs

Sie können den Opt-Status der Region für Mitgliedskonten von Organisationen aktivieren, deaktivieren, lesen und auflisten, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Mindestberechtigungen**
>
> Um die folgenden Schritte ausführen zu können, benötigen Sie die entsprechende Berechtigung für diesen Vorgang:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`

- `account:ListRegions`

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern nur das Lesen von Opt-Informationen für Regionen gewähren und anderen Benutzern Lese- und Schreibberechtigungen gewähren.

Im folgenden Beispiel wird eine Region für das angegebene Mitgliedskonto in einer Organisation aktiviert. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

Beachten Sie, dass Sie eine Region auch mit demselben Befehl deaktivieren und dann durch `enable-region` ersetzen `disable-region` können.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

> **Note**
>
> Eine Organisation kann zu einem bestimmten Zeitpunkt nur bis zu 20 Regionsanfragen haben. Andernfalls erhalten Sie eine`TooManyRequestsException`.

Der Vorgang ist asynchron. Mit dem folgenden Befehl können Sie den aktuellen Status der Anfrage anzeigen.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Erstelle oder aktualisiere deinen AWS-Konto Alias

Wenn Sie möchten, dass die URL für Ihre IAM-Benutzer Ihren Firmennamen (oder eine andere easy-to-remember Kennung) anstelle der AWS-Konto ID enthält, können Sie einen Kontoalias erstellen.

Informationen zum Erstellen oder Aktualisieren eines Kontoalias finden Sie im IAM-Benutzerhandbuch unter AWS-KontoAlias erstellen, löschen und auflisten.

Abrechnung für IhreAWS-Konto

Für abrechnungsbezogene Verfahren und Aufgaben, die mit Ihrem zusammenhängenAWS-Kontokönnen Sie den folgenden Themen im entnehmenAWS Billing and Cost Management-Benutzerhandbuch:

- Ändern der Währung, in der Sie Ihre Rechnung bezahlen
- Aktualisieren und Löschen von Steuer-Registrierungsnummern
- Aktivieren der Vererbung der Steuereinstellungen

Konten in Indien verwalten

Wenn Sie sich für ein neues anmeldenAWS-Kontound wählen Sie Indien als Kontaktadresse, Ihre Benutzervereinbarung ist mitAmazon Internet Services Private Limited(AISPL), ein EinheimischerAWSVerkäufer in Indien. AISPL verwaltet Ihre Abrechnung und Ihr Rechnungsbetrag wird in indischen Rupien (INR) statt in US-Dollar (USD) aufgeführt. Nachdem Sie ein Konto bei AISPL erstellt haben, können Sie das Land in Ihren Kontaktinformationen nicht mehr ändern.

Wenn Sie eine bestehende habenAWS-Kontomit einer Adresse in Indien ist Ihr Konto entweder beiAWSoder AISPL, je nachdem, wann Sie das Konto eröffnet haben. Um zu erfahren, ob Ihr Konto beiAWSoder AISPL, sieheDetermining which company your account is with. Wenn Sie bereits AWS-Kunde sind, können Sie Ihr AWS-Konto weiterhin nutzen. Sie können sich auch dafür entscheiden, beide zu habenAWS-Kontound ein AISPL-Konto, obwohl sie nicht zu demselben konsolidiert werden könnenAWSOrganisation. Für Informationen zur Verwaltung einesAWS-Konto, sieheVerwalte deineAWS-Konto.

Wenn Ihr Konto bei AISPL ist, befolgen Sie die in diesem Thema beschriebenen Verfahren, um Ihr Konto zu verwalten. In diesem Thema wird erklärt, wie Sie sich für ein AISPL-Konto anmelden, Informationen zu Ihrem AISPL-Konto bearbeiten und Ihre permanente Kontonummer (PAN) hinzufügen oder bearbeiten.

Als Teil des Prüfverfahrens für die Kreditkarte während der Anmeldung belastet AISPL Ihre Kreditkarte mit 2 INR. AISPL erstattet die 2 INR nach Abschluss der Überprüfung zurück. Sie werden möglicherweise bei der Verifizierung zu Ihrer Bank umgeleitet.

Themen

- Ermitteln Sie, bei welchem Unternehmen Ihr Konto ist
- Erstelle eineAWS-Kontomit AISPL
- Verwalte dein AISPL-Konto

Ermitteln Sie, bei welchem Unternehmen Ihr Konto ist

AWS-Services werden von AWS und AISPL bereitgestellt. Verwenden Sie dieses Verfahren, um zu ermitteln, bei welchem Verkäufer Sie Ihr Konto haben.

AWS Management Console

Feststellen, bei welchem Unternehmen Sie Ihr Konto haben:

> **Mindestberechtigungen**
>
> Um die folgenden Schritte ausführen zu können, müssen Sie mindestens über die folgenden IAM-Berechtigungen verfügen:
>
> - Für dieses Verfahren sind keine besonderen Berechtigungen erforderlich.

1. Öffnen Sie die AWS Management Console unter AWS Management Console.
2. Sehen Sie sich in der Fußzeile unten auf der Seite den Copyright-Hinweis an. Wenn das Copyright für Amazon Web Services gilt, haben Sie Ihr Konto bei AWS. Wenn das Copyright für Amazon Internet Services Private Ltd. gilt, haben Sie Ihr Konto bei AISPL.

AWS CLI & SDKs

Diese Aufgabe wird nicht unterstützt in derAWS CLIoder durch eine API-Operation von einem derAWSSDKs. Sie können diese Aufgabe nur ausführen, indem Sie denAWS Management Console.

Erstelle eineAWS-Kontomit AISPL

AISPL ist ein lokaler Verkäufer vonAWSin Indien. Führen Sie die folgenden Schritte aus, um ein AISPL-Konto anzumelden, wenn Ihre Kontaktadresse in Indien ist.

AWS Management Console

Für ein AISPL-Konto registrieren

> **Mindestberechtigungen**
>
> Um die folgenden Schritte ausführen zu können, müssen Sie mindestens über die folgenden IAM-Berechtigungen verfügen:
>
> - Weil dieser Vorgang stattfindet, bevor Sie eineAWS-Konto, dieser Vorgang erfordert keineAWSBerechtigungen.

1. Öffne dieAWS Management Console, und wählen Sie dannMelden Sie sich bei der Konsole an.
2. Auf derLoggen Sie sich einSeite, geben Sie die E-Mail-Adresse ein, die Sie verwenden möchten.
3. Wählen Sie unter der E-Mail-Adresse I am a new user (Ich bin ein neuer Benutzer) aus und klicken Sie auf Sign in using our secure server (Über den sicheren Server anmelden).
4. Geben Sie für jedes Feld mit Anmeldeinformationen Ihre Daten ein und wählen Sie dannKonto erstellen.
5. Geben Sie für jedes der Kontaktinformationsfelder Ihre Daten ein.
6. Nachdem Sie die Kundenvereinbarung gelesen haben, aktivieren Sie das Kontrollkästchen „Geschäftsbedingungen“ und wählen Sie anschließend Create Account and Continue (Konto erstellen und fortfahren) aus.
7. Wählen Sie auf der Seite Zahlungsinformationen die Zahlungsweise aus, die Sie verwenden möchten.
8. UnterPAN-Informationen, wähleNeinwenn Sie keine permanente Kontonummer (PAN) haben oder diese später hinzufügen möchten. Wenn Sie eine PAN haben und diese jetzt hinzufügen möchten, wählen SieJa, und in derPFANNEFeld geben Sie Ihre PAN ein.
9. Wählen Sie Verify Card and Continue (Karte überprüfen und fortfahren) aus. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben. AISPL belastet Ihre Karte im Zuge des Überprüfungsprozesses mit 2 INR. AISPL erstattet die 2 INR nach Abschluss der Überprüfung zurück.
10. FürGeben Sie eine Telefonnummer an, geben Sie Ihre Telefonnummer ein. Wenn Sie eine Telefondurchwahl haben, fürExt., geben Sie Ihre Telefondurchwahl ein.

11. Wählen Sie Calle Me Now (Mich jetzt anrufen) aus. Nach kurzer Zeit wird eine vierstellige PIN auf dem Bildschirm angezeigt.
12. Akzeptieren Sie den automatisierten Anruf von AISPL. Geben Sie auf der Tastatur Ihres Telefons die vierstellige PIN ein, die auf Ihrem Bildschirm angezeigt wird.
13. Sobald Ihre Kontaktnummer vom automatisierten Anruf überprüft wurde, wählen Sie Auswahl des Support-Programms fortsetzen aus.
14. Wählen Sie auf der Seite Support-Plan Ihren Support-Plan aus und klicken Sie anschließend auf Weiter. Nachdem Ihre Zahlungsmethode verifiziert und Ihr Konto aktiviert wurde, erhalten Sie eine E-Mail-Nachricht, in der die Aktivierung Ihres Kontos bestätigt wird.

AWS CLI & SDKs

Diese Aufgabe wird nicht unterstützt in derAWS CLIoder durch eine API-Operation von einem derAWSSDKs. Sie können diese Aufgabe nur ausführen, indem Sie denAWS Management Console.

Verwalte dein AISPL-Konto

Mit Ausnahme der folgenden Aufgaben sind die Verfahren zur Verwaltung Ihres Kontos dieselben wie bei Konten, die außerhalb Indiens erstellt wurden. Siehe Verwalte deineAWS-Konto.

Benutze dieAWS Management Consoleum die folgenden Aufgaben auszuführen:

- Eine permanente Kontonummer (PAN) hinzufügen oder bearbeiten
- Bearbeiten Sie mehrere permanente Kontonummern (PANs)
- Bearbeiten Sie mehrere Waren- und Dienstleistungssteuernummern (GSTs)
- Eine Steuerrechnung anzeigen

Schließe eine AWS-Konto

Wenn Sie Ihre nicht mehr benötigen AWS-Konto, können Sie sie jederzeit schließen, indem Sie den Anweisungen in diesem Abschnitt folgen. Nachdem Sie es geschlossen haben, können Sie es innerhalb von 90 Tagen ab dem Tag, an dem Sie das Konto geschlossen haben, wieder öffnen. Die Zeitspanne zwischen dem Tag, an dem Sie das Konto geschlossen haben, und dem Tag, an dem das Konto AWS dauerhaft geschlossen wird, wird als Zeitraum nach der Schließung bezeichnet.

Was müssen Sie wissen, bevor Sie Ihr Konto schließen

Bevor Sie Ihr AWS-Konto Konto schließen, sollten Sie Folgendes beachten:

- Die Schließung Ihres Kontos gilt als Kündigung der AWS Kundenvereinbarung für dieses Konto.
- Sie müssen keine Ressourcen in Ihrem löschen, AWS-Konto bevor Sie es schließen. Wir empfehlen Ihnen jedoch, alle Ressourcen oder Daten zu sichern, die Sie behalten möchten. Anweisungen zum Sichern einer bestimmten Ressource finden Sie in der entsprechenden AWS Dokumentation für diesen Dienst.
- Sie können Ihr Konto während der Zeit nach der Schließung erneut öffnen. Die Gebühren für die Dienste, die in Ihrem Konto verblieben sind, werden wieder aufgenommen, wenn Sie es erneut öffnen. Sie bleiben auch für unbezahlte Rechnungen und ausstehende Reserved Instances und Savings Plans verantwortlich.
- Sie sind weiterhin für alle ausstehenden Gebühren und Entgelte für die vor der Kontoschließung in Anspruch genommenen Dienste verantwortlich. Sie erhalten im darauffolgenden Monat nach Schließung Ihres Kontos eine AWS Rechnung. Wenn Sie Ihr Konto beispielsweise am 15. Januar geschlossen haben, erhalten Sie Anfang Februar eine Rechnung für die Nutzung zwischen dem 1. Januar und dem 15. Januar. Sie erhalten nach der Schließung Ihres Kontos weiterhin Rechnungen für Reserved Instances und Savings Plans, bis diese ablaufen.
- Sie können nicht mehr auf AWS Dienste zugreifen, die zuvor in Ihrem Konto verfügbar waren. Sie können sich jedoch nur AWS-Konto während der Zeit nach der Schließung anmelden und auf ein geschlossenes Konto zugreifen, um frühere Rechnungsinformationen einzusehen, auf Kontoeinstellungen zuzugreifen oder Kontakt aufzunehmen. AWS Support
- Sie können nicht dieselbe E-Mail-Adresse, mit der Sie zum AWS-Konto Zeitpunkt der Schließung registriert waren, als primäre E-Mail-Adresse einer anderen Person verwenden. AWS-Konto Wenn Sie dieselbe E-Mail-Adresse für eine andere verwenden möchten, empfehlen wir AWS-Konto, sie vor dem Schließen zu aktualisieren. Anweisungen Aktualisieren des AWS-Konto Namens, der E-Mail-Adresse oder des Passworts für den Root-Benutzer zur Aktualisierung deiner E-Mail-Adresse findest du unter.
- Wenn Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren AWS-Konto Root-Benutzer aktiviert oder ein MFA-Gerät für einen IAM-Benutzer konfiguriert haben, wird MFA nicht automatisch entfernt, wenn Sie das Konto schließen. Wenn Sie MFA während der 90 Tage nach der Schließung eingeschaltet lassen möchten, lassen Sie das MFA-Gerät aktiv, bis der Zeitraum nach der Schließung abgelaufen ist, falls Sie während dieser Zeit auf das Konto zugreifen müssen. Beachten Sie, dass die Hardware-TOTP-Token-Geräte nach der dauerhaften Schließung Ihres Kontos keinem anderen Benutzer zugeordnet werden können. Wenn Sie das Hardware-TOTP-Token

später mit einem anderen Benutzer verwenden möchten, haben Sie die Möglichkeit, das Hardware-MFA-Gerät zu deaktivieren, bevor Sie das Konto schließen. MFA-Geräte für IAM-Benutzer müssen vom Kontoadministrator gelöscht werden.

Zusätzliche Überlegungen zu Mitgliedskonten

- Wenn Sie ein Mitgliedskonto schließen, wird dieses Konto erst nach Ablauf der Zeit nach der Schließung aus der Organisation entfernt. Während der Phase nach Kontoschließung wird ein geschlossenes Mitgliedskonto weiterhin auf Ihr Kontingent an Konten in der Organisation angerechnet. Um zu vermeiden, dass das Konto auf das Kontingent angerechnet wird, finden Sie weitere Informationen unter Entfernen eines Mitgliedskontos aus Ihrer Organisation, bevor Sie es schließen.
- Sie können nur 10 % der Mitgliedskonten innerhalb eines fortlaufenden Zeitraums von 30 Tagen schließen. Dieses Kontingent ist nicht an einen Kalendermonat gebunden, sondern beginnt, wenn Sie ein Konto schließen. Innerhalb von 30 Tagen nach der ersten Kontoschließung können Sie das Limit von 10 % für die Kontoschließung nicht überschreiten. Die Mindestanzahl für Kontoschließungen beträgt 10 und die Höchstgrenze für Kontoschließungen 1000, auch wenn 10% der Konten 1000 überschreiten. Weitere Informationen zu Kontingenten für Organizations finden Sie unter Kontingente für AWS Organizations.
- Wenn Sie AWS Control Tower verwenden, müssen Sie die Verwaltung des Mitgliedskontos aufheben, bevor Sie versuchen, das Konto zu schließen. Siehe Managment eines Mitgliedskontos aufheben im AWS -Control-Tower-Benutzerhandbuch.

Servicespezifische Überlegungen

- AWS Marketplace Abonnements werden bei Kontoschließung nicht automatisch gekündigt. Wenn Sie Abonnements haben, kündigen Sie zunächst alle Instanzen Ihrer Software in den Abonnements. Rufen Sie dann in der AWS Marketplace Konsole die Seite „Abonnements verwalten“ auf und kündigen Sie Ihre Abonnements.
- Domains, die bei Route 53 registriert sind, werden nicht automatisch gelöscht. Bevor Sie Ihre schließen AWS-Konto, haben Sie vier Möglichkeiten:
  - Sie können die automatische Verlängerung deaktivieren, und die Domains werden automatisch gelöscht, wenn der Registrierungszeitraum abläuft. Weitere Informationen finden Sie unter Enabling or Disabling Automatic Renewal for a Domain (Aktivieren oder Deaktivieren der automatischen Verlängerung für eine Domain) im Entwicklerhandbuch für Amazon Route 53.

- Sie können die Domains auf ein anderes AWS-Kontoübertragen. Weitere Informationen finden Sie unter Übertragen einer Domain auf ein anderes AWS-Konto.
- Sie können die Domains zu einer anderen Domainvergabestelle übertragen. Weitere Informationen finden Sie unter Übertragen einer Domain von Route 53 an eine andere Vergabestelle.
- Wenn Sie Ihr Konto bereits geschlossen haben, können Sie einen Fall eröffnen, um Hilfe AWS Support bei der Übertragung der Domain zu erhalten.

Wie können Sie Ihr Konto schließen

Sie können Ihr Konto AWS-Konto mit dem folgenden Verfahren schließen. Beachten Sie, dass je nach Kontotyp [eigenständig, Mitglied, Verwaltung und AWS GovCloud (US)], das Sie schließen möchten, auf jeder Registerkarte unterschiedliche Anleitungen angezeigt werden.

Falls bei der Schließung Ihres Kontos Probleme auftreten, finden Sie weitere Informationen unterFehlerbehebung bei Problemen mit AWS-Konto der Schließung.

Standalone account

Ein eigenständiges Konto ist ein individuell verwaltetes Konto, das nicht Teil von ist AWS Organizations.

Um ein eigenständiges Konto von der Kontoseite aus zu schließen

1. Melden Sie sich AWS Management Console als Root-Benutzer in dem an AWS-Konto , den Sie schließen möchten. Sie können ein Konto nicht schließen, während Sie als IAM-Benutzer oder als IAM-Rolle angemeldet sind.
2. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke Ihren Kontonamen oder Ihre Kontonummer und dann Konto aus.
3. Scrollen Sie auf der Kontoseite zum Ende der Seite zum Abschnitt Konto schließen. Lesen Sie den Vorgang zur Kontoschließung und stellen Sie sicher, dass Sie ihn verstanden haben.
4. Wählen Sie die Schaltfläche Konto schließen, um den Kontoschließungsprozess einzuleiten.
5. Innerhalb weniger Minuten sollten Sie eine E-Mail-Bestätigung erhalten, dass Ihr Konto geschlossen wurde.

> **Note**
>
> Diese Aufgabe wird im AWS CLI oder durch eine API-Operation von einem der AWS SDKs nicht unterstützt. Sie können diese Aufgabe nur mit dem AWS Management Console ausführen.

Member account

Ein Mitgliedskonto ist ein AWS-Konto , das Teil von ist AWS Organizations.

Um ein Mitgliedskonto über die AWS Organizations Konsole zu schließen

1. Melden Sie sich an der AWS Organizations -Konsole an.
2. Suchen und wählen Sie auf der Seite AWS-Konten den Namen des Mitgliedskontos, das Sie schließen möchten. Sie können durch die OU-Hierarchie navigieren oder eine flache Liste von Konten ohne die OU-Struktur anzeigen.
3. Wählen Sie oben auf der Seite neben dem Kontonamen Close (Schließen) aus. Organizations im Modus „Konsolidierte Abrechnung“ können die Schaltfläche „Schließen“ in der Konsole nicht sehen. Um ein Konto im konsolidierten Abrechnungsmodus zu schließen, müssen Sie die Schritte auf der Registerkarte Eigenständiges Konto befolgen.
4. Aktivieren Sie jedes Kontrollkästchen, um alle erforderlichen Kontoschließungs-Anweisungen zu bestätigen.
5. Geben Sie die Mitgliedskonto-ID ein und wählen Sie dann Konto schließen.

Um ein Mitgliedskonto von der Kontoseite aus zu schließen

Optional können Sie ein AWS Mitgliedskonto direkt auf der Seite Konten im schließen AWS Management Console. Wenn Sie step-by-step Hilfe benötigen, folgen Sie den Anweisungen auf der Registerkarte Eigenständiges Konto.

So schließen Sie ein Mitgliedskonto mithilfe von AWS CLI SDKs

Anweisungen zum Schließen eines Mitgliedskontos mithilfe der SDKs AWS CLI und finden Sie im AWS Organizations Benutzerhandbuch unter Schließen eines Mitgliedskontos in Ihrer Organisation.

Management account

Ein Verwaltungskonto ist ein Konto AWS-Konto , das als übergeordnetes Konto oder Stammkonto für AWS Organizations fungiert.

> **Note**
>
> Sie können ein Verwaltungskonto nicht direkt von der AWS Organizations Konsole aus schließen.

Um ein Verwaltungskonto von der Kontoseite aus zu schließen

1. Melden Sie sich AWS Management Console als Root-Benutzer für das Verwaltungskonto an, das Sie schließen möchten. Sie können ein Konto nicht schließen, während Sie als IAM-Benutzer oder als IAM-Rolle angemeldet sind.
2. Stellen Sie sicher, dass in Ihrer Organisation keine aktiven Mitgliedskonten mehr vorhanden sind. Rufen Sie dazu die AWS Organizations Konsole auf und stellen Sie sicher, dass alle Mitgliedskonten `Suspended` neben ihren Kontonamen angezeigt werden. Wenn Sie ein Mitgliedskonto haben, das noch aktiv ist, müssen Sie die Anweisungen zur Kontoschließung befolgen, die auf der Registerkarte Mitgliedskonto aufgeführt sind, bevor Sie mit dem nächsten Schritt fortfahren können.
3. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke Ihren Kontonamen oder Ihre Kontonummer und dann Konto aus.
4. Scrollen Sie auf der Kontoseite zum Ende der Seite zum Abschnitt Konto schließen. Lesen Sie den Vorgang zur Kontoschließung und stellen Sie sicher, dass Sie ihn verstanden haben.
5. Wählen Sie die Schaltfläche Konto schließen, um den Kontoschließungsprozess einzuleiten.
6. Innerhalb weniger Minuten sollten Sie eine E-Mail-Bestätigung erhalten, dass Ihr Konto geschlossen wurde.

> **Note**
>
> Diese Aufgabe wird im AWS CLI oder durch eine API-Operation von einem der AWS SDKs nicht unterstützt. Sie können diese Aufgabe nur mit dem AWS Management Console ausführen.

AWS GovCloud (US) account

Ein AWS GovCloud (US) Konto ist zu Abrechnungs- und Zahlungszwecken immer mit einem einzigen Standard AWS-Konto verknüpft.

Um ein AWS GovCloud (US) Konto zu schließen

Wenn Sie ein Konto haben AWS-Konto , das mit einem AWS GovCloud (US) Konto verknüpft ist, müssen Sie das Standardkonto schließen, bevor Sie das AWS GovCloud (US) Konto schließen. Weitere Informationen, unter anderem dazu, wie Sie Daten sichern und unbeabsichtigte AWS GovCloud (US) Gebühren vermeiden können, finden Sie im AWS GovCloud (US) Benutzerhandbuch unter Ein AWS GovCloud (US) Konto schließen.

Was erwartet Sie, nachdem Sie Ihr Konto geschlossen haben

Unmittelbar nach der Schließung Ihres Kontos passiert Folgendes:

- Sie erhalten eine E-Mail mit der Bestätigung der Kontoschließung an die E-Mail-Adresse des Root-Benutzers. Wenn Sie diese E-Mail nicht innerhalb weniger Stunden erhalten, finden Sie weitere Informationen unterFehlerbehebung bei Problemen mit AWS-Konto der Schließung.
- Für jedes Mitgliedskonto, das Sie schließen, wird in der AWS Organizations Konsole neben dem Kontonamen ein SUSPENDED Etikett angezeigt.
- Wenn Sie anderen Konten Berechtigungen für den Zugriff auf Dienste in Ihrem AWS-Konto Konto erteilt haben, sollten alle Zugriffsanfragen, die von diesen Konten aus gestellt werden, nach der Kontoschließung fehlschlagen. Wenn Sie Ihr Konto erneut öffnen AWS-Konto, AWS-Konten können andere wieder auf die AWS Dienste und Ressourcen Ihres Kontos zugreifen, sofern Sie ihnen die erforderlichen Berechtigungen erteilt haben.

Zeitraum nach der Schließung

Die Zeit nach der Schließung bezieht sich auf die Zeitspanne zwischen dem Tag, an dem Sie Ihr Konto geschlossen haben, und dem Tag, an dem Ihr Konto AWS dauerhaft geschlossen wird. AWS-Konto Die Frist nach der Schließung beträgt 90 Tage. Während der Zeit nach der Schließung können Sie nur dann auf Ihre Inhalte und AWS Dienste zugreifen, wenn Sie Ihr Konto erneut öffnen. Nach Ablauf der Frist nach der Schließung wird Ihr AWS AWS-Konto Konto dauerhaft geschlossen und Sie können es nicht mehr erneut öffnen. AWS löscht außerdem alle Inhalte und Ressourcen in Ihrem Konto. Nachdem ein Konto dauerhaft geschlossen wurde, kann seine AWS-Konto ID niemals wiederverwendet werden.

Wiedereröffnung Ihres AWS-Konto

Ihr Konto wird innerhalb von 90 Tagen dauerhaft geschlossen. Danach können Sie Ihr Konto nicht erneut öffnen und AWS löschen die in Ihrem Konto verbleibenden Inhalte. Um Ihr Konto wieder zu eröffnen, bevor es dauerhaft geschlossen wird, (1) müssen Sie uns AWS Supportso schnell wie möglich kontaktieren und (2) wir müssen innerhalb von 60 Tagen ab dem Datum der Kontoschließung die vollständige Zahlung aller ausstehenden Beträge erhalten, einschließlich der Bereitstellung der erforderlichen Informationen, wie auf der Rechnung angegeben.

Verwenden Sie die AWS Kontoverwaltung in Ihrer Organisation

AWS Organizationsist ein AWS Dienst, mit dem Sie Ihre AWS-Konten Gruppe verwalten können. Dies bietet Funktionen wie die konsolidierte Abrechnung, bei der alle Rechnungen Ihrer Konten zusammengefasst und von einem einzigen Zahler bearbeitet werden. Sie können die Sicherheit Ihres Unternehmens auch zentral verwalten, indem Sie richtlinienbasierte Kontrollen verwenden. Weitere Informationen zu AWS Organizations finden Sie im AWS Organizations Benutzerhandbuch.

Vertrauenswürdiger Zugriff

Wenn AWS Organizations Sie Ihre Konten als Gruppe verwalten, können die meisten Verwaltungsaufgaben für die Organisation nur vom Verwaltungskonto der Organisation ausgeführt werden. Standardmäßig umfasst dies nur Operationen, die sich auf die Verwaltung der Organisation selbst beziehen. Sie können diese zusätzliche Funktionalität auf andere AWS Dienste ausdehnen, indem Sie den vertrauenswürdigen Zugriff zwischen Organisationen und diesem Dienst aktivieren. Vertrauenswürdiger Zugriff gewährt dem angegebenen AWS Dienst die Berechtigung, auf Informationen über die Organisation und die darin enthaltenen Konten zuzugreifen. Wenn Sie den vertrauenswürdigen Zugriff für die Kontoverwaltung aktivieren, gewährt der Kontoverwaltungsdienst Organisationen und ihren Verwaltungskonten Berechtigungen für den Zugriff auf die Metadaten, z. B. die primären oder alternativen Kontaktinformationen, für alle Mitgliedskonten der Organisation.

Weitere Informationen finden Sie unter Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

Delegierter Admin

Nachdem Sie den vertrauenswürdigen Zugriff aktiviert haben, können Sie auch eines Ihrer Mitgliedskonten als delegiertes Administratorkonto für AWS die Kontoverwaltung festlegen. Auf diese Weise kann das delegierte Administratorkonto dieselben Metadatenverwaltungsaufgaben für die Mitgliedskonten in Ihrer Organisation ausführen, die zuvor nur das Verwaltungskonto ausführen konnte. Das delegierte Administratorkonto kann nur auf die Verwaltungsaufgaben für den Kontoverwaltungsdienst zugreifen. Das delegierte Administratorkonto hat nicht den gesamten administrativen Zugriff auf die Organisation, den das Verwaltungskonto hat.

Weitere Informationen finden Sie unter Aktivieren eines delegierten Administrators fürAWSKontenverwaltung.

Service-Kontrollrichtlinien

Wenn Sie AWS-Konto Teil einer Organisation sind, die von der Organisation verwaltet wirdAWS Organizations, kann der Administrator der Organisation Service Control Policies (SCPs) anwenden, die einschränken können, was die Principals in den Mitgliedskonten tun können. Ein SCP gewährt niemals Berechtigungen. Stattdessen ist es ein Filter, der einschränkt, welche Berechtigungen vom Mitgliedskonto verwendet werden können. Ein Benutzer oder eine Rolle (ein Principal) in einem Mitgliedskonto kann nur die Operationen ausführen, die im Schnittpunkt zwischen den für das Konto geltenden SCPs und den dem Principal zugewiesenen IAM-Berechtigungsrichtlinien liegen. Beispielsweise können Sie SCPs verwenden, um zu verhindern, dass ein Principal eines Accounts die alternativen Kontakte seines eigenen Accounts ändert.

Zum Beispiel SCPs, die gelten fürAWS-Konten, sieheBeschränken des Zugriffs mitAWS OrganizationsService-Kontrollrichtlinien.

Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren

Durch die Aktivierung des vertrauenswürdigen Zugriffs für AWS die Kontoverwaltung kann der Administrator des Verwaltungskontos die Informationen und Metadaten (z. B. primäre oder alternative Kontaktdaten) ändern, die für jedes Mitgliedskonto in spezifisch sindAWS Organizations. Weitere Informationen finden Sie unter AWSKontoverwaltung und AWS Organizations im AWS OrganizationsBenutzerhandbuch. Allgemeine Informationen zur Funktionsweise des vertrauenswürdigen Zugriffs finden Sie unter Verwendung AWS Organizations mit anderen AWS Diensten.

Nachdem der vertrauenswürdige Zugriff aktiviert wurde, können Sie den `accountID` Parameter in den API-Vorgängen der Kontoverwaltung verwenden, die ihn unterstützen. Sie können diesen Parameter nur dann erfolgreich verwenden, wenn Sie den Vorgang mit Anmeldeinformationen vom Verwaltungskonto oder vom delegierten Administratorkonto für Ihre Organisation, falls Sie eines aktivieren, aus aufrufen. Weitere Informationen finden Sie unter Aktivieren eines delegierten Administrators fürAWSKontenverwaltung.

Gehen Sie wie folgt vor, um den vertrauenswürdigen Zugriff für die Kontoverwaltung in Ihrer Organisation zu aktivieren.

> **Mindestberechtigungen**
>
> Um diese Aufgaben ausführen zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie können dies nur über das Verwaltungskonto der Organisation ausführen.
- Für Ihre Organisation müssen alle Funktionen aktiviert sein.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Zugriff für die AWS Kontoverwaltung

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer:in anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer:in anmelden (nicht empfohlen).
2. Wählen Sie im Navigationsbereich Dienste aus.
3. Wählen Sie in der Liste der Dienste die Option AWSKontoverwaltung aus.
4. Wählen Sie Vertrauenswürdigen Zugriff aktivieren.
5. Geben Sie im Dialogfeld Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren ein, um dies zu bestätigen, und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

AWS CLI & SDKs

So aktivieren Sie den vertrauenswürdigen Zugriff für die AWS Kontoverwaltung

Nachdem Sie den folgenden Befehl ausgeführt haben, können Sie die Anmeldeinformationen aus dem Verwaltungskonto der Organisation verwenden, um API-Operationen zur Kontoverwaltung aufzurufen, die den `--accountId` Parameter verwenden, um auf Mitgliedskonten in einer Organisation zu verweisen.

- AWS CLI: enable-aws-service-access

  Das folgende Beispiel aktiviert den vertrauenswürdigen Zugriff für die AWS Kontoverwaltung in der Organisation des Anrufers.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Aktivieren eines delegierten Administrators fürAWSKontenverwaltung

Ein delegiertes Administratorkonto kann denAWS-API-Vorgänge für die Kontoverwaltung für andere Mitgliedskonten in der Organisation. Gehen Sie wie folgt vor, um ein Mitgliedskonto in Ihrer Organisation als delegiertes Administratorkonto festzulegen.

Mindestberechtigungen

Um diese Aufgaben ausführen zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Dies können Sie nur über das Verwaltungskonto der Organisation ausführen.
- Für Ihre Organisation müssen alle Funktionen aktiviert sein.
- Mussvertrauenswürdiger Zugriff für die Kontoverwaltung in Ihrer Organisation aktiviertaus.

Nachdem Sie ein delegiertes Administratorkonto für Ihre Organisation angegeben haben, können Benutzer und Rollen in diesem KontoAWS CLIundAWSSDK-Abläufe im`account`Namespace, der im Organisationsmodus arbeiten kann, indem er ein optionales unterstützt`AccountId`-Parameter.

AWS Management Console

Diese Aufgabe wird nicht inAWSManagementkonsole für die Kontoverwaltung. Diese Aufgabe können Sie nur mitAWS CLIoder eine API-Operation von einem derAWSSDKs.

AWS CLI & SDKs

So registrieren Sie ein delegiertes Administratorkonto für den Kontoverwaltungsdienst

Mit den folgenden Befehlen können Sie einen delegierten Administrator für den Kontoverwaltungsdienst aktivieren.

Sie müssen den folgenden Serviceprinzipal angeben:

```
account.amazonaws.com
```

- AWS CLI:registrierend-delegierter Administrator

  Im folgenden Beispiel wird ein Mitgliedskonto der Organisation als delegierten Administrator für den Kontoverwaltungsdienst registriert.

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Nachdem Sie diesen Befehl ausgeführt haben, können Sie die Anmeldeinformationen aus dem Konto 123456789012 verwenden, um die Kontoverwaltung aufzurufenAWS CLIund SDK-API-Operationen, die die`--account-id`-Parameter, um auf Mitgliedskonten in einer Organisation zu verweisen.

Beschränken des Zugriffs mitAWS OrganizationsService-Kontrollrichtlinien

In diesem Thema finden Sie Beispiele, die zeigen, wie Sie Service-Kontrollrichtlinien (SCPs) verwenden können, um einzuschränken, was die Benutzer und Rollen in den Konten in Ihrer Organisation tun können. Weitere Informationen zu Service-Kontrollrichtlinien finden Sie in folgenden Themen im.AWS OrganizationsBenutzerhandbuch:

- SCPs erstellen
- SCPs an OUs und Accounts anhängen
- Strategien für SCPs
- Syntax der SCP-Richtlinie

Example Beispiel 1: Verhindern Sie, dass Konten ihre eigenen alternativen Kontakte ändern

Das folgende Beispiel bestreitet die`PutAlternateContact`und`DeleteAlternateContact`API-Operationen werden von keinem Mitgliedskonto in aufgerufenStandalone-Konto-Modusaus. Dadurch wird verhindert, dass ein Auftraggeber in den betroffenen Konten seine eigenen alternativen Kontakte ändert.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
```

```
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Beispiel 2: Verhindern, dass ein Mitgliedskonto alternative Kontakte für ein anderes Mitgliedskonto in der Organisation ändert

Das folgende Beispiel verallgemeinert die`Resource`-Element auf „*“, was bedeutet, dass es für beide gilt[Anforderungen im eigenständigen Modus und Anforderungen im Organisationsmodus](#)aus. Dies bedeutet, dass selbst das delegierte Administratorkonto für die Kontoverwaltung, falls der SCP darauf zutrifft, daran gehindert wird, alternative Kontakte für ein Konto in der Organisation zu ändern.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example Beispiel 3: Verhindern, dass ein Mitgliedskonto in einer Organisationseinheit seine eigenen alternativen Kontakte ändert

Das folgende Beispiel für SCP enthält eine Bedingung, die den Organisationspfad des Kontos mit einer Liste von zwei Organisationseinheiten vergleicht. Dies führt dazu, dass ein Principal in einem Konto in den angegebenen OUs daran gehindert wird, seine eigenen alternativen Kontakte zu ändern.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

Sicherheit inAWSKontenverwaltung

Die Sicherheit in der Cloud hat AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für die Kontenverwaltung gelten, finden Sie unterAWS-Servicesim Umfang nach Compliance-Programmaus.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. 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 erläudert, wie das Modell der geteilten Verantwortung bei der Verwendung von zum Tragen kommtAWSKontenverwaltung. Es zeigt Ihnen, wie Sie die Kontenverwaltung konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren außerdem, wie man andere benutztAWS-Services, die Ihnen helfen, Ihre -Kontoverwaltungs-Ressourcen zu überwachen und zu schützen.

Themen

- Datenschutz in der AWS Kontoverwaltung
- AWS PrivateLinkzumAWSKontenverwaltung
- Identity and Access Management für die AWS Kontoverwaltung
- AWSverwaltete Richtlinien fürAWSVerwaltung von Benutzerkonten
- Konformitätsvalidierung für die AWS Kontoverwaltung
- Ausfallsicherheit inAWSKontenverwaltung
- Sicherheit der Infrastruktur in AWS Account Management

Datenschutz in der AWS Kontoverwaltung

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in der AWS Kontoverwaltung. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. 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, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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 für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 auf AWS über eine Befehlszeilenschnittstelle oder über 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 Kontoverwaltung oder anderen AWS-Services über die KonsoleAWS CLI, API oder AWS SDKs arbeiten. 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.

AWS PrivateLinkzumAWSKontenverwaltung

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) verwenden, um IhreAWS-Ressourcen können Sie aufAWSKontoverwaltungsdienst von der VPC aus, ohne das öffentliche Internet überqueren zu müssen.

Mit Amazon VPC können Sie startenAWS-Ressourcen in einem benutzerdefinierten virtuellen Netzwerk. Mit einer VPC können Sie Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways, steuern. Weitere Informationen über VPCs finden Sie unterAmazon VPC User Guideaus.

Um Ihre Amazon VPC mit der Kontoverwaltung zu verbinden, müssen Sie zuerst eineSchnittstellen-VPC-Endpunkt, mit dem Sie Ihre VPC mit anderen verbinden könnenAWS-Services. Der Endpunkt bietet eine zuverlässige, skalierbare Konnektivität, ohne dass ein Internet-Gateway, eine NAT-Instance (Network Address Translation) oder eine VPN-Verbindung erforderlich ist. Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Erstellen des Endpunkts

Sie können einAWSEndpunkt der Kontoverwaltung in Ihrer VPC mit demAWS Management Console, derAWS Command Line Interface(AWS CLI), einAWSSDK, dasAWSKontoverwaltungs-API oderAWS CloudFormationaus.

Informationen zum Erstellen und Konfigurieren eines Endpunkts über die Amazon-VPC-Konsole oder die AWS CLI finden Sie unter Creating an Interface Endpoint (Erstellen eines Schnittstellenendpunkts) im Amazon-VPC-Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen Endpunkt erstellen, geben Sie an, dass Kontenverwaltung der Service ist, mit dem Ihre VPC eine Verbindung einrichten soll, verwenden Sie das folgende Format:
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> Sie müssen die Zeichenfolge genau wie gezeigt verwenden und dieus-east-1Region : Als globaler Dienst wird Account Management nur in diesem gehostetAWSRegion :

Informationen zum Erstellen und Konfigurieren eines Endpunkts mit AWS CloudFormation finden Sie in der AWS::EC2::VPCEndpoint-Ressource im AWS CloudFormation-Benutzerhandbuch.

Amazon VPC-Endpunktrichtlinien

Sie können steuern, welche Aktionen über diesen Service-Endpunkt ausgeführt werden können, indem Sie beim Erstellen des Amazon VPC-Endpunkts eine Endpunktrichtlinie anhängen. Sie können komplexe IAM-Regeln erstellen, indem Sie mehrere Endpunktrichtlinien anfügen. Weitere Informationen finden Sie unter:

- Amazon Virtual Private Cloud Cloud-Endpunktrichtlinien für Kontenverwaltung
- Kontrollieren des Zugriffs auf Services mit VPC-EndpunktenimAWS PrivateLink-Handbuchaus.

Amazon Virtual Private Cloud Cloud-Endpunktrichtlinien für Kontenverwaltung

Sie können eine Amazon VPC-Endpunktrichtlinie für die Kontenverwaltung erstellen, in der Sie Folgendes angeben:

- Prinzipal, der die Aktionen ausführen kann
- Die Aktionen, die die Prinzipale ausführen können.
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Das folgende Beispiel zeigt eine Amazon VPC-Endpunktrichtlinie, die es einem IAM-Benutzer namens Alice im Konto 123456789012 ermöglicht, die alternativen Kontaktinformationen für alle abzurufen und zu ändernAWS-Konto, verweigert jedoch allen IAM-Benutzern die Erlaubnis, alternative Kontaktinformationen für jedes Konto zu löschen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
```

```
            "Principal": {
              "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

Wenn Sie Zugriff auf Konten gewähren möchten, die Teil einerAWSOrganisation zu einem Prinzipal, der sich in einem der Mitgliedskonten der Organisation befindet, dann die`Resource`-Element muss das folgende Format verwenden:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Weitere Informationen zum Erstellen von Endpunktrichtlinien finden Sie unterKontrollieren des Zugriffs auf Services mit VPC-EndpunktenimAWS PrivateLink-Handbuchaus.

Identity and Access Management für die AWS Kontoverwaltung

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, -Kontenverwaltungsressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert AWS die Kontoverwaltung mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für die AWS Kontoverwaltung
- Fehlerbehebung bei Identität und Zugriff auf die AWS Kontoverwaltung

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in der Kontoverwaltung.

Service-Benutzer – Wenn Sie den Kontoverwaltungsservice zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie zur Ausführung von Aufgaben weitere Kontoverwaltungsfunktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf ein Feature in der Kontoverwaltung zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung bei Identität und Zugriff auf die AWS Kontoverwaltung.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für die Kontoverwaltungsressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Kontoverwaltung. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Features und Ressourcen der Kontoverwaltung Ihre Service-Benutzer 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 dazu, wie Ihr Unternehmen IAM mit Kontoverwaltung verwenden kann, finden Sie unter So funktioniert AWS die Kontoverwaltung mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Account Management verfassen können. Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat

der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. 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 ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. 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.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. 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 in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, 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. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (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 Features 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 zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte

es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. 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.
- Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. 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

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen

in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in 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 festlegen, wer zum Zugriff auf was berechtigt ist. 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 Benutzerinformationen über die AWS Management Console, die AWS CLI oder die 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 AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von 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.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und

Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete 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-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren,

können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. 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 dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

So funktioniert AWS die Kontoverwaltung mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Account Management zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit Account Management verwenden können.

IAM-Funktionen, die Sie mit der AWS Kontoverwaltung verwenden können

IAM-Feature	Unterstützung für die Kontoverwaltung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja

IAM-Feature	Unterstützung für die Kontoverwaltung
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen Überblick über das Zusammenwirken von Kontoverwaltung und anderen -AWSServices mit den meisten IAM-Funktionen finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für die Kontoverwaltung

Unterstützt Richtlinien auf Identitätsbasis.	Ja

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.

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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung

Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung.

Ressourcenbasierte Richtlinien in der Kontoverwaltung

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für die Kontoverwaltung

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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 die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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.

Eine Liste der Kontoverwaltungsaktionen finden Sie unter Von AWS Kontoverwaltung definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in der Kontoverwaltung verwenden das folgende Präfix vor der Aktion.

```
account
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Um beispielsweise alle Aktionen anzugeben, die mit den alternativen AWS-KontoKontakten eines funktionieren, schließen Sie die folgende Aktion ein.

```
"Action": "account:*AlternateContact"
```

Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung.

Richtlinienressourcen für die Kontoverwaltung

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Der -Kontoverwaltungsservice unterstützt die folgenden spezifischen Ressourcentypen im -`Resources`Element einer IAM-Richtlinie, damit Sie die Richtlinie filtern und zwischen diesen Typen von unterscheiden könnenAWS-Konten:

- Konto

  Dieser `resource` Typ entspricht nur eigenständigen KontenAWS-Konten, die keine Mitgliedskonten in einer vom AWS Organizations Service verwalteten Organisation sind.

- accountInOrganization

  Dieser `resource` Typ stimmt nur mit übereinAWS-Konten, die Mitgliedskonten in einer vom AWS Organizations Service verwalteten Organisation sind.

Eine Liste der Ressourcentypen für die Kontoverwaltung und ihrer ARNs finden Sie unter Von der AWS Kontoverwaltung definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Kontoverwaltung definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung.

Richtlinienbedingungsschlüssel für die Kontoverwaltung

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Der -Kontoverwaltungsservice unterstützt die folgenden Bedingungsschlüssel, mit denen Sie eine differenzierte Filterung für Ihre IAM-Richtlinien bereitstellen können:

- -Konto:TargetRegion

  Dieser Bedingungsschlüssel verwendet ein Argument, das aus einer Liste von AWS Regionscodes besteht. Sie können die Richtlinie so filtern, dass sie sich nur auf die Aktionen auswirkt, die für die angegebenen Regionen gelten.
- -Konto:AlternateContactTypes

Dieser Bedingungsschlüssel verwendet eine Liste alternativer Kontakttypen:

- BILLING
- OPERATIONEN
- SECURITY

Mit diesem Schlüssel können Sie die Anforderung nur nach den Aktionen filtern, die auf die angegebenen alternativen Kontakttypen abzielen.

- -Konto:AccountResourceOrgPaths

  Dieser Bedingungsschlüssel verwendet ein Argument, das aus einer Liste von ARNs mit Platzhaltern besteht, die Konten in einer Organisation darstellen. Sie können die Richtlinie so filtern, dass sie sich nur auf die Aktionen auswirkt, die Konten mit übereinstimmenden ARNs anvisieren. Der folgende ARN entspricht beispielsweise nur den Konten in der angegebenen Organisation und der angegebenen Organisationseinheit (OU).

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- -Konto:AccountResourceOrgTags

  Dieser Bedingungsschlüssel verwendet ein Argument, das aus einer Liste von Tag-Schlüsseln und -Werten besteht. Sie können die Richtlinie so filtern, dass sie sich nur auf die Konten auswirkt, die Mitglieder einer Organisation sind und mit den angegebenen Tag-Schlüsseln und -Werten gekennzeichnet sind.

Eine Liste der Bedingungsschlüssel für die Kontoverwaltung finden Sie unter Bedingungsschlüssel für die AWS Kontoverwaltung in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Kontoverwaltung definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien für die Kontoverwaltung finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung.

Zugriffskontrolllisten in Kontoverwaltung

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Attributbasierte Zugriffskontrolle mit Kontoverwaltung

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit der Kontoverwaltung

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, unter anderem darüber, welche AWS-Services mit temporären

Anmeldeinformationen arbeiten, finden Sie unter AWS-Services, die mit IAM arbeiten im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für die Kontoverwaltung

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für die Kontoverwaltung

Unterstützt Servicerollen	Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, 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.

Serviceverknüpfte Rollen für die Kontoverwaltung

Unterstützt serviceverknüpfte Rollen	Nein

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Ressourcen für die Kontoverwaltung. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. 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.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von der -Kontoverwaltung definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Kontoverwaltung in der Service-Autorisierungs-Referenz.

Themen

- Bewährte Methoden für Richtlinien

- Verwenden der Seite Konto im AWS Management Console
- Gewähren von schreibgeschütztem Zugriff auf die Seite Konto im AWS Management Console
- Gewähren von Vollzugriff auf die Seite Konto in der AWS Management Console

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Kontoverwaltungsressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene

Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Seite Konto im AWS Management Console

Um auf die Seite Konto in der zugreifen zu könnenAWS Management Console, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu Ihrem aufzulisten und anzuzeigenAWS-Konto. 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 Benutzer und Rollen die -Kontoverwaltungskonsole verwenden können, können Sie entweder die von `AWSAccountManagementFullAccess` AWS verwaltete Richtlinie `AWSAccountManagementReadOnlyAccess` oder an die Entitäten anfügen. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Sie müssen keine Mindestkonsolenberechtigungen für Benutzer zulassen, die nur Aufrufe für die AWS CLI oder AWS API durchführen. In vielen Fällen können Sie stattdessen den Zugriff nur auf die Aktionen zulassen, die den API-Operationen entsprechen, die Sie ausführen möchten.

Gewähren von schreibgeschütztem Zugriff auf die Seite Konto im AWS Management Console

Im folgenden Beispiel möchten Sie einem IAM-Benutzer in Ihrem AWS-Kontoschreibgeschützten Zugriff auf die Seite Konto in der gewährenAWS Management Console. Benutzer, denen diese Richtlinie angefügt ist, können keine Änderungen vornehmen.

Die `account:GetAccountInformation` Aktion gewährt Zugriff, um die meisten Einstellungen auf der Seite Konto anzuzeigen. Um jedoch die aktuell aktivierten AWS Regionen anzuzeigen, müssen Sie auch die `account:ListRegions` Aktion einschließen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Gewähren von Vollzugriff auf die Seite Konto in der AWS Management Console

Im folgenden Beispiel möchten Sie einem IAM-Benutzer in Ihrem AWS-Konto vollen Zugriff auf die Seite Konto in der gewährenAWS Management Console. Benutzer, denen diese Richtlinie angefügt ist, können die Einstellungen für das Konto ändern.

Diese Beispielrichtlinie baut auf der vorherigen Beispielrichtlinie auf, indem jede der verfügbaren Schreibberechtigungen (mit Ausnahme von CloseAccount) hinzugefügt wird, wodurch der Benutzer die meisten Einstellungen für das Konto ändern kann, einschließlich der `account:DisableRegion` Berechtigungen `account:EnableRegion` und .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
```

```
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für die AWS Kontoverwaltung

Eine vollständige Erläuterung von AWS-Konten und IAM-Benutzern finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch.

Eine Anleitung zum Aktualisieren von kundenverwalteten Richtlinien finden Sie unter Bearbeiten von vom Kunden verwalteten Richtlinien (Konsole) im IAM-Benutzerhandbuch.

AWS Richtlinien für Kontoverwaltungsaktionen

Diese Tabelle fasst die Berechtigungen zusammen, die Zugriff auf Ihre Kontoeinstellungen gewähren. Beispiele für Richtlinien, die diese Berechtigungen verwenden, finden Sie unter AWS Beispiele für Kontoverwaltungsrichtlinien.

> **Note**
>
> Um IAM-Benutzern Schreibzugriff auf eine bestimmte Kontoeinstellung auf der Seite Konto der zu gewährenAWS Management Console, müssen Sie zusätzlich zu der Berechtigung (oder den Berechtigungen), die Sie zum Ändern dieser Einstellung verwenden möchten, die `GetAccountInformation` Berechtigung erteilen.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:ListRegions`	Auflisten	Gewährt die Berechtigung zum Auflisten der verfügbaren Regionen.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:GetAccount Information`	Lesen	Gewährt die Berechtigung zum Abrufen der Kontoinfo rmationen für ein Konto.
`account:GetAlterna teContact`	Lesen	Gewährt die Berechtigung zum Abrufen der alternativen Kontakte für ein Konto.
`account:GetChallen geQuestions`	Lesen	Gewährt die Berechtigung zum Abrufen der Aufforder ungsfragen für ein Konto.
`account:GetContact Information`	Lesen	Gewährt die Berechtigung zum Abrufen der primären Kontaktinformationen für ein Konto.
`account:GetRegionO ptStatus`	Lesen	Gewährt die Berechtigung zum Abrufen des Opt-In-St atus einer Region.
`account:CloseAccount`	Schreiben	Gewährt die Berechtigung zum Schließen eines Kontos. **Note** Diese Berechtig ung gilt nur für die Konsole. Für diese Berechtigung ist kein API-Zugriff verfügbar.
`account:DeleteAlte rnateContact`	Schreiben	Gewährt die Berechtigung zum Löschen der alternativen Kontakte für ein Konto.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:DisableRegion`	Schreiben	Gewährt die Berechtigung zum Deaktivieren der Verwendung einer Region.
`account:EnableRegion`	Schreiben	Gewährt die Berechtigung zum Aktivieren der Verwendung einer Region.
`account:PutAlternateContact`	Schreiben	Gewährt die Berechtigung zum Ändern der alternativen Kontakte für ein Konto.
`account:PutChallengeQuestions`	Schreiben	Gewährt die Berechtigung zum Ändern der Aufforderungsfragen für ein Konto. **Note** Diese Berechtigung gilt nur für die Konsole. Für diese Berechtigung ist kein API-Zugriff verfügbar.
`account:PutContactInformation`	Schreiben	Gewährt die Berechtigung zum Aktualisieren der primären Kontaktinformationen für ein Konto.

Fehlerbehebung bei Identität und Zugriff auf die AWS Kontoverwaltung

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Kontoverwaltung und IAM auftreten können.

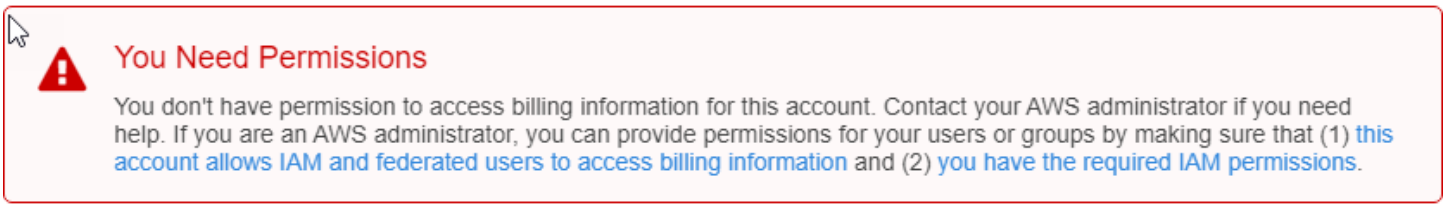
Themen

- Ich bin nicht autorisiert, eine Aktion auf der Seite Konto auszuführen
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert.
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Kontodaten gewähren

Ich bin nicht autorisiert, eine Aktion auf der Seite Konto auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zu verwenden, um Details zu seinem AWS-Konto auf der Seite Konto des anzuzeigenAWS Management Console, aber nicht über die `account:GetAccountInformation` Berechtigungen verfügt.



In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *`my-example-widget`* auf die Ressource `account:`*`GetWidget`* zugreifen zu können.

Ich bin nicht zur Ausführung von **`iam:PassRole`** autorisiert.

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an die Kontoverwaltung übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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 der Kontoverwaltung 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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Kontodaten gewähren

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 dazu, ob Account Management diese Funktionen unterstützt, finden Sie unter So funktioniert AWS die Kontoverwaltung mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- 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.

AWSverwaltete Richtlinien fürAWSVerwaltung von Benutzerkonten

AWSAccount Management bietet derzeit zweiAWSverwaltete Richtlinien, die für Ihre Verwendung verfügbar sind:

- AWS verwaltete Richtlinie: AWSAccountManagementReadOnlyAccess
- AWS verwaltete Richtlinie: AWSAccountManagementFullAccess
- Aktualisierungen der Kontoverwaltung fürAWSverwaltete Richtlinien

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSAccountManagementReadOnlyAccess

Sie können die `AWSAccountManagementReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Leserechte, mit denen nur Folgendes angezeigt werden kann:

- Die Metadaten über IhreAWS-Konten
- DerAWS-Regionendie aktiviert oder deaktiviert sind für dieAWS-Konto(Sie können den Status der Regionen in Ihrem Konto nur mithilfe derAWSKonsole)

Dies geschieht, indem es die Erlaubnis erteilt, eines der`Get*`oder`List*`Operationen. Es bietet keine Möglichkeit, die Kontometadaten zu ändern oder zu aktivieren oder zu deaktivierenAWS-Regionenfür das Konto.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `account`— Ermöglicht es Schulleitern, die Metadateninformationen abzurufen überAWS-Konten. Es ermöglicht Schulleitern auch, die aufzulistenAWS-Regionendie für das Konto aktiviert sind in derAWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AWSAccountManagementFullAccess

Sie können die `AWSAccountManagementFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie bietet vollen Administratorzugriff, um Folgendes einzusehen oder zu ändern:

- Die Metadaten über IhreAWS-Konten
- DerAWS-Regionendie aktiviert oder deaktiviert sind für dieAWS-Konto(Sie können den Status einsehen oder Regionen für Ihr Konto aktivieren oder deaktivieren, indem Sie dieAWSKonsole)

Dies geschieht, indem es die Erlaubnis erteilt, beliebige auszuführen`account`Operationen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `account`— Ermöglicht es Schulleitern, die Metadateninformationen über einzusehen oder zu ändernAWS-Konten. Es ermöglicht Schulleitern auch, die aufzulistenAWS-Regionendie für das Konto aktiviert sind und sie aktivieren oder deaktivieren in derAWS Management Console.

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

Aktualisierungen der Kontoverwaltung fürAWSverwaltete Richtlinien

Details zu Updates für anzeigenAWSverwaltete Richtlinien für die Kontoverwaltung, seit dieser Dienst damit begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf der Kontoverwaltungsdokumente.

Änderung	Beschreibung	Datum
AWSAccount Managemen t gestartet mit neuenAWSv erwaltete Richtlinien und begann, Änderungen zu verfolgen	Account Management wurde ursprünglich mit den folgenden Funktione n gestartetAWSverwaltete Richtlinien: • AWSAccountManageme ntReadOnlyAccess • AWSAccountManageme ntFullAccess	30. September 2021

Konformitätsvalidierung für die AWS Kontoverwaltung

Externe Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften der AWS Dienste, die in Ihrem Unternehmen im AWS-Konto Rahmen mehrerer AWS Compliance-Programme ausgeführt werden können. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS Dienstleistungen, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie unter AWS-ServicesUmfang nach Compliance-Programm AWS-Services unter . Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie im AWS Artifact Benutzerhandbuch unter unter Berichte herunterladen. AWS Artifact

Ihre Compliance-Verantwortung bei der Nutzung der Dienste in Ihrem AWS-Konto Unternehmen hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWSstellt die folgenden Ressourcen bereit, um Sie bei der Einhaltung von Vorschriften zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

  > **Note**
  >
  > Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

- AWS Audit Manager – Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit inAWSKontenverwaltung

DieAWSDie globale Infrastruktur ist aufgebautAWS-Regionenund Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen 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 über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Sicherheit der Infrastruktur in AWS Account Management

Als Managed Services AWS-Konto sind die in Ihrem System laufenden AWS Dienste durch die AWS globale Netzwerksicherheit geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Kontoeinstellungen zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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.

Überwachung der AWS Kontoverwaltung

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Account Management und Ihren anderen AWS Lösungen. AWSbietet die folgenden Überwachungstools, um die Kontoverwaltung zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst (protokolliert) API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und schreibt die Protokolldateien in einen von Ihnen angegebenen Amazon Simple Storage Service (Amazon S3) -Bucket. Auf diese Weise können Sie feststellen, welche Benutzer und Konten angerufen wurdenAWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.
- Amazon EventBridge fügt Ihren AWS Services zusätzliche Automatisierung hinzu, indem es automatisch auf Systemereignisse wie Probleme mit der Verfügbarkeit von Anwendungen oder Ressourcenänderungen reagiert. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

ProtokollierungAWS-Kontoverwaltungs-API-Aufrufe mitAWS CloudTrail

DieAWSAccount Management-APIs sind integriert mitAWS CloudTrail, einen Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWSDienst, der einen Account Management-Vorgang aufruft. CloudTrail erfasst alle -API-Aufrufe zur Kontoverwaltung als Ereignisse. Die erfassten Anrufe beinhalten alle Anrufe an die Kontoverwaltungsvorgänge. Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignissen für Kontoverwaltungsvorgänge. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Ereignisverlauf anzeigen. Anhand der von CloudTrail erfassten Informationen können Sie die Anforderung, die als Kontoverwaltungsvorgang bezeichnet wurde, die IP-Adresse, die für die Anforderung verwendete IP-Adresse, den Absenden der Anfrage und den Zeitpunkt der Anfrage sowie weitere Details bestimmen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Informationen zur Kontoverwaltung in CloudTrail

CloudTrail wird in IhremAWS-Kontowenn Sie das Konto erstellen. Wenn die mit einem -Kontoverwaltungsvorgang auftretenden Aktivitäten auftreten, zeichnet CloudTrail diese Aktivitäten zusammen mit anderen aufAWS-Service-Ereignisse inEreignisverlaufaus. Sie können die neuesten Ereignisse in IhremAWS-Kontoaus. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Für eine kontinuierliche Aufzeichnung von Ereignissen in IhremAWS-KontoErstellen Sie einen Trail, einschließlich Ereignissen für Kontoverwaltungsvorgänge. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn Sie einen Trail in derAWS Management Console, der Trail gilt für alleAWS-Regionenaus. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Sie können 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
- Empfangen von CloudTrail-Protokolldateien von mehreren Konten

AWS CloudTrailprotokolliert alle Account-Management-API-Vorgänge im-API-ReferenzAbschnitt in diesem Handbuch. Zum Beispiel werden durch Aufrufe der Operationen `CreateAccount`, `DeleteAlternateContact` und `PutAlternateContact` Einträge in den CloudTrail-Protokolldateien generiert.

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 Anforderung mit Root-Benutzer ausgeführt wurde oderAWS Identity and Access Management(IAM) Benutzeranmeldeinformationen
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine IAM-Rolle oder einen Verbundbenutzer ausgeführt wurde

- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter CloudTrail-Element userIdentity.

Verstehen der Logeinträge zur Kontoverwaltung

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 und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Operation, Anforderungsparameter usw. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Beispiel 1: Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen - Aufruf`GetAlternateContact`Operation zum Abrufen des aktuellen`OPERATIONS`alternativer Kontakt für ein Konto. Die von der Operation zurückgegebenen Werte sind nicht in den protokollierten Informationen enthalten.

Example Beispiel 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
```

```
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Beispiel 2: Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen - Aufruf`PutAlternateContact`So fügen Sie ein neues hinzu`BILLING`alternativer Kontakt zu einem Konto.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
```

```
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Beispiel 3: Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen - Aufruf`DeleteAlternateContact`So löschen Sie den aktuellen`OPERATION`Salternativer Kontakt.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
```

```
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Überwachung von Kontoverwaltungsereignissen mit EventBridge

Amazon EventBridge, früher CloudWatch Events genannt, unterstützt Sie bei der Überwachung von Ereignissen, die spezifisch für Sie sind, und bei der Initiierung von Zielaktionen, bei denen andere AWS-Services verwendet werden. Ereignisse von AWS-Services werden nahezu EventBridge in Echtzeit zugestellt.

Mithilfe können Sie Regeln erstellen EventBridge, die eingehenden Ereignissen entsprechen, und diese zur Verarbeitung an Ziele weiterleiten.

Weitere Informationen finden Sie unter Erste Schritte mit Amazon EventBridge im EventBridge Amazon-Benutzerhandbuch.

Ereignisse im Bereich Kontoverwaltung

Die folgenden Beispiele zeigen Ereignisse für die Kontoverwaltung. Ereignisse werden auf die bestmögliche Weise ausgegeben.

Für die Kontoverwaltung sind derzeit nur Ereignisse verfügbar, die sich speziell auf die Aktivierung und Deaktivierung von Regionen und API-Aufrufen über CloudTrail beziehen.

Ereignistypen

- Ereignis zur Aktivierung und Deaktivierung von Regionen

Ereignis zur Aktivierung und Deaktivierung von Regionen

Wenn Sie eine Region in einem Konto entweder über die Konsole oder über die API aktivieren oder deaktivieren, wird eine asynchrone Aufgabe gestartet. Die erste Anfrage wird als CloudTrail Ereignis im Zielkonto protokolliert. Darüber hinaus wird ein EventBridge Ereignis an das aufrufende Konto gesendet, wenn entweder der Aktivierungs- oder Deaktivierungsvorgang gestartet wurde, und erneut, sobald einer der Prozesse abgeschlossen ist.

Das folgende Beispielereignis zeigt, wie eine Anfrage gesendet wird, die angibt, dass `ENABLED` für `2020-09-30` die `ap-east-1` Region ein Konto eingerichtet wurde`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

Es gibt vier mögliche Status, die den von den APIs `GetRegionOptStatus` und `ListRegions` zurückgegebenen Status entsprechen:

- `ENABLED`— Die Region wurde erfolgreich für die angegebene Region aktiviert `accountId`
- `ENABLING`— Die Region wird gerade für die `accountId` angegebene Version aktiviert
- `DISABLED`— Die Region wurde für die `accountId` angegebene Region erfolgreich deaktiviert
- `DISABLING`— Die Region wird gerade für den `accountId` angegebenen Zeitraum deaktiviert

Das folgende Beispiel für ein Ereignismuster erstellt eine Regel, die alle Ereignisse in der Region erfasst.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

Mit dem folgenden Beispielereignismuster wird eine Regel erstellt, die nur Ereignisse `ENABLED` und Ereignisse aus `DISABLED` der Region erfasst.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

API-Referenz

Die API-Operationen in der Kontoverwaltung (`account`) Namespace ermöglichen es Ihnen, Ihren zu ändernAWS-Konto.

JederAWS-Kontounterstützt Metadaten mit Informationen über das Konto, einschließlich Informationen über bis zu drei alternative Kontakte, die mit dem Konto verknüpft sind. Diese gelten zusätzlich zu der E-Mail-Adresse, die mit dem verknüpft istRoot-Benutzerdes Kontos. Sie können nur einen der folgenden Kontakttypen angeben, die einem Konto zugeordnet sind.

- Ansprechpartner für Rechnungsstellung
- Ansprechpartner für den Betrieb
- Sicherheitskontakt

Standardmäßig gelten die in diesem Handbuch beschriebenen API-Operationen direkt für das Konto, das den Vorgang aufruft. DerIdentitätIn dem Konto, das den Vorgang aufruft, handelt es sich in der Regel um eine IAM-Rolle oder einen IAM-Benutzer, der über eine gemäß einer IAM-Richtlinie erteilte Berechtigung zum Aufrufen des API-Vorgangs verfügen muss. Alternativ können Sie diese API-Operationen von einer Identität in einemAWS OrganizationsVerwaltungskonto und geben Sie die Konto-ID-Nummer für jedes Konto anAWS-Kontodas ist ein Mitglied der Organisation.

API-Version

Diese Version der Accounts API-Referenz dokumentiert die Account-Management-API-Version 2021-02-01.

> **Note**
>
> Als Alternative zur direkten Verwendung der API können Sie eine derAWSSDKs, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (Java, Ruby, .NET, iOS, Android und mehr) bestehen. Die SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff aufAWSOrganisationen. Die SDKs kümmern sich beispielsweise darum, Anfragen kryptografisch zu signieren, Fehler zu verwalten und Anfragen automatisch zu wiederholen. Weitere Informationen über die AWS-SDKs, inkl. Herunterladen und Installation, finden Sie unter Tools für Amazon Web Services.

Wir empfehlen Ihnen, denAWSSDKs für programmatische API-Aufrufe an den Account Management Service. Sie können jedoch auch die Account Management Query API verwenden, um direkte Aufrufe an den Account Management-Webservice zu tätigen. Weitere Informationen zur Account Management Query API finden Sie unterAufrufen der API mittels HTTP-Abfrageanforderungenim Benutzerleitfaden zur Kontoverwaltung. Organisationen unterstützen GET- und POST-Anfragen für alle Aktionen. Das heißt, die API verlangt nicht, dass Sie für einige Aktionen GET und für andere POST verwenden. Allerdings unterliegen GET-Anforderungen der Größenbeschränkung von URLs. Verwenden Sie daher für Operationen, die größere Größen erfordern, eine POST-Anfrage.

Signieren von Anforderungen

Wenn Sie HTTP-Anfragen senden anAWS, Sie müssen die Anfragen unterschreiben, damitAWSkann identifizieren, wer sie geschickt hat. Du unterschreibst Anfragen mit deinemAWSZugriffsschlüssel, der aus einer Zugangsschlüssel-ID und einem geheimen Zugangsschlüssel besteht. Wir empfehlen dringend, keinen Zugangsschlüssel für Ihr Root-Konto zu erstellen. Jeder, der den Zugangsschlüssel für Ihr Root-Konto besitzt, hat uneingeschränkten Zugriff auf alle Ressourcen in Ihrem Konto. Erstellen Sie stattdessen einen Zugriffsschlüssel für einen IAM-Benutzer mit Administratorrechten. Als weitere Option verwenden SieAWSSecurity Token Service, um temporäre Sicherheitsanmeldeinformationen zu generieren und diese Anmeldeinformationen zum Signieren von Anfragen zu verwenden.

Um Anfragen zu signieren, empfehlen wir Ihnen, Signature Version 4 zu verwenden. Wenn Sie eine bestehende Anwendung haben, die Signature Version 2 verwendet, müssen Sie sie nicht aktualisieren, um Signature Version 4 zu verwenden. Für einige Operationen ist jetzt jedoch Signature Version 4 erforderlich. In der Dokumentation für Operationen, für die Version 4 erforderlich ist, wird auf diese Anforderung hingewiesen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Signieren von AWS-API-Anforderungen.

Wenn du den benutztAWSBefehlszeilenschnittstelle (AWSCLI) oder eines derAWSSDKs, an die Sie Anfragen richten könnenAWS, signieren diese Tools die Anfragen automatisch für Sie mit dem Zugriffsschlüssel, den Sie bei der Konfiguration der Tools angeben.

Support und Feedback für die Kontoverwaltung

Wir freuen uns über Ihr Feedback. Schicken Sie Ihre Kommentare anfeedback-awsaccounts@amazon.comoder posten Sie Ihr Feedback und Ihre Fragen in derSupport-Forum zur Kontoverwaltung. Weitere Informationen zu den AWS-Support-Foren finden Sie unter Forenhilfe.

Wie werden Beispiele präsentiert

Das von der Kontoverwaltung als Antwort auf Ihre Anfragen zurückgegebene JSON wird als einzelne lange Zeichenfolge ohne Zeilenumbrüche oder formatierte Leerzeichen zurückgegeben. In den Beispielen in diesem Handbuch werden sowohl Zeilenumbrüche als auch Leerzeichen verwendet, um die Lesbarkeit zu verbessern. Wenn Beispieleingabeparameter ebenfalls zu langen Zeichenketten führen würden, die über den Bildschirm hinausreichen würden, fügen wir Zeilenumbrüche ein, um die Lesbarkeit zu verbessern. Sie sollten die Eingabe immer als einzelne JSON-Textzeichenfolge einreichen.

API-Anfragen aufzeichnen

Account Management unterstütztCloudTrail, ein Dienst, der aufzeichnetAWSAPI-Aufrufe für IhreAWS-Kontound liefert Protokolldateien an einen Amazon S3-Bucket. Durch die Verwendung von Informationen, die gesammelt wurden vonCloudTrail, können Sie feststellen, welche Anfragen erfolgreich an die Kontoverwaltung gestellt wurden, wer die Anfrage gestellt hat, wann sie gestellt wurde usw. Weitere Informationen zur Kontoverwaltung und deren Unterstützung fürCloudTrail, siehe ProtokollierungAWS-Kontoverwaltungs-API-Aufrufe mitAWS CloudTrail. Um mehr zu erfahren überCloudTrail, einschließlich Informationen zum Einschalten und Auffinden Ihrer Logdateien, finden Sie in derAWS CloudTrailBenutzerleitfaden.

Aktionen

Folgende Aktionen werden unterstützt:

- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation

DeleteAlternateContact

Löscht den angegebenen alternativen Kontakt aus einemAWS-Konto.

Vollständige Informationen zur Verwendung der alternativen Kontaktfunktionen finden Sie unter Zugreifen auf alternative Kontakte oder deren Aktualisierung.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren könnenAWS-Konto, die von verwaltet wirdAWS Organizations, müssen Sie zunächst die Integration zwischen der AWS Kontoverwaltung und Organizations aktivieren. Weitere Informationen finden Sie unter Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

Anforderungssyntax

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer des AWS Kontos an, auf das Sie mit diesem Vorgang zugreifen oder das Sie ändern möchten.

Wenn Sie diesen Parameter nicht angeben, wird standardmäßig das AWS Konto der Identität verwendet, mit der der Vorgang aufgerufen wurde.

Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln, und die angegebene Konto-ID muss ein Mitgliedskonto in derselben Organisation sein. In der Organisation müssen alle Funktionen aktiviert sein, und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert sein und optional muss ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen`AccountId`, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an und rufen Sie den Vorgang mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

AlternateContactType

Gibt an, welcher der alternativen Kontakte gelöscht werden soll.

Typ: Zeichenfolge

Zulässige Werte: `BILLING | OPERATIONS | SECURITY`

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

ResourceNotFoundException

Der Vorgang ist fehlgeschlagen, weil eine Ressource angegeben wurde, die nicht gefunden werden kann.

HTTP Status Code: 404

TooManyRequestsException

Der Vorgang schlug fehl, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Beispiele

Beispiel 1

Im folgenden Beispiel wird der alternative Sicherheitskontakt für das Konto gelöscht, dessen Anmeldeinformationen zum Aufrufen des Vorgangs verwendet werden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Beispiel 2

Im folgenden Beispiel wird der alternative Abrechnungskontakt für das angegebene Mitgliedskonto in einer Organisation gelöscht. Sie müssen die Anmeldeinformationen entweder aus dem Verwaltungskonto der Organisation oder aus dem delegierten Administratorkonto des Kontoverwaltungsdienstes verwenden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für V3 JavaScript
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

DisableRegion

Deaktiviert (deaktiviert) eine bestimmte Region für ein Konto.

> **Note**
>
> Durch die Deaktivierung einer Region wird jeglicher IAM-Zugriff auf alle Ressourcen, die sich in dieser Region befinden, entfernt.

Anforderungssyntax

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer der Person an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Erforderlich: Nein

RegionName

Gibt den Regionalcode für einen bestimmten Regionsnamen an (z. B.`af-south-1`). Wenn Sie eine Region deaktivieren, AWS führt Aktionen aus, um diese Region in Ihrem Konto zu deaktivieren, z. B. die Zerstörung von IAM-Ressourcen in der Region. Dieser Vorgang nimmt für die meisten Konten ein paar Minuten in Anspruch, kann aber auch einige Stunden dauern. Sie können die Region erst aktivieren, wenn der Deaktivierungsvorgang vollständig abgeschlossen ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, finden Sie unter Häufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die Identität des Anrufers nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

ConflictException

Die Anfrage konnte aufgrund eines Konflikts im aktuellen Status der Ressource nicht verarbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT).

HTTP-Statuscode: 409

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagen. AWS Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

EnableRegion

Aktiviert (aktiviert) eine bestimmte Region für ein Konto.

Anforderungssyntax

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

RegionName

Gibt den Regionalcode für einen bestimmten Regionsnamen an (z. B.`af-south-1`). Wenn Sie eine Region aktivieren, führt AWS Aktionen zur Vorbereitung Ihres Kontos in der jeweiligen Region aus, z. B. die Verteilung Ihrer IAM-Ressourcen in die Region. Dieser Vorgang dauert bei den meisten Konten einige Minuten, kann aber auch mehrere Stunden dauern. Sie können eine Region erst verwenden, wenn dieser Vorgang abgeschlossen ist. Darüber hinaus können Sie die Region erst deaktivieren, wenn der Aktivierungsvorgang vollständig abgeschlossen ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 50 Zeichen.

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

ConflictException

Die Anfrage konnte aufgrund eines Konflikts im aktuellen Status der Ressource nicht verarbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT).

HTTP-Statuscode: 409

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagen. AWS Versuchen Sie den Vorgang später erneut.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für JavaScript V3
- AWS SDK für PHP V3

- AWS SDK für Python
- AWS SDK für Ruby V3

GetAlternateContact

Ruft den angegebenen alternativen Kontakt ab, der an einen AWS-Konto angehängt ist.

Vollständige Informationen zur Verwendung der alternativen Kontaktoperationen finden Sie unter Zugreifen auf alternative Kontakte oder deren Aktualisierung.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren könnenAWS-Konto, die von verwaltet wirdAWS Organizations, müssen Sie zunächst die Integration zwischen der AWS Kontoverwaltung und Organizations aktivieren. Weitere Informationen finden Sie unter Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

Anforderungssyntax

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer des AWS Kontos an, auf das Sie mit diesem Vorgang zugreifen oder das Sie ändern möchten.

Wenn Sie diesen Parameter nicht angeben, wird standardmäßig das AWS Konto der Identität verwendet, die zum Aufrufen des Vorgangs verwendet wurde.

Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln, und die angegebene Konto-ID muss ein Mitgliedskonto in derselben Organisation sein. In der Organisation müssen alle Funktionen aktiviert sein, und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert sein und optional muss ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen`AccountId`, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an und rufen Sie den Vorgang mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

AlternateContactType

Gibt an, welchen alternativen Kontakt Sie abrufen möchten.

Typ: Zeichenfolge

Zulässige Werte: `BILLING | OPERATIONS | SECURITY`

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
      "Name": "string",
      "PhoneNumber": "string",
      "Title": "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

AlternateContact

Eine Struktur, die die Details für den angegebenen alternativen Kontakt enthält.

Typ: AlternateContact Objekt

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

ResourceNotFoundException

Der Vorgang ist fehlgeschlagen, weil eine Ressource angegeben wurde, die nicht gefunden werden kann.

HTTP Status Code: 404

TooManyRequestsException

Der Vorgang schlug fehl, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Beispiele

Beispiel 1

Im folgenden Beispiel wird der alternative Sicherheitskontakt für das Konto abgerufen, dessen Anmeldeinformationen zum Aufrufen des Vorgangs verwendet werden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

Beispiel 2

Im folgenden Beispiel wird der alternative Betriebskontakt für das angegebene Mitgliedskonto in einer Organisation abgerufen. Sie müssen die Anmeldeinformationen entweder aus dem Verwaltungskonto der Organisation oder aus dem delegierten Administratorkonto des Kontoverwaltungsdienstes verwenden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für V3 JavaScript
- AWS SDK für PHP V3

- AWS SDK für Python
- AWS SDK für Ruby V3

GetContactInformation

Ruft die primären Kontaktinformationen eines AWS-Konto ab.

Vollständige Informationen zur Verwendung der primären Kontaktfunktionen finden Sie unter Aktualisieren der primären und alternativen Kontaktinformationen.

Anforderungssyntax

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer der Person an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

ContactInformation

Enthält die Details der primären Kontaktinformationen, die mit einem verknüpft sindAWS-Konto.

Typ: ContactInformation Objekt

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

ResourceNotFoundException

Der Vorgang ist fehlgeschlagen, weil eine Ressource angegeben wurde, die nicht gefunden werden kann.

HTTP Status Code: 404

TooManyRequestsException

Der Vorgang schlug fehl, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für JavaScript V3
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

GetRegionOptStatus

Ruft den Opt-In-Status einer bestimmten Region ab.

Anforderungssyntax

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer der Person an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

RegionName

Gibt den Regionalcode für einen bestimmten Regionsnamen an (z. B.`af-south-1`). Diese Funktion gibt den Status der Region zurück, die Sie an diesen Parameter übergeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 50 Zeichen.

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

RegionName

Der Regionalcode, der übergeben wurde.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 50 Zeichen.

RegionOptStatus

Einer der möglichen Status, den eine Region haben kann (Aktiviert, Aktiviert, Deaktiviert, Deaktiviert, Deaktiviert, Enabled_By_Default).

Typ: Zeichenfolge

Zulässige Werte: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unter. Häufige Fehler

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für JavaScript V3
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

ListRegions

Listet alle Regionen für ein bestimmtes Konto und ihren jeweiligen Opt-in-Status auf. Optional kann diese Liste nach dem Parameter gefiltert werden. `region-opt-status-contains`

Anforderungssyntax

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

MaxResults

Die Gesamtzahl der Elemente, die in der Ausgabe des Befehls zurückgegeben werden sollen. Wenn die Gesamtzahl der verfügbaren Elemente den angegebenen Wert übersteigt, `NextToken` wird in der Ausgabe des Befehls a angegeben. Um die Seitennummerierung fortzusetzen, geben Sie den `NextToken`-Wert im `starting-token`-Argument eines nachfolgenden Befehls an. Verwenden Sie das `NextToken` Antwortelement nicht direkt außerhalb der AWS CLI. Anwendungsbeispiele finden Sie unter Pagination im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Typ: Ganzzahl

Gültiger Bereich: Mindestwert 1. Maximaler Wert von 50.

Required: No

NextToken

Ein Token, das verwendet wird, um anzugeben, wo mit der Paginierung begonnen werden soll. Dies ist eine Antwort `NextToken` aus einer zuvor gekürzten Antwort. Anwendungsbeispiele finden Sie unter Pagination im Benutzerhandbuch für die AWS Befehlszeilenschnittstelle.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 0. Höchstlänge = 1 000 Zeichen.

Required: No

RegionOptStatusContains

Eine Liste von Regionsstatus (Aktiviert, Aktiviert, Deaktiviert, Deaktiviert, Enabled_by_Default), anhand derer die Liste der Regionen für ein bestimmtes Konto gefiltert werden kann. Wenn Sie beispielsweise den Wert ENABLING übergeben, wird nur eine Liste von Regionen mit dem Regionsstatus ENABLING zurückgegeben.

Typ: Zeichenfolge-Array

Zulässige Werte: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Required: No

Antwortsyntax

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

NextToken

Wenn mehr Daten zurückgegeben werden müssen, werden diese aufgefüllt. Es sollte an den `next-token` Anforderungsparameter von übergeben werden`list-regions`.

Typ: Zeichenfolge

Regions

Dies ist eine Liste von Regionen für ein bestimmtes Konto oder, falls der gefilterte Parameter verwendet wurde, eine Liste von Regionen, die den im `filter` Parameter festgelegten Filterkriterien entsprechen.

Typ: Array von Region-Objekten

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für JavaScript V3
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

PutAlternateContact

Ändert den angegebenen alternativen Kontakt, der an einen AWS-Konto angehängt ist.

Vollständige Informationen zur Verwendung der alternativen Kontaktfunktionen finden Sie unter Zugreifen auf alternative Kontakte oder deren Aktualisierung.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren könnenAWS-Konto, die von verwaltet wirdAWS Organizations, müssen Sie zunächst die Integration zwischen der AWS Kontoverwaltung und Organizations aktivieren. Weitere Informationen finden Sie unter Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

Anforderungssyntax

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer des AWS Kontos an, auf das Sie mit diesem Vorgang zugreifen oder das Sie ändern möchten.

Wenn Sie diesen Parameter nicht angeben, wird standardmäßig das AWS Konto der Identität verwendet, mit der der Vorgang aufgerufen wurde.

Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln, und die angegebene Konto-ID muss ein Mitgliedskonto in derselben Organisation sein. In der Organisation müssen alle Funktionen aktiviert sein, und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert sein und optional muss ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen`AccountId`, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an und rufen Sie den Vorgang mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

AlternateContactType

Gibt an, welchen alternativen Kontakt Sie erstellen oder aktualisieren möchten.

Typ: Zeichenfolge

Zulässige Werte: `BILLING | OPERATIONS | SECURITY`

Erforderlich: Ja

EmailAddress

Gibt eine E-Mail-Adresse für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 64 Zeichen.

Pattern: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

Erforderlich: Ja

Name

Gibt einen Namen für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 64 Zeichen.

Erforderlich: Ja

PhoneNumber

Gibt eine Telefonnummer für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Die maximale Länge beträgt 25.

Pattern: `^[\s0-9()+-]+$`

Erforderlich: Ja

Title

Gibt einen Titel für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 50 Zeichen.

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Führen Sie den Vorgang später erneut aus.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Beispiele

Beispiel 1

Im folgenden Beispiel wird der alternative Abrechnungskontakt für das Konto festgelegt, dessen Anmeldeinformationen zum Aufrufen des Vorgangs verwendet werden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AlternateContactType": "Billing",
```

```
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Beispiel 2

Im folgenden Beispiel wird der alternative Abrechnungskontakt für das angegebene Mitgliedskonto in einer Organisation festgelegt oder überschrieben. Sie müssen die Anmeldeinformationen entweder aus dem Verwaltungskonto der Organisation oder aus dem delegierten Administratorkonto des Kontoverwaltungsdienstes verwenden.

Beispielanforderung

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Beispielantwort

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWSSDK für V3 JavaScript
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

PutContactInformation

Aktualisiert die primären Kontaktinformationen einesAWS-Konto.

Vollständige Informationen zur Verwendung der primären Kontaktfunktionen finden Sie unter Aktualisieren der primären und alternativen Kontaktinformationen.

Anforderungssyntax

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

URI-Anfrageparameter

Die Anforderung verwendet keine URI-Parameter.

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

AccountId

Gibt die 12-stellige Konto-ID-Nummer der Person an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. Wenn Sie diesen Parameter nicht angeben, wird

standardmäßig die Identität verwendet, die zum Aufrufen AWS-Konto des Vorgangs verwendet wurde. Um diesen Parameter verwenden zu können, muss es sich bei dem Anrufer um eine Identität im Verwaltungskonto der Organisation oder um ein delegiertes Administratorkonto handeln. Bei der angegebenen Konto-ID muss es sich auch um ein Mitgliedskonto in derselben Organisation handeln. Für die Organisation müssen alle Funktionen aktiviert sein und für die Organisation muss der vertrauenswürdige Zugriff für den Kontoverwaltungsdienst aktiviert und optional ein delegiertes Administratorkonto zugewiesen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben. Es muss den Vorgang im eigenständigen Kontext aufrufen, ohne den `AccountId` Parameter einzubeziehen.

Um diesen Vorgang für ein Konto aufzurufen, das nicht Mitglied einer Organisation ist, geben Sie diesen Parameter nicht an. Rufen Sie den Vorgang stattdessen mit einer Identität auf, die zu dem Konto gehört, dessen Kontakte Sie abrufen oder ändern möchten.

Typ: Zeichenfolge

Pattern: `^\d{12}$`

Required: No

ContactInformation

Enthält die Details der primären Kontaktinformationen, die mit einem verknüpft sindAWS-Konto.

Typ: ContactInformation Objekt

Erforderlich: Ja

Antwortsyntax

```
HTTP/1.1 200
```

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP 200-Antwort mit leerem HTTP-Textinhalt zurück.

Fehler

Informationen zu den Fehlern, die allen Aktionen gemeinsam sind, finden Sie unterHäufige Fehler.

AccessDeniedException

Der Vorgang ist fehlgeschlagen, da die aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagenAWS. Versuchen Sie den Vorgang später erneut.

HTTP Status Code: 500

TooManyRequestsException

Der Vorgang ist fehlgeschlagen, weil er zu häufig aufgerufen wurde und eine Drosselungsgrenze überschritten wurde.

HTTP-Statuscode: 429

ValidationException

Der Vorgang ist fehlgeschlagen, weil einer der Eingabeparameter ungültig war.

HTTP Status Code: 400

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-Befehlszeilenschnittstelle
- AWS-SDK für .NET
- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2

- AWSSDK für JavaScript V3
- AWS SDK für PHP V3
- AWS SDK für Python
- AWS SDK für Ruby V3

Verwandte Aktionen in anderenAWSDienstleistungen

Die folgenden Operationen beziehen sich aufAWS Account Managementsind aber Teil desAWS OrganizationsNamespace:

- CreateAccount
- createGovCloudAccount
- DescribeAccount

CreateAccount

Die`CreateAccount`Der API-Betrieb kann nur im Kontext einer Organisation verwendet werden, die von derAWS OrganizationsService-Service Der API-Vorgang ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie unterCreateAccountimAWS Organizations-API-Referenzaus.

createGovCloudAccount

Die`CreateGovCloudAccount`Der API-Betrieb kann nur im Kontext einer Organisation verwendet werden, die von derAWS OrganizationsService. Der API-Vorgang ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie untercreateGovCloudAccountimAWS Organizations-API-Referenzaus.

DescribeAccount

Die`DescribeAccount`Der API-Betrieb kann nur im Kontext einer Organisation verwendet werden, die von derAWS OrganizationsService. Der API-Vorgang ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie unterDescribeAccountimAWS Organizations-API-Referenzaus.

Datentypen

Die folgenden Datentypen werden unterstützt:

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

Eine Struktur, die die Details eines alternativen Kontakts enthält, der einem AWS Konto zugeordnet ist

Inhalt

AlternateContactType

Die Art des alternativen Kontakts.

Typ: Zeichenfolge

Zulässige Werte: `BILLING | OPERATIONS | SECURITY`

Required: No

EmailAddress

Die E-Mail-Adresse, die mit diesem alternativen Kontakt verknüpft ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 64 Zeichen.

Pattern: `^[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*$`

Erforderlich: Nein

Name

Der Name, der diesem alternativen Kontakt zugeordnet ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 64 Zeichen.

Required: No

PhoneNumber

Die mit diesem alternativen Kontakt verknüpfte Telefonnummer.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge von 25.

Pattern: `^[\s0-9()+-]+$`

Erforderlich: Nein

Title

Der Titel, der diesem alternativen Kontakt zugeordnet ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Höchstlänge = 50 Zeichen.

Required: No

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWS SDK für Ruby V3

ContactInformation

Enthält die Details der primären Kontaktinformationen, die mit einem verknüpft sindAWS-Konto.

Inhalt

AddressLine1

Die erste Zeile der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Die maximale Länge beträgt 60.

Erforderlich: Ja

City

Die Stadt der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Ja

CountryCode

Der zweibuchstabige ISO-3166-Ländercode für die primäre Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Feste Länge von 2.

Erforderlich: Ja

FullName

Der vollständige Name der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Ja

PhoneNumber

Die Telefonnummer der primären Kontaktinformationen. Die Nummer wird validiert und in einigen Ländern auf Aktivierung überprüft.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge von 20.

Pattern: `^[+][\s0-9()-]+$`

Erforderlich: Ja

PostalCode

Die Postleitzahl der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge von 20.

Erforderlich: Ja

AddressLine2

Die zweite Zeile der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Die maximale Länge beträgt 60.

Erforderlich: Nein

AddressLine3

Die dritte Zeile der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Die maximale Länge beträgt 60.

Erforderlich: Nein

CompanyName

Der Name des Unternehmens, das mit den primären Kontaktinformationen verknüpft ist, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Nein

DistrictOrCounty

Der Bezirk oder Bezirk der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Nein

StateOrRegion

Das Bundesland oder die Region der primären Kontaktadresse. Wenn sich die Postanschrift in den Vereinigten Staaten (USA) befindet, kann der Wert in diesem Feld entweder ein zweistelliger Landescode (z. B.`NJ`) oder der vollständige Name des Bundesstaates (z. B.`New Jersey`) sein. Dieses Feld ist in den folgenden Ländern erforderlich: `US`CA, `GB`DE,`JP`,`IN`, und`BR`.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Nein

WebsiteUrl

Die URL der Website, die mit den primären Kontaktinformationen verknüpft ist, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 256 Zeichen.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWS-SDK für Ruby V3

Region

Dies ist eine Struktur, die die Region für ein bestimmtes Konto ausdrückt und aus einem Namen und einem Opt-in-Status besteht.

Inhalt

RegionName

Der Regionalcode einer bestimmten Region (z. B.`us-east-1`).

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 50 Zeichen.

Erforderlich: Nein

RegionOptStatus

Einer der möglichen Status, den eine Region haben kann (Aktiviert, Aktiviert, Deaktiviert, Deaktiviert, Deaktiviert, Enabled_By_Default).

Typ: Zeichenfolge

Zulässige Werte: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Erforderlich: Nein

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-SDK für C++
- AWS-SDK für Go
- AWS-SDK für Java V2
- AWS-SDK für Ruby V3

ValidationExceptionField

Die Eingabe entsprach nicht den vomAWS Dienst in einem bestimmten Feld angegebenen Einschränkungen.

Inhalt

message

Eine Meldung über die Validierungsausnahme.

Typ: Zeichenfolge

Erforderlich: Ja

name

Der Feldname, in dem der ungültige Eintrag erkannt wurde.

Typ: Zeichenfolge

Erforderlich: Ja

Weitere Informationen finden Sie unter:

Weitere Informationen zur Verwendung dieser API in einem der sprachspezifischen AWS-SDKs finden Sie unter:

- AWS-SDK für C++
- AWS-SDK for Go
- AWS-SDK für Java V2
- AWS SDK für Ruby V3

Geläufige Parameter

Die folgende Liste enthält die Parameter, die alle Aktionen zum Signieren von Signature-Version-4-Anforderungen mit einer Abfragezeichenfolge verwenden. Alle aktionsspezifischen Parameter werden im Thema für diese Aktion aufgelistet. Weitere Informationen zu Signature Version 4 finden Sie unter Signieren vonAWS API-Anfragen im IAM-Benutzerhandbuch.

Action

Die auszuführende Aktion.

Typ: Zeichenfolge

Erforderlich: Ja

Version

Die API-Version, für die die Anforderung geschrieben wurde, ausgedrückt im Format JJJJ-MM-TT.

Typ: Zeichenfolge

Erforderlich: Ja

X-Amz-Algorithm

Der Hashalgorithmus, den Sie zum Erstellen der Anforderungssignatur verwendet haben.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Zulässige Werte: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

Der Wert des Anmeldeinformationsumfangs. Dabei handelt es sich um eine Zeichenfolge, die Ihren Zugriffsschlüssel, das Datum, die gewünschte Region und eine Zeichenfolge zur Beendigung („aws4_request“) beinhaltet. Der Wert wird im folgenden Format ausgedrückt: Zugriffsschlüssel/JJJJMMTT/Region/Service/aws4_request.

Weitere Informationen finden Sie unter Erstellen einer signiertenAWS API-Anfrage im IAM-Benutzerhandbuch.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Date

Das Datum, das zum Erstellen der Signatur verwendet wird. Das Format muss das ISO 8601-Basisformat (JJJJMMTT'T'SSMMSS'Z') sein. Die folgende Datumszeit ist beispielsweise ein gültiger X-Amz-Date-Wert: `20120325T120000Z`.

Bedingung: X-Amz-Date ist bei allen Anforderungen optional. Damit kann das Datum überschrieben werden, das zum Signieren von Anforderungen verwendet wird. Wenn der Date-Header im ISO 8601-Basisformat angegeben ist, ist X-Amz-Date nicht erforderlich. Wenn X-Amz-Date verwendet wird, überschreibt es immer den Wert des Date-Headers. Weitere Informationen finden Sie unter Elemente einerAWS API-Anforderungssignatur im IAM-Benutzerhandbuch.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Security-Token

Das temporäre Sicherheitstoken, das durch einen Anruf vonAWS Security Token Service (AWS STS) abgerufen wurde. Eine Liste der Services, die temporäre Sicherheitsanmeldeinformationen von unterstützenAWS STS AWS-Services, finden Sie unter, die mit IAM arbeiten im IAM-Benutzerhandbuch.

Bedingung: Wenn Sie temporäre Sicherheitsanmeldeinformationen von nutzenAWS STS, müssen Sie das Sicherheitstoken einschließen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Signature

Gibt die hex-codierte Signatur an, die aus der zu signierenden Zeichenfolge und dem abgeleiteten Signaturschlüssel berechnet wurde.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

X-Amz-SignedHeaders

Gibt alle HTTP-Header an, die als Teil der kanonischen Anforderung enthalten waren. Weitere Informationen zur Angabe signierter Header finden Sie unter Erstellen einer signiertenAWS API-Anfrage im IAM-Benutzerhandbuch.

Bedingung: Geben Sie diesen Parameter an, wenn Sie Authentifizierungsinformationen in eine Abfragezeichenfolge anstatt in den HTTP-Autorisierungsheader aufnehmen.

Typ: Zeichenfolge

Required: Conditional

Häufige Fehler

In diesem Abschnitt sind Fehler aufgeführt, die häufig bei den API-Aktionen aller AWS-Services auftreten. Informationen zu Fehlern, die spezifisch für eine API-Aktion für diesen Service sind, finden Sie unter dem Thema für diese API-Aktion.

AccessDeniedException

Sie haben keinen ausreichenden Zugriff zum Durchführen dieser Aktion.

HTTP Status Code: 400

IncompleteSignature

Die Anforderungssignatur entspricht nicht den AWS-Standards.

HTTP Status Code: 400

InternalFailure

Die Anforderungsverarbeitung ist fehlgeschlagen, da ein unbekannter Fehler, eine Ausnahme oder ein Fehler aufgetreten ist.

HTTP Status Code: 500

InvalidAction

Die angeforderte Aktion oder Operation ist ungültig. Überprüfen Sie, ob die Aktion ordnungsgemäß eingegeben wurde.

HTTP Status Code: 400

InvalidClientTokenId

Das angegebene X.509-Zertifikat oder die AWS-Zugriffsschlüssel-ID ist nicht in unseren Datensätzen vorhanden.

HTTP Status Code: 403

NotAuthorized

Sie haben keine Berechtigung zum Ausführen dieser Aktion.

HTTP Status Code: 400

OptInRequired

Die AWS-Zugriffsschlüssel-ID benötigt ein Abonnement für den Service.

HTTP Status Code: 403

RequestExpired

Die Anforderung hat den Service mehr als 15 Minuten nach dem Datumsstempel oder mehr als 15 Minuten nach dem Ablaufdatum der Anforderung erreicht (z. B. für vorsignierte URLs) oder der Datumsstempel auf der Anforderung liegt mehr als 15 Minuten in der Zukunft.

HTTP Status Code: 400

ServiceUnavailable

Die Anforderung ist aufgrund eines temporären Fehlers des Servers fehlgeschlagen.

HTTP Status Code: 503

ThrottlingException

Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt.

HTTP Status Code: 400

ValidationError

Die Eingabe erfüllt nicht die von einem AWS-Service definierten Einschränkungen.

HTTP Status Code: 400

Aufrufen der API mittels HTTP-Abfrageanforderungen

Dieser Abschnitt enthält allgemeine Informationen zur Verwendung der Abfrage-API fürAWSKontoverwaltung. Weitere Informationen über die API-Vorgänge und Fehler finden Sie in der API-Referenz.

> **Note**
>
> Anstatt direkt an die zu telefonierenAWSAccount Management Query API, Sie können eine derAWSSDKs. Die AWS-SDKs bestehen aus Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen (darunter Java, Ruby, .NET, iOS und Android). Die SDKs bieten eine bequeme Möglichkeit, programmatischen Zugriff aufAWSKontoverwaltung undAWS. Mithilfe der SDKs lassen sich unter anderem Anforderungen kryptografisch signieren, Fehler verwalten und Anforderungen automatisch wiederholen. Weitere Informationen über die AWS-SDKs, das Herunterladen und die Installation finden Sie unter Tools für Amazon Web Services.

Mit der Abfrage-API fürAWSKontoverwaltung, Sie können Serviceaktionen aufrufen. Abfrage-API-Anfragen sind HTTPS-Anfragen, die eine enthalten müssen`Action`Parameter zur Angabe der auszuführenden Operation.AWS Account Management unterstützt`GET`und`POST`Anfragen für alle Operationen. Das heißt, Sie müssen die API nicht verwenden`GET`für einige Aktionen und`POST`für andere. Jedoch`GET`Anfragen unterliegen der Größenbeschränkung einer URL. Dieses Limit ist zwar browserabhängig, ein typisches Limit liegt jedoch bei 2.048 Byte. Daher müssen Sie für Abfrage-API-Anfragen, die größere Größen erfordern, eine`POST`Anfrage.

Die Antwort erfolgt in Form eines XML-Dokuments. Weitere Informationen über die Antwort finden Sie auf den Seiten zu den einzelnen Aktionen in der API-Referenz.

Themen

- Endpunkte
- HTTPS erforderlich
- SignierenAWSAPI-Anfragen zur Kontoverwaltung

Endpunkte

AWSAccount Management verfügt über einen einzigen globalen API-Endpunkt, der im Osten der USA (Nord-Virginia) gehostet wird.AWS-Region.

Weitere Informationen zu AWS-Endpunkten und -Regionen für alle Services finden Sie unter Regionen und Endpunkte im Allgemeine AWS-Referenz.

HTTPS erforderlich

Da die Abfrage-API vertrauliche Informationen wie Sicherheitsanmeldeinformationen zurückgeben kann, müssen Sie HTTPS verwenden, um alle API-Anfragen zu verschlüsseln.

SignierenAWSAPI-Anfragen zur Kontoverwaltung

Anforderungen müssen über eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel signiert werden. Wir empfehlen Ihnen dringend, Ihre nicht zu verwendenAWSAnmeldedaten für das Root-Konto für die tägliche Arbeit mitAWSKontoverwaltung. Sie können die Anmeldeinformationen verwenden für eineAWS Identity and Access Management(IAM-) Benutzer- oder temporäre Anmeldeinformationen, wie Sie sie für eine IAM-Rolle verwenden.

Zum Signieren von API-Anforderungen müssen Sie Signature Version 4 für AWS verwenden. Weitere Informationen zur Verwendung von Signature Version 4 finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Weitere Informationen finden Sie hier:

- AWS-Sicherheitsanmeldeinformationen – Bietet allgemeine Informationen zu den Arten der Anmeldeinformationen, mit denen Sie auf AWS zugreifen können.
- Bewährte Sicherheitsmethoden in IAM— Bietet Vorschläge zur Verwendung des IAM-Dienstes zum Schutz IhresAWSRessourcen, einschließlich derer inAWSKontoverwaltung.
- Temporäre Sicherheitsanmeldeinformationen in IAM – Beschreibt die Erstellung und Verwendung von temporären Sicherheitsanmeldeinformationen.

Kontingente für AWS Account Management

Das AWS-Konto verfügt über Standardkontingente (früher als Limits bezeichnet) für jeden AWS-Service. Sofern nicht anders angegeben, ist jedes Kontingent AWS-Region -spezifisch.

Jedes AWS-Konto hat die folgenden Kontingente, die sich auf die Kontoverwaltung beziehen.

Ressource	Kontingent
Anzahl der alternativen Kontakte in einem AWS-Konto	3 — jeweils einer für `BILLINGSECURITY`, und `OPERATIONS`
Anzahl gleichzeitiger Region-Opt-Anfragen pro Konto	6
Anzahl gleichzeitiger Region-Opt-Anfragen pro Organisation	20
Rate der Anfragen pro Konto `DeleteAlternateContact`	1 pro Sekunde, Burst auf 6 pro Sekunde
Rate der `DisableRegion` Anfragen pro Konto	1 pro Sekunde, Burst auf 1 pro Sekunde
Rate der `EnableRegion` Anfragen pro Konto	1 pro Sekunde, Burst auf 1 pro Sekunde
Rate der `GetAlternateContact` Anfragen pro Konto	10 pro Sekunde, Burst auf 15 pro Sekunde
Rate der `GetContactInformation` Anfragen pro Konto	10 pro Sekunde, Burst auf 15 pro Sekunde
Rate der `GetRegionOptStatus` Anfragen pro Konto	5 pro Sekunde, Burst auf 5 pro Sekunde
Rate der `ListRegions` Anfragen pro Konto	5 pro Sekunde, Burst auf 5 pro Sekunde
Rate der `PutAlternateContact` Anfragen pro Konto	5 pro Sekunde, Burst auf 8 pro Sekunde

Ressource	Kontingent
Rate der `PutContactInformation` Anfragen pro Konto	5 pro Sekunde, Burst auf 8 pro Sekunde

Fehlerbehebung bei Ihrem AWS-Konto

Verwenden Sie die Informationen in den folgenden Themen, um Probleme mit Ihrem zu diagnostizieren und zu behebenAWS-Konto. Hilfe zum Root-Benutzer finden Sie unter Beheben von Problemen mit dem Root-Benutzer im IAM-Benutzerhandbuch. Hilfe zum Anmeldevorgang finden Sie unter Beheben von AWS-Konto Anmeldeproblemen im AWS Benutzerhandbuch für die Anmeldung.

Themen zur Fehlerbehebung

- Behebung von Problemen bei der AWS-Konto Erstellung
- Fehlerbehebung bei Problemen mit AWS-Konto der Schließung
- Beheben von anderen Problemen mitAWS-Konten

Behebung von Problemen bei der AWS-Konto Erstellung

Verwenden Sie die Informationen hier, um Probleme im Zusammenhang mit der Erstellung eines zu behebenAWS-Konto. Falls Sie Probleme bei der Anmeldung bei Ihrem neuen Konto haben sollten, nachdem es erstellt wurde, finden Sie weitere Informationen unter Problembehebung bei der AWS-Konto Anmeldung im AWSAnmeldehandbuch.

Problembereiche

- Ich habe den Anruf von AWS zur Bestätigung meines neuen Kontos nicht erhalten
- Ich erhalte die Fehlermeldung „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine Versuche AWS-Konto telefonisch zu verifizieren
- Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert

Ich habe den Anruf von AWS zur Bestätigung meines neuen Kontos nicht erhalten

Wenn Sie eine erstellenAWS-Konto, müssen Sie eine Telefonnummer angeben, unter der Sie entweder eine SMS-Nachricht oder einen Sprachanruf erhalten können. Sie geben an, mit welcher Methode die Nummer verifiziert werden soll.

Wenn Sie die Nachricht oder den Anruf nicht erhalten, überprüfen Sie Folgendes:

- Sie haben bei der Registrierung die richtige Telefonnummer eingegeben und die richtige Landesvorwahl ausgewählt.
- Wenn Sie ein Mobiltelefon verwenden, stellen Sie sicher, dass Sie über ein Mobilfunksignal verfügen, mit dem Sie SMS-Nachrichten oder Anrufe empfangen können.
- Die Informationen, die Sie für Ihre Zahlungsmethode eingegeben haben, sind korrekt.

Wenn Sie keine SMS oder keinen Anruf erhalten haben, um den Identitätsprüfungsprozess abzuschließen, AWS Support kann Ihnen dies bei der AWS-Konto manuellen Aktivierung helfen. Gehen Sie dazu wie folgt vor:

1. Stellen Sie sicher, dass Sie unter der Telefonnummer erreichbar sind, die Sie für Ihre angegeben habenAWS-Konto.
2. Öffnen Sie die AWS SupportKonsole und wählen Sie dann Kundenvorgang erstellen aus.
   a. Wählen Sie Konto- und -Rechnungssupportservice aus.
   b. Wählen Sie als Typ die Option Konto aus.
   c. Wählen Sie als Kategorie die Option Aktivierung aus.
   d. Geben Sie im Abschnitt Fallbeschreibung ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.
   e. Wählen Sie im Abschnitt Kontaktoptionen die Option Chat für Kontaktmethoden aus.
   f. Wählen Sie Absenden aus.

> **Note**
>
> Sie können einen Kundenvorgang mit erstellen, AWS Support auch wenn Ihr AWS-Konto Konto noch nicht aktiviert ist.

Ich erhalte die Fehlermeldung „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine Versuche AWS-Konto telefonisch zu verifizieren

AWS Supportkann Ihnen helfen, Ihr Konto manuell zu aktivieren. Dazu gehen Sie wie folgt vor:

1. Melden Sie sich AWS-Konto mit der E-Mail-Adresse und dem Passwort an, die Sie bei der Erstellung Ihres Kontos angegeben haben.
2. Öffnen Sie die AWS SupportKonsole und wählen Sie dann Kundenvorgang erstellen aus.
3. Wählen Sie Konto- und Abrechnungssupport.
4. Wählen Sie als Typ die Option Konto aus.
5. Wählen Sie als Kategorie die Option Aktivierung aus.
6. Geben Sie im Abschnitt Fallbeschreibung ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.
7. Wählen Sie im Abschnitt Kontaktoptionen die Option Chat für Kontaktmethoden aus.
8. Wählen Sie Absenden aus.

AWS Supportwird sich mit Ihnen in Verbindung setzen und versuchen, Ihre manuell zu aktivierenAWS-Konto.

Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert

Die Kontoaktivierung kann sich manchmal verzögern. Wenn der Vorgang länger als 24 Stunden dauert, überprüfen Sie Folgendes:

- Beenden Sie den Kontoaktivierungsprozess.

  Wenn Sie das Fenster für den Anmeldevorgang geschlossen haben, bevor Sie alle erforderlichen Informationen hinzugefügt haben, öffnen Sie die Registrierungsseite. Wählen Sie Bei vorhandenem AWS-Konto Konto anmelden und melden Sie sich mit der E-Mail-Adresse und dem Passwort an, die Sie für das Konto ausgewählt haben.
- Überprüfe die mit deiner Zahlungsmethode verknüpften Informationen.

  Überprüfen Sie in der AWS Billing and Cost Management Konsole die Zahlungsmethoden auf Fehler.
- Wenden Sie sich an Ihr Finanzinstitut.

  Manchmal lehnen Finanzinstitute Autorisierungsanfragen von abAWS. Wenden Sie sich an die Institution, die mit Ihrer Zahlungsmethode verknüpft ist, und bitten Sie sie, Autorisierungsanfragen von zu genehmigenAWS. AWSstorniert die Autorisierungsanfrage, sobald sie von Ihrem Finanzinstitut genehmigt wurde, sodass Ihnen die Autorisierungsanfrage nicht in Rechnung gestellt

wird. Autorisierungsanfragen können auf den Kontoauszügen Ihres Finanzinstituts dennoch als geringe Gebühr (normalerweise 1 USD) erscheinen.

- Suchen Sie in Ihrem E-Mail- und Spam-Ordner nach Anfragen nach weiteren Informationen.
- Versuchen Sie es mit einem anderen Browser.
- KontaktAWS Support.

  Kontakt AWS Supportfür Hilfe. Erwähnen Sie alle Schritte zur Fehlerbehebung, die Sie bereits versucht haben.

> **Note**
>
> Geben Sie in keiner Korrespondenz mit vertraulichen Informationen wie Kreditkartennummern anAWS.

Fehlerbehebung bei Problemen mit AWS-Konto der Schließung

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die während der Kontoschließung gefunden wurden. Allgemeine Informationen zum Kontoschließungsprozess finden Sie unter Schließe eine AWS-Konto.

Themen

- Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann
- Ich sehe die Schaltfläche Konto schließen auf der Seite Konten nicht
- Ich habe mein Konto geschlossen, aber immer noch keine E-Mail-Bestätigung erhalten
- Ich erhalte die Fehlermeldung „ConstraintViolationException“, wenn ich versuche, mein Konto zu schließen
- Ich erhalte die Fehlermeldung „CLOSE_ACCOUNT_QUOTA_EXCEED“, wenn ich versuche, ein Mitgliedskonto zu schließen
- Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließen kann?

Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann

Um Ihr Konto zu schließen, folgen Sie den Anweisungen unter Schließe eine AWS-Konto.

Ich sehe die Schaltfläche Konto schließen auf der Seite Konten nicht

Wenn Sie nicht als Stammbenutzer angemeldet sind, wird die Schaltfläche Konto schließen auf der Seite Konten nicht angezeigt. Sie müssen sich bei der AWS Management Console als Root-Benutzer anmelden, um Ihr Konto zu schließen. Wenn Sie sich nicht anmelden können, finden Sie weitere Informationen unter Fehlerbehebung bei Problemen mit dem Root-Benutzer .

Ich habe mein Konto geschlossen, aber immer noch keine E-Mail-Bestätigung erhalten

Diese Bestätigungs-E-Mail wird nur an die E-Mail-Adresse des Root-Benutzers des gesendet AWS-Konto. Wenn Sie diese E-Mail nicht innerhalb weniger Stunden erhalten, können Sie sich bei der AWS Management Console als Root-Benutzer anmelden, um zu überprüfen, ob Ihr Konto geschlossen ist. Wenn Ihr Konto erfolgreich geschlossen wurde, wird eine Meldung angezeigt, die angibt, dass Ihr Konto geschlossen wurde. Wenn das geschlossene Konto ein Mitgliedskonto ist, können Sie überprüfen, ob das geschlossene Konto `SUSPENDED` in der AWS Organizations Konsole als gekennzeichnet ist. Weitere Informationen finden Sie unter Schließen eines Mitgliedskontos in Ihrer Organisation im AWS Organizations -Benutzerhandbuch.

Wenn Sie versuchen, ein Verwaltungskonto zu schließen und keine E-Mail-Bestätigung über die Kontoschließung erhalten, verfügt Ihre Organisation höchstwahrscheinlich über aktive Mitgliedskonten. Sie können das Verwaltungskonto nur schließen, wenn Ihre Organisation keine aktiven Mitgliedskonten hat. Um zu überprüfen, ob in Ihrer Organisation keine aktiven Mitgliedskonten mehr vorhanden sind, rufen Sie die - AWS Organizations Konsole auf und stellen Sie sicher, dass alle Mitgliedskonten `Suspended` neben ihren Kontonamen angezeigt werden. Danach können Sie das Verwaltungskonto schließen.

Ich erhalte die Fehlermeldung „ConstraintViolationException“, wenn ich versuche, mein Konto zu schließen

Sie versuchen, ein Verwaltungskonto mit der AWS Organizations Konsole zu schließen, was nicht möglich ist. Um ein Verwaltungskonto zu schließen, müssen Sie sich bei der AWS Management Console als Stammbenutzer des Verwaltungskontos anmelden und es auf der Seite Konten schließen. Weitere Informationen finden Sie unter Schließen eines Verwaltungskontos in Ihrer Organisation im AWS Organizations -Benutzerhandbuch.

Ich erhalte die Fehlermeldung „CLOSE_ACCOUNT_QUOTA_EXCEED“, wenn ich versuche, ein Mitgliedskonto zu schließen

Sie können nur 10 % der Mitgliedskonten innerhalb eines fortlaufenden Zeitraums von 30 Tagen schließen. Dieses Kontingent ist nicht an einen Kalendermonat gebunden, sondern beginnt, wenn Sie ein Konto schließen. Innerhalb von 30 Tagen nach der ersten Kontoschließung können Sie das Limit von 10 % für die Kontoschließung nicht überschreiten. Die minimale Kontoschließung beträgt 10 und die maximale Kontoschließung 1 000, auch wenn 10 % der Konten 1 000 überschreiten. Weitere Informationen zu Organizations-Kontingenten finden Sie unter Kontingente für AWS Organizations im AWS Organizations -Benutzerhandbuch.

Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließen kann?

Nein, Sie müssen Ihre AWS Organisation nicht löschen, bevor Sie das Verwaltungskonto schließen. Sie können das Verwaltungskonto jedoch nur schließen, wenn Ihre Organisation keine aktiven Mitgliedskonten hat. Um zu überprüfen, ob in Ihrer Organisation keine aktiven Mitgliedskonten mehr vorhanden sind, rufen Sie die - AWS Organizations Konsole auf und stellen Sie sicher, dass alle Mitgliedskonten `Suspended` neben ihren Kontonamen angezeigt werden. Danach können Sie das Verwaltungskonto schließen.

Beheben von anderen Problemen mitAWS-Konten

Verwenden Sie die Informationen hier, um Sie bei der Behandlung von Problemen im Zusammenhang mit IhremAWS-Kontoaus.

Problembereiche

- Ich muss die Kreditkarte für meine ändernAWS-Konto
- Ich muss betrügerisch meldenAWS-KontoAktivität
- Ich muss meine schließenAWS-Konto

Ich muss die Kreditkarte für meine ändernAWS-Konto

So ändern Sie die Kreditkarte für IhreAWS-Konto, müssen Sie sich anmelden können.AWSverfügt über Schutzmaßnahmen, bei denen Sie nachweisen müssen, dass Sie der Kontoinhaber sind.

Detaillierte Anweisungen finden Sie unterVerwalten von KreditkartenzahlungsartenimAWS Billing-Benutzerhandbuchaus.

Ich muss betrügerisch meldenAWS-KontoAktivität

Wenn Sie betrügerische Aktivitäten mit Ihrem Verdacht habenAWS-Kontound möchte einen Bericht erstellen, siheWie melde ich Missbrauch vonAWSRessourcenaus.

Wenn Sie Probleme mit einem Kauf auf Amazon.de haben, finden Sie unterAmazon-Kundenserviceaus.

Ich muss meine schließenAWS-Konto

Wenn Sie Hilfe bei der Behebung von Problemen beim Schließen IhresAWS-Konto, finden Sie unterSchließe eine AWS-Kontoaus.

Dokumentverlauf für das Benutzerhandbuch zur Kontoverwaltung

In der folgenden Tabelle werden die Dokumentationsversionen für AWS Account Management beschrieben.

Änderung	Beschreibung	Datum
Umschreiben des Themas Konto schließen	Das gesamte Thema zum Schließen von Konten wurde vollständig überarbeitet, einschließlich der Schritte zum Schließen von Mitglieds- und Verwaltungskonten.	1. Februar 2024
Ende der Unterstützung für das Hinzufügen neuer Sicherheitsabfragen	Es wurde ein neuer Inhalt hinzugefügt, in dem darauf hingewiesen wird, dass die Option zum Hinzufügen neuer Aufforderungsfragen von der Seite Konten entfernt wurde.	5. Januar 2024
Ende der Unterstützung für den `aws-portal` Namespace	AWS Identity and Access Management (IAM)-Aktionen, die zuvor zur Verwaltung Ihres Kontos verwendet wurden (z. B. `aws-portal:ModifyAccount` und `aws-portal:ViewAccount`), haben das Ende des Standard-Supports erreicht.	1. Januar 2024
Umschreiben des Themas Regionen	Das gesamte Thema der Regionen einschließlich des Hinzufügens von Erweiterungs- und Eingrenzungskontro	8. Oktober 2023

	llen wurde vollständig überlastet.	
Stammbenutzerthemen wurden in das IAM-Benutzerhandbuch verschoben	Die Diskussion über Root-Benutzer wurde in einem Thema zusammengefasst und es wurden Querverweise auf Root-Benutzerthemen hinzugefügt, die in das IAM-Benutzerhandbuch verschoben wurden.	18. September 2023
Neuer Abschnitt zum Kontaktthema des primären Kontos hinzugefügt	Neuer Abschnitt mit den Anforderungen an Telefonnummern und E-Mail-Adressen hinzugefügt.	12. September 2023
Neue Kontaktinformations-APIs	Unterstützung für neue - `GetContactInformation` und -`PutContactInformation` APIs. APIs	22. Juli 2022
AWS Die Kontoverwaltung unterstützt jetzt die Aktualisierung alternativer Kontakte über die AWS Organizations Konsole.	Sie können jetzt die alternativen Kontakte Ihrer Organisation über die AWS Organizations Konsole mithilfe von Konto-API-Berechtigungen aktualisieren, die von aktualisierten AWS Organizations verwalteten Richtlinien bereitgestellt werden.	8. Februar 2022
Erstversion	Erste Version des Referenzhandbuchs zur AWS Kontoverwaltung	30. September 2021

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.