Referenzhandbuch

AWS Verwaltung von Benutzerkonten

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

AWS Verwaltung von Benutzerkonten: Referenzhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist ein AWS-Konto? ... 1
Merkmale eines AWS-Konto ... 3
Benutzen Sie das Produkt zum ersten Mal? AWS ... 3
Verbundene AWS Dienstleistungen ... 4
Verwenden des Root-Benutzers ... 5
Support und Feedback ... 5
Andere AWS Ressourcen ... 6
Erste Schritte mit deinem Konto ... 7
Überprüfen Sie die Voraussetzungen ... 7
Schritt 1: Erstelle dein Konto ... 8
Schritt 2: MFA für Ihren Root-Benutzer aktivieren ... 11
Schritt 3: Erstellen Sie einen Administratorbenutzer ... 12
Verwandte Themen ... 12
Zugriff auf Ihr -Konto ... 12
Planen Sie Ihre Führungsstruktur ... 14
Vorteile der Verwendung mehrerer AWS-Konten ... 14
Verwaltung mehrerer AWS-Konten ... 15
Wann zu verwenden AWS Organizations ... 16
Den vertrauenswürdigen Zugriff aktivieren ... 17
Aktivieren Sie ein delegiertes Administratorkonto ... 19
Beschränken Sie den Zugriff mit SCPs ... 20
Wann zu verwenden AWS Control Tower ... 22
Grundlegendes zu API-Betriebsmodi ... 23
Erteilen von Berechtigungen zum Aktualisieren von Kontoattributen ... 24
Konfiguriere dein Konto ... 27
Erstelle oder aktualisiere deinen Account-Alias ... 27
AWS-Regionen In Ihrem Konto aktivieren oder deaktivieren ... 27
Überlegungen vor dem Aktivieren und Deaktivieren von Regionen ... 29
Aktiviere oder deaktiviere eine Region für eigenständige Konten ... 32
Aktivieren oder deaktivieren Sie eine Region in Ihrer Organisation ... 34
Aktualisieren Sie die Abrechnung für Ihre AWS-Konto ... 37
Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () ... 37
Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für einen eigenständigen Benutzer AWS-Konto ... 38

Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für alle Benutzer AWS-Konto in Ihrer Organisation ... 39
Root-Benutzerpasswort aktualisieren ... 43
Aktualisiere deinen AWS-Konto Namen ... 43
Aktualisieren Sie Ihren Kontonamen für ein eigenständiges AWS-Konto ... 44
Aktualisieren Sie Ihren Kontonamen für alle Konten AWS-Konto in Ihrer Organisation ... 46
Aktualisieren Sie die alternativen Kontakte für Ihre AWS-Konto ... 48
Anforderungen an Telefonnummer und E-Mail-Adresse ... 49
Aktualisieren Sie die alternativen Kontakte für eine eigenständige Version AWS-Konto ... 49
Aktualisieren Sie die alternativen Kontakte für alle Kontakte AWS-Konto in Ihrer Organisation ... 53
Konto: AlternateContactTypes Kontextschlüssel ... 57
Aktualisieren Sie den Hauptansprechpartner für Ihren AWS-Konto ... 57
Anforderungen an Telefonnummer und E-Mail-Adresse ... 58
Aktualisieren Sie den Hauptkontakt für ein eigenständiges Konto AWS-Konto ... 59
Aktualisieren Sie den Hauptansprechpartner für alle Kontakte AWS-Konto in Ihrer Organisation ... 61
Sehen Sie sich Ihre Kontokennungen an ... 64
Finden Sie Ihren AWS-Konto Ausweis ... 65
Finden Sie die kanonische Benutzer-ID für AWS-Konto ... 67
Sichere dein Konto ... 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 ... 80
AWS Kontoverwaltung und IAM ... 83
Beispiele für identitätsbasierte Richtlinien ... 92
Verwenden identitätsbasierter Richtlinien ... 95
Fehlerbehebung ... 98
AWS verwaltete Richtlinien ... 100
AWSAccountManagementReadOnlyAccess ... 101

AWSAccountManagementFullAccess ... 102
Richtlinienaktualisierungen ... 103
Compliance-Validierung ... 103
Ausfallsicherheit ... 104
Sicherheit der Infrastruktur ... 105
Überwachen Sie Ihr Konto ... 106
CloudTrail protokolliert ... 106
Informationen zur Kontoverwaltung in CloudTrail ... 107
Grundlegendes zu den Protokolleinträgen der Kontoverwaltung ... 108
Überwachung von Kontoverwaltungsereignissen mit EventBridge ... 111
Ereignisse zur Kontoverwaltung ... 112
Beheben Sie Probleme mit Ihrem Konto ... 114
Probleme bei der Kontoerstellung ... 114
Probleme mit der Kontoschließung ... 115
Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann ... 116
Ich sehe die Schaltfläche „Konto schließen“ auf der Kontoseite nicht ... 116
Ich habe mein Konto geschlossen, aber immer noch keine E-Mail-Bestätigung erhalten ... 116
Ich erhalte die Fehlermeldung "ConstraintViolationException", wenn ich versuche, mein Konto zu schließen ... 116
Ich erhalte die Fehlermeldung „CLOSE_ACCOUNT_QUOTA_EXCEEDED“, wenn ich versuche, ein Mitgliedskonto zu schließen ... 117
Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließe? ... 117
Sonstige Probleme ... 117
Ich muss die Kreditkarte für meine ändern AWS-Konto ... 118
Ich muss betrügerische AWS-Konto Aktivitäten melden ... 118
Ich muss meine schließen AWS-Konto ... 118
Schließe dein Konto ... 119
Was müssen Sie wissen, bevor Sie Ihr Konto schließen ... 119
Wie schließt du dein Konto ... 121
Was erwartet Sie, nachdem Sie Ihr Konto geschlossen haben ... 125
Zeitraum nach der Schließung ... 125
Wiedereröffnung Ihres AWS-Konto ... 125
API-Referenz ... 127
Aktionen ... 129
AcceptPrimaryEmailUpdate ... 131
DeleteAlternateContact ... 135

DisableRegion ... 140
EnableRegion ... 144
GetAccountInformation ... 148
GetAlternateContact ... 154
GetContactInformation ... 160
GetPrimaryEmail ... 164
GetRegionOptStatus ... 167
ListRegions ... 171
PutAccountName ... 176
PutAlternateContact ... 181
PutContactInformation ... 187
StartPrimaryEmailUpdate ... 191
Zugehörige Aktionen ... 194
CreateAccount ... 194
CreateGovCloudAccount ... 195
DescribeAccount ... 195
Datentypen ... 195
AlternateContact ... 196
ContactInformation ... 198
Region ... 202
ValidationExceptionField ... 203
Geläufige Parameter ... 203
Häufige Fehler ... 206
Erstellen von HTTP-Abfrageanforderungen ... 208
Endpunkte ... 209
HTTPS erforderlich ... 209
API-Anfragen für die AWS Kontoverwaltung signieren ... 209
Kontingente ... 210
Konten in Indien verwalten ... 212
Erstelle eine AWS-Konto mit AWS Indien ... 212
Verwalte deine Informationen zur Kundenverifizierung ... 215
Überprüfen Sie den Status Ihrer Kundenverifizierung ... 215
Erstellen Sie Ihre Informationen zur Kundenverifizierung ... 216
Bearbeiten Sie Ihre Kundenbestätigungsinformationen ... 216
Akzeptierte indische Dokumente zur Kundenverifizierung ... 217
Verwalte dein Konto AWS in Indien ... 219

Dokumentverlauf 221
..... ccxxiv

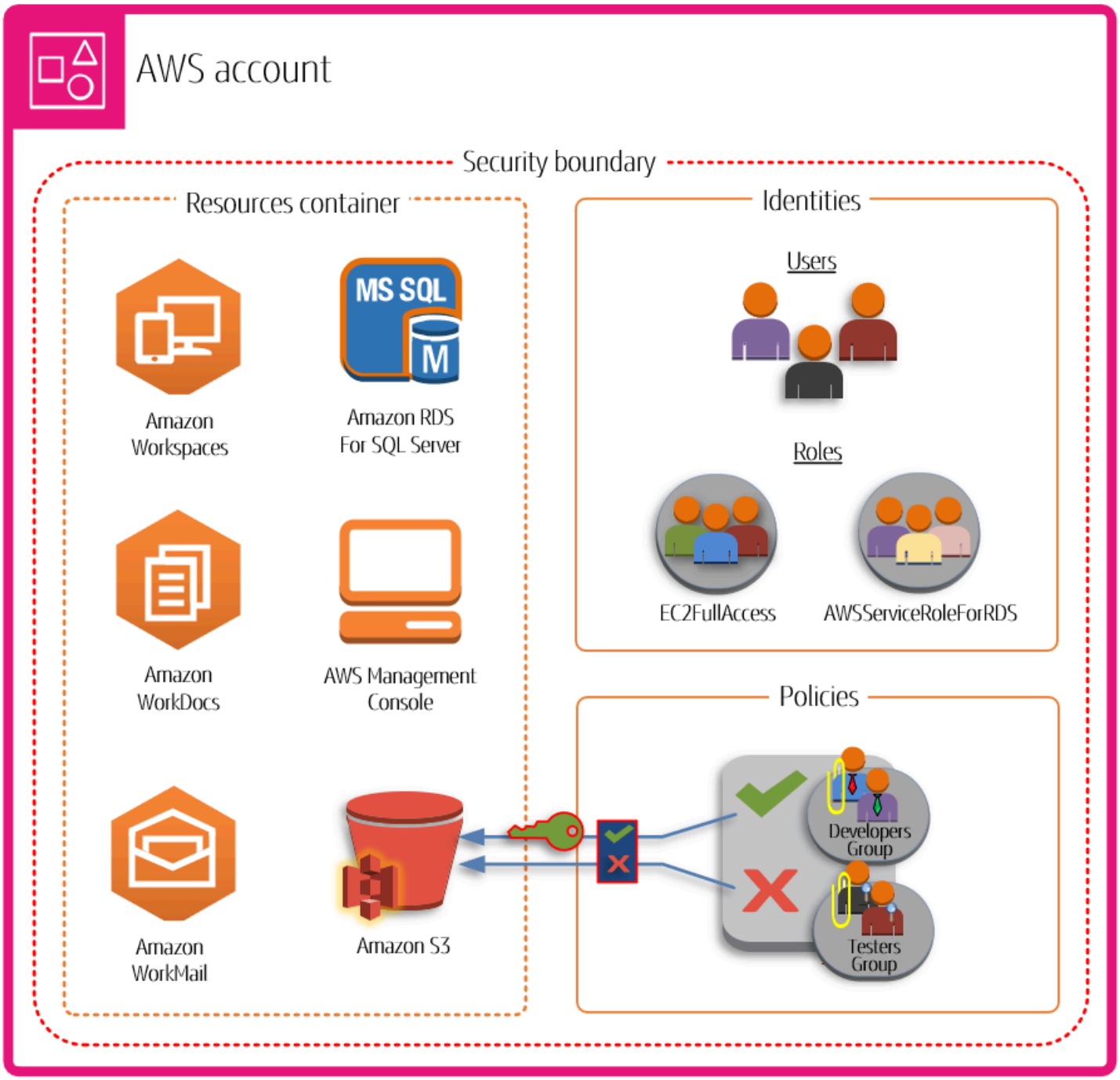
Was ist ein AWS-Konto?

An AWS-Konto steht für eine formelle Geschäftsbeziehung, mit der Sie eine eingehen AWS. Sie erstellen und verwalten Ihre AWS Ressourcen in einem AWS-Konto, und Ihr Konto bietet Identitätsverwaltungsfunktionen für den Zugriff und die Abrechnung. Jedes AWS-Konto hat eine eindeutige ID, die es von anderen AWS-Konten unterscheidet.

Ihre Cloud-Ressourcen und -Daten sind in einem AWS-Konto enthalten. Ein Konto dient als Isolationsgrenze für Identitäts- und Zugriffsmanagement. Wenn Sie Ressourcen und Daten zwischen zwei Konten gemeinsam nutzen müssen, müssen Sie diesen Zugriff ausdrücklich zulassen. Standardmäßig ist kein Zugriff zwischen Konten zulässig. Wenn Sie beispielsweise verschiedene Konten für Ihre Ressourcen und Daten aus der Produktion und anderen Umgebungen angeben, ist standardmäßig kein Zugriff zwischen diesen Umgebungen zulässig.

AWS-Konten sind auch ein grundlegender Bestandteil des Zugriffs auf AWS Dienste. Wie in der folgenden Abbildung dargestellt, AWS-Konto erfüllt ein und zwei Hauptfunktionen:

- Ressourcencontainer — 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 Identitäten verfügen auch über Berechtigungsrichtlinien, die festlegen, was ein Benutzer mit den Ressourcen im Konto tun kann (Autorisierung).



Die Verwendung mehrerer Optionen AWS-Konten ist eine bewährte Methode für die Skalierung Ihrer Umgebung, da sie eine natürliche Abrechnungsgrenze für Kosten bietet, Ressourcen aus Sicherheitsgründen isoliert, Einzelpersonen und Teams Flexibilität bietet und zudem an neue Geschäftsprozesse anpassbar ist. Weitere Informationen finden Sie unter Vorteile der Verwendung mehrerer AWS-Konten.

Merkmale eines AWS-Konto

AWS-Konten umfassen die folgenden Kernfunktionen:

- Kosten überwachen und kontrollieren — Ein Konto ist die Standardmethode, mit der AWS Kosten zugewiesen werden. Aus diesem Grund können Sie durch die Verwendung verschiedener Konten für verschiedene Geschäftsbereiche und Gruppen von Workloads Ihre Cloud-Ausgaben einfacher verfolgen, kontrollieren, prognostizieren, budgetieren und ausweisen. Neben der Kostenberichterstattung auf Kontoebene bietet es AWS auch eine integrierte Unterstützung für die Konsolidierung und Berichterstattung der Kosten für Ihre gesamte Kontogruppe, falls Sie sich AWS Organizations irgendwann dafür entscheiden sollten. Sie können AWS Service Quotas auch verwenden, um sich vor unerwarteter übermäßiger Bereitstellung von AWS Ressourcen und böswilligen Aktionen zu schützen, die sich dramatisch auf Ihre AWS Kosten auswirken könnten.
- Isolationseinheit — An AWS-Konto bietet Sicherheit, Zugriffs- und Abrechnungsgrenzen für Ihre AWS Ressourcen und kann Ihnen so helfen, Ressourcenautonomie und -isolierung zu erreichen. Standardmäßig sind alle in einem Konto bereitgestellten Ressourcen logisch von Ressourcen isoliert, die in anderen Konten bereitgestellt werden, auch in Ihrer eigenen Umgebung. AWS Diese Isolationsgrenze bietet Ihnen die Möglichkeit, das Risiko anwendungsbezogener Probleme, Fehlkonfigurationen oder böswilliger Aktionen zu begrenzen. Wenn ein Problem innerhalb eines Kontos auftritt, können die Auswirkungen auf die Workloads anderer Konten entweder reduziert oder vermieden werden.
- Spiegeln Sie Ihre geschäftlichen Workloads wider — Verwenden Sie mehrere Konten, um Workloads mit einem gemeinsamen Geschäftszweck in verschiedenen Konten zu gruppieren. Auf diese Weise können Sie die Eigentümerschaft und die Entscheidungsfindung an diesen Konten ausrichten und Abhängigkeiten und Konflikte bei der Sicherung und Verwaltung von Workloads in anderen Konten vermeiden. Abhängig von Ihrem allgemeinen Geschäftsmodell können Sie sich dafür entscheiden, verschiedene Geschäftsbereiche oder Tochtergesellschaften in verschiedenen Konten zu isolieren. Dieser Ansatz könnte auch die Veräußerung dieser Einheiten im Laufe der Zeit erleichtern.

Benutzen Sie das Produkt zum ersten Mal? AWS

Wenn Sie zum ersten Mal Benutzer von sind AWS, registrieren Sie sich zunächst für einen AWS-Konto. Wenn Sie sich registrieren, AWS erstellt ein Konto mit den von Ihnen angegebenen Daten und weist Ihnen das Konto zu. Nachdem Sie Ihren erstellt haben AWS-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.

step-by-stepAnweisungen zum Einrichten eines neuen Kontos finden Sie unter. Erste Schritte mit einem AWS-Konto

Verbundene AWS Dienstleistungen

AWS-Konten arbeiten nahtlos mit den folgenden Diensten zusammen:

- IAM

  Your AWS-Konto ist eng mit AWS Identity and Access Management (IAM) integriert. Sie können IAM mit Ihrem Konto verwenden, um sicherzustellen, dass andere Personen, die in Ihrem Konto arbeiten, so viel Zugriff haben, wie sie benötigen, um ihre Arbeit zu erledigen. Sie verwenden IAM auch, um den Zugriff auf all Ihre AWS Ressourcen zu kontrollieren, nicht nur auf kontospezifische Informationen. Es ist wichtig, dass Sie sich mit den wichtigsten Konzepten und bewährten Methoden von IAM vertraut machen, bevor Sie mit der Einrichtung der IAM-Struktur zu weit gehen. AWS-Konto Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.
- AWS Organizations

  Wenn Ihr Unternehmen groß ist oder voraussichtlich wachsen wird, möchten Sie möglicherweise mehrere AWS Konten einrichten, die der spezifischen Struktur Ihres Unternehmens entsprechen. AWS Organizations stellt die zugrunde liegende Infrastruktur und die Funktionen bereit, mit denen Sie Ihre Umgebungen mit mehreren Konten erstellen und verwalten können. Sie können Ihre bestehenden Konten in einer Organisation zusammenfassen und diese Konten dann zentral verwalten. Sie können Konten erstellen, die automatisch Teil Ihrer Organisation werden, und Sie können andere Kunden zum Beitritt zu Ihrer Organisation einladen. Sie können außerdem Richtlinien anhängen, die sich auf einige oder alle Konten auswirken. Weitere Informationen finden Sie unter Wann zu verwenden AWS Organizations.
- AWS Control Tower

  AWS Control Tower bietet eine vereinfachte Möglichkeit, eine sichere Umgebung mit mehreren Konten AWS einzurichten und zu verwalten. AWS Control Tower automatisiert die Erstellung Ihrer Umgebung mit mehreren Konten mithilfe AWS Organizations, Instanziierung einer Reihe von Ausgangskonten und mit einigen Standardplanken und -konfigurationen für die Umgebung. Damit können AWS Control Tower Sie AWS-Konten in wenigen Schritten neue Konten bereitstellen und

gleichzeitig sicherstellen, dass die Konten Ihren Unternehmensrichtlinien entsprechen. Weitere Informationen finden Sie unter Wann zu verwenden AWS Control Tower.

Mit dem Root-Benutzer des AWS-Kontos

Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, 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.

> **Important**
>
> Jeder, der über Root-Benutzeranmeldedaten für Sie AWS-Konto verfügt, hat uneingeschränkten Zugriff auf alle Ressourcen in Ihrem Konto, einschließlich der Rechnungsinformationen.

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.

Support für die AWS Kontoverwaltung

Sie können Feedback und Fragen über das AWS Account Management-Supportforum posten. Allgemeine Informationen zu AWS Foren finden Sie unter AWS re:Post.

Wenn Sie die Antworten, nach denen Sie suchen, nicht finden können AWS re:Post, können Sie über das ein Konto oder eine abrechnungsbezogene Support-Anfrage erstellen AWS Management Console. Weitere Informationen finden Sie unter Beispiel: Einen Supportfall für Konto und Abrechnung erstellen.

Andere AWS Ressourcen

- AWS Schulungen und Kurse — Links zu rollen- und Spezialkursen sowie Übungen zum Selbststudium, mit denen Sie Ihre AWS Fähigkeiten verbessern und praktische Erfahrungen sammeln können.
- AWS Entwicklertools — Links zu Entwicklertools und Ressourcen mit Dokumentation, Codebeispielen, Versionshinweisen und anderen Informationen, die Sie bei der Entwicklung innovativer Anwendungen unterstützen. AWS
- AWS -Support Center — Die zentrale Anlaufstelle für die Erstellung und Verwaltung Ihrer AWS Support-Fälle. Enthält auch Links zu anderen hilfreichen Ressourcen wie Foren, technischen Informationen FAQs, Servicestatus und AWS Trusted Advisor.
- AWS Support — Die wichtigste Webseite mit Informationen zu AWS Support, einem Support-Kanal mit schnellen Reaktionszeiten one-on-one, der Sie bei der Entwicklung und Ausführung von Anwendungen in der Cloud unterstützt.
- Kontaktieren Sie uns — Eine zentrale Anlaufstelle für Anfragen zu AWS Rechnungen, Konten, Veranstaltungen, Missbrauch und anderen Problemen.
- AWS Nutzungsbedingungen der Website — Detaillierte Informationen zu unseren Urheberrechten und Marken, zu Ihrem Konto, Ihrer Lizenz und Ihrem Zugriff auf die Website sowie zu anderen Themen.

Erste Schritte mit einem AWS-Konto

Wenn Sie neu bei uns sind AWS, besteht der erste Schritt darin, sich für ein anzumelden AWS-Konto. Wenn Sie dies tun, AWS wird mit den von Ihnen angegebenen Daten ein Konto erstellt und es Ihnen zugewiesen.

Die Themen in diesem Abschnitt helfen Ihnen dabei, sich mit einem neuen System vertraut zu machen und es einzurichten AWS-Konto.

Themen

- Voraussetzungen für die Erstellung eines neuen AWS-Konto
- Erstelle eine AWS-Konto
- Aktivieren Sie MFA für Ihren Root-Benutzer
- Erstellen Sie einen Administratorbenutzer
- Zugriff auf Ihre AWS-Konto

Voraussetzungen für die Erstellung eines neuen AWS-Konto

Um sich für eine anzumelden AWS-Konto, müssen Sie die folgenden Informationen angeben:

- E-Mail-Adresse des Root-Benutzers — 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.

- AWS 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 einen Benennungsstandard wie Vorname — Nachname — Zweck verwenden (z. B. paulo-santos-testaccount).
- Adresse — Wenn sich Ihre Kontakt- und Rechnungsadresse in Indien befindet, besteht die Benutzervereinbarung für Ihr Konto mit Amazon Web Services India Private Limited (AWS Indien), einem lokalen AWS Verkäufer in Indien. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben. Abhängig von Ihrer Bank müssen Sie möglicherweise auch ein Einmalpasswort eingeben. AWS Indien berechnet Ihrer Zahlungsmethode im Rahmen des Überprüfungsprozesses 2 INR. AWS Indien erstattet die 2 INR nach Abschluss der Überprüfung.
- 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.

Erstelle eine AWS-Konto

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

Diese Anweisungen gelten für die Gründung eines AWS-Konto Außerhalb Indien. Informationen zum Erstellen eines Kontos in Indien finden Sie unterErstelle eine AWS-Konto mit AWS Indien.

AWS Management Console

Um ein zu erstellen 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 aus AWS-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 verlieren AWS-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. AWS setzt 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 mit Ihrem AWS-Konto Namen oder Ihrer E-Mail-Adresse identisch 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 AWS Kundenvereinbarung. 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 Support Tarife 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.

Aktivieren Sie MFA für Ihren Root-Benutzer

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 AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer 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 finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Administratorbenutzer

Da Sie nicht einschränken können, was ein Root-Benutzer tun kann, empfehlen wir Ihnen 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-Konto Zugriff 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.

Zugriff auf Ihre AWS-Konto

Sie können auf eine der folgenden Arten auf Ihre AWS-Konto zugreifen:

AWS Management Console

Das AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie Ihre AWS-Konto Einstellungen und Ihre AWS Ressourcen verwalten können.

AWS Befehlszeilentools

Mit den AWS Befehlszeilentools können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um AWS Aufgaben auszuführen AWS-Konto . Die Arbeit mit der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilentools sind auch nützlich, wenn Sie Skripts erstellen möchten, die AWS Aufgaben ausführen. AWS stellt zwei Gruppen von Befehlszeilentools bereit:

- AWS Command Line Interface(AWS CLI). Informationen zur Installation und Verwendung von finden Sie im AWS Command Line Interface Benutzerhandbuch. AWS CLI
- AWS Tools for Windows PowerShell. Informationen zur Installation und Verwendung der Tools für Windows PowerShell finden Sie im AWS Tools for Windows PowerShell Benutzerhandbuch.

AWS SDKs

Sie AWS SDKs bestehen aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (z. B. Java, Python, Ruby, .NET, iOS und Android). SDKs Sie kümmern sich um Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Weitere Informationen zu den AWS SDKs, einschließlich deren Download und Installation, finden Sie unter Tools für Amazon Web Services.

AWS HTTPS-Abfrage-API für Kontoverwaltung

Die HTTPS-Abfrage-API für die AWS Kontoverwaltung bietet Ihnen programmatischen Zugriff auf Ihr AWS-Konto und AWS. Mit der HTTPS-Query-API können Sie HTTPS-Anforderungen direkt an den Service richten. Wenn Sie die HTTPS-API nutzen, müssen Sie Code zur digitalen Signierung von Anfragen über Ihre Anmeldeinformationen einsetzen. Weitere Informationen finden Sie unter Aufrufen der API durch HTTP-Abfrageanfragen.

Planen Sie Ihre AWS-Konto Führungsstruktur

Auch wenn Sie Ihre AWS Reise vielleicht mit einem einzigen Konto begonnen haben, AWS empfiehlt es sich, mehrere Konten einzurichten, wenn Ihre Workloads an Größe und Komplexität zunehmen. Unabhängig davon, ob Sie ein mittelständisches oder ein großes Unternehmen sind, sollten Sie einen Governance-Strukturplan erstellen, der sicherstellt, dass Ihre Daten- und Workload-Anforderungen erfüllt werden.

In diesem Abschnitt werden die Vorteile und Verwaltungsdienste beschrieben, die Ihnen bei der AWS Einrichtung einer Verwaltungsstruktur mit mehreren Konten zur Verfügung stehen.

Themen

- Vorteile der Verwendung mehrerer AWS-Konten
- Wann zu verwenden AWS Organizations
- Wann zu verwenden AWS Control Tower
- Grundlegendes zu API-Betriebsmodi

Vorteile der Verwendung mehrerer AWS-Konten

AWS-Konten bilden die grundlegende Sicherheitsgrenze in der AWS Cloud. Sie dienen als Container für Ressourcen und bieten eine wichtige Isolationsebene, die für die Schaffung einer sicheren, gut verwalteten Umgebung unerlässlich ist. Weitere Informationen finden Sie unter Was ist ein AWS-Konto?.

Durch die Aufteilung Ihrer Ressourcen in AWS-Konten separate Ressourcen können Sie die folgenden Prinzipien in Ihrer Cloud-Umgebung unterstützen:

- Sicherheitskontrolle — Verschiedene Anwendungen können unterschiedliche Sicherheitsprofile haben und erfordern daher unterschiedliche Kontrollrichtlinien und -mechanismen. Zum Beispiel ist es viel einfacher, mit einem Prüfer zu sprechen und auf einen einzigen Anbieter verweisen zu können AWS-Konto , der alle Elemente Ihres Workloads hostet, die den Sicherheitsstandards der Payment Card Industry (PCI) unterliegen.
- Isolierung — An AWS-Konto ist eine Sicherheitseinheit. Potenzielle Risiken und Sicherheitsbedrohungen sollten in einer zusammengefasst werden, AWS-Konto ohne andere zu beeinträchtigen. Aufgrund unterschiedlicher Teams oder unterschiedlicher Sicherheitsprofile können unterschiedliche Sicherheitsanforderungen bestehen.

- Viele Teams — Verschiedene Teams haben unterschiedliche Verantwortlichkeiten und Ressourcenanforderungen. Sie können verhindern, dass sich Teams gegenseitig stören, indem Sie sie voneinander trennen AWS-Konten.
- Datenisolierung — Neben der Isolierung der Teams ist es wichtig, die Datenspeicher für ein Konto zu isolieren. Dies kann dazu beitragen, die Anzahl der Personen zu begrenzen, die auf diesen Datenspeicher zugreifen und ihn verwalten können. Dies trägt dazu bei, den Zugriff auf äußerst private Daten einzudämmen und kann daher zur Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) der Europäischen Union beitragen.
- Geschäftsprozess — Verschiedene Geschäftsbereiche oder Produkte können völlig unterschiedliche Zwecke und Prozesse haben. Mit mehreren AWS-Konten können Sie die spezifischen Bedürfnisse einer Geschäftseinheit erfüllen.
- Abrechnung — Ein Konto ist die einzig wahre Möglichkeit, Artikel auf Abrechnungsebene zu trennen. Mithilfe mehrerer Konten können Artikel auf Abrechnungsebene nach Geschäftseinheiten, Funktionsteams oder einzelnen Benutzern getrennt werden. Sie können weiterhin alle Ihre Rechnungen an einen einzigen Zahler konsolidieren (mithilfe AWS Organizations und konsolidierter Abrechnung) und gleichzeitig die Einzelposten durch AWS-Konto trennen.
- Kontingentzuweisung — AWS Servicekontingenten werden für jeden Service separat durchgesetzt. AWS-Konto Durch die Aufteilung der Workloads in verschiedene Workloads AWS-Konten wird verhindert, dass sie sich gegenseitig Kontingente verbrauchen.

Alle in diesem Dokument beschriebenen Empfehlungen und Verfahren entsprechen dem AWS Well-Architected Framework. Dieses Framework soll Ihnen helfen, eine flexible, belastbare und skalierbare Cloud-Infrastruktur zu entwerfen. Auch wenn Sie klein anfangen, empfehlen wir, dass Sie diese Leitlinien im Framework einhalten. Auf diese Weise können Sie Ihre Umgebung sicher skalieren, ohne Ihren laufenden Betrieb zu beeinträchtigen, wenn Sie wachsen.

Verwaltung mehrerer AWS-Konten

Bevor Sie mit dem Hinzufügen mehrerer Konten beginnen, sollten Sie einen Plan für deren Verwaltung entwickeln. Zu diesem Zweck empfehlen wir Ihnen AWS Organizations, diesen kostenlosen AWS Dienst zu verwenden, mit dem Sie alle AWS-Konten in Ihrem Unternehmen verwalten können.

AWS bietet auch AWS Control Tower, wodurch Organizations Ebenen AWS verwalteter Automatisierung hinzugefügt und diese automatisch in andere AWS Dienste wie AWS CloudTrail, AWS Config CloudWatch AWS Service Catalog, Amazon und andere integriert werden. Für diese

Dienste können zusätzliche Kosten anfallen. Weitere Informationen finden Sie unter AWS Control Tower Preise.

Weitere Informationen finden Sie auch unter

- Wann zu verwenden AWS Organizations
- Wann zu verwenden AWS Control Tower

Wann zu verwenden AWS Organizations

AWS Organizations ist 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 Sie Ihre Konten AWS Organizations früher als Gruppe verwalten, können die meisten Verwaltungsaufgaben für die Organisation nur über das Verwaltungskonto der Organisation ausgeführt werden. Standardmäßig umfasst dies nur Vorgänge, 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 Organizations und diesem Dienst aktivieren. Vertrauenswürdiger Zugriff gewährt dem angegebenen AWS Dienst Berechtigungen für den Zugriff auf Informationen über die Organisation und die darin enthaltenen Konten. Wenn Sie den vertrauenswürdigen Zugriff für die Kontoverwaltung aktivieren, gewährt der Kontoverwaltungsdienst Organizations 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 Administrator

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 Aufgaben zur Verwaltung der Metadaten der Kontoverwaltung 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 Administratorzugriff auf die Organisation, über den das Verwaltungskonto verfügt.

Weitere Informationen finden Sie unter Aktivieren Sie ein delegiertes Administratorkonto für die AWS Kontoverwaltung.

Service-Kontrollrichtlinien

Wenn Sie AWS-Konto Teil einer Organisation sind, die von verwaltet wird AWS Organizations, kann der Administrator der Organisation Dienststeuerungsrichtlinien (SCPs) anwenden, die einschränken können, was die Hauptbenutzer in 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 sich an der Schnittstelle zwischen den für das Konto geltenden Regeln und den SCPs IAM-Berechtigungsrichtlinien befinden, die dem Prinzipal zugeordnet sind. Mit dieser Option können Sie beispielsweise verhindern SCPs , dass ein Hauptbenutzer eines Kontos die alternativen Kontakte seines eigenen Kontos ändert.

Beispiele SCPs , die für gelten AWS-Konten, finden Sie unterBeschränken Sie den Zugriff mithilfe von AWS Organizations Dienststeuerungsrichtlinien.

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) für jedes Mitgliedskonto in AWS Organizationsändern. Weitere Informationen finden Sie unter AWS Kontoverwaltung und AWS Organizations im AWS Organizations Benutzerhandbuch. Allgemeine Informationen zur Funktionsweise von Trusted Access 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 für die 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, aufrufen. Weitere Informationen finden Sie unter Aktivieren Sie ein delegiertes Administratorkonto für die AWS Kontoverwaltung.

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

Um den vertrauenswürdigen Zugriff für die AWS Kontoverwaltung zu aktivieren

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 AWS Kontoverwaltung aus.
4. Wählen Sie Vertrauenswürdigen Zugriff aktivieren.
5. Geben Sie im Dialogfeld Vertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren den Text enable ein, um dies zu bestätigen, und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

AWS CLI & SDKs

Um vertrauenswürdigen Zugriff für die AWS Kontoverwaltung zu aktivieren

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

- AWS CLI: enable-aws-service-access

  Das folgende Beispiel ermöglicht den vertrauenswürdigen Zugriff für die AWS Kontoverwaltung in der Organisation des aufrufenden Kontos.

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

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Aktivieren Sie ein delegiertes Administratorkonto für die AWS Kontoverwaltung

Sie aktivieren ein delegiertes Administratorkonto, sodass Sie die AWS Kontoverwaltungs-API-Operationen für andere Mitgliedskonten in aufrufen können. AWS Organizations Nachdem Sie ein delegiertes Administratorkonto für Ihre Organisation registriert haben, können Benutzer und Rollen in diesem Konto die AWS CLI und AWS SDK-Operationen in dem `account` Namespace aufrufen, die im Organisationsmodus funktionieren können, indem sie einen optionalen `AccountId` Parameter unterstützen.

Gehen Sie wie folgt vor, um ein Mitgliedskonto in Ihrer Organisation als delegiertes Administratorkonto zu registrieren.

AWS CLI & SDKs

Um ein delegiertes Administratorkonto für den Account Management Service zu registrieren

Sie können die folgenden Befehle verwenden, um einen delegierten Administrator für den Kontoverwaltungsdienst 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.
> - Sie müssen den vertrauenswürdigen Zugriff für die Kontoverwaltung in Ihrer Organisation aktiviert haben.

Sie müssen den folgenden Dienstprinzipal angeben:

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

Im folgenden Beispiel wird ein Mitgliedskonto der Organisation als delegierter Administrator für den Account Management Service 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 des Kontos 123456789012 verwenden, um Kontoverwaltungs AWS CLI - und SDK-API-Operationen aufzurufen, die den `--account-id` Parameter verwenden, um auf Mitgliedskonten in einer Organisation zu verweisen.

AWS Management Console

Diese Aufgabe wird in der AWS Kontoverwaltungskonsole nicht unterstützt. Sie können diese Aufgabe nur mithilfe der AWS CLI oder einer API-Operation von einem der ausführen AWS SDKs.

Beschränken Sie den Zugriff mithilfe von AWS Organizations Dienststeuerungsrichtlinien

In diesem Thema werden Beispiele vorgestellt, die zeigen, wie Sie mithilfe von Dienststeuerungsrichtlinien (SCPs) einschränken können, was die Benutzer und Rollen in den Konten in Ihrer Organisation tun können. AWS Organizations Weitere Informationen zu Dienststeuerungsrichtlinien finden Sie in den folgenden Themen im AWS Organizations Benutzerhandbuch:

- Erstellen SCPs
- An Konten SCPs OUs anhängen
- Strategien für SCPs
- Syntax der SCP-Richtlinie

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

Im folgenden Beispiel wird verhindert, dass die Operationen `PutAlternateContact` und die `DeleteAlternateContact` API von einem Mitgliedskonto im eigenständigen Kontomodus aufgerufen werden. Dadurch wird verhindert, dass ein Hauptbenutzer 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 Sie, dass ein Mitgliedskonto alternative Kontakte für ein anderes Mitgliedskonto in der Organisation ändert

Im folgenden Beispiel wird das `Resource` Element auf „*“ verallgemeinert, was bedeutet, dass es sowohl für Anfragen im eigenständigen Modus als auch für Anfragen im Organisationsmodus gilt. Das bedeutet, dass selbst das delegierte Administratorkonto für die Kontoverwaltung, sofern der SCP darauf zutrifft, daran gehindert wird, alternative Kontakte für jedes 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 OUs zweien vergleicht. Dies führt dazu, dass ein Hauptbenutzer in einem beliebigen Konto im angegebenen OUs Bereich 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/"
                    ]
                }
            }
    ]
}
```

Wann zu verwenden AWS Control Tower

AWS Organizations ist der grundlegende Service, mit dem Sie Ihre gesamte AWS Umgebung zentral verwalten und sichern können. Ein entscheidender Bestandteil dieses AWS Organizations-zentrierten Ansatzes ist. AWS Control Tower AWS Control Tower fungiert als Verwaltungskonsole innerhalb von Organizations und bietet eine optimierte Möglichkeit, eine sichere AWS Umgebung mit mehreren Konten einzurichten und zu verwalten, indem vorgeschriebene Best Practices angewendet werden.

Dieser bewährte Sicherheitsansatz von AWS Control Tower erweitert die Kernfunktionen von. AWS Organizations AWS Control Tower wendet eine Reihe präventiver und detektiver Schutzmaßnahmen an, um sicherzustellen, dass Ihr Unternehmen und Ihre Konten die empfohlenen Sicherheits- und Compliance-Standards einhalten.

Durch die Einrichtung einer gut durchdachten AWS Organizations Struktur können Sie schnell eine skalierbare AWS Control Tower, sichere und konforme Umgebung einrichten. AWS Dieser zentralisierte Ansatz für Cloud-Management und Governance ist für Unternehmen unerlässlich, die das volle Potenzial der Cloud nutzen und AWS Cloud gleichzeitig die höchsten Sicherheits- und Compliance-Standards einhalten möchten.

Weitere Informationen finden Sie unter Was ist AWS Control Tower? im AWS Control Tower - Benutzerhandbuch.

Grundlegendes zu API-Betriebsmodi

Die API-Operationen, die mit den Attributen AWS-Konto von an funktionieren, funktionieren immer in einem von zwei Betriebsmodi:

- Eigenständiger Kontext — dieser Modus wird verwendet, wenn ein Benutzer oder eine Rolle in einem Konto auf ein Kontoattribut im selben Konto zugreift oder dieses ändert. Der eigenständige Kontextmodus wird automatisch verwendet, wenn Sie den `AccountId` Parameter nicht angeben, wenn Sie einen der Kontoverwaltungs AWS CLI - oder AWS SDK-Vorgänge aufrufen.
- 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 dieses ändert. Der Kontextmodus der Organisation wird automatisch verwendet, wenn Sie den `AccountId` Parameter angeben, wenn Sie einen der Kontoverwaltungs AWS CLI - oder AWS SDK-Operationen aufrufen. Sie können die Operationen in diesem Modus nur vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto für die Kontoverwaltung aus aufrufen.

Die AWS CLI und AWS SDK-Operationen können entweder eigenständig oder im Unternehmenskontext ausgeführt werden.

- Wenn Sie den `AccountId` Parameter nicht angeben, wird der Vorgang im eigenständigen Kontext ausgeführt und die Anforderung wird automatisch auf das Konto angewendet, das Sie für die Anforderung verwendet haben. Dies gilt unabhängig davon, ob das Konto Mitglied einer Organisation ist oder nicht.

- Wenn Sie den `AccountId` Parameter angeben, wird der Vorgang im Organisationskontext ausgeführt, und der Vorgang funktioniert für das angegebene Organisationskonto.
  - Wenn es sich bei dem Konto, das den Vorgang aufruft, um das Verwaltungskonto oder das delegierte Administratorkonto für den Kontoverwaltungsdienst handelt, können Sie im `AccountId` Parameter ein beliebiges Mitgliedskonto dieser Organisation angeben, um das angegebene Konto zu aktualisieren.
  - Das einzige Konto in einer Organisation, das einen der alternativen Kontaktvorgänge anrufen und seine eigene Kontonummer im `AccountId` Parameter angeben kann, ist das Konto, das als delegiertes Administratorkonto für den Kontoverwaltungsdienst angegeben wurde. Für jedes andere Konto, einschließlich des Verwaltungskontos, gilt eine `AccessDenied` Ausnahme.
- Wenn Sie einen Vorgang im eigenständigen Modus ausführen, müssen Sie berechtigt sein, den Vorgang mit einer IAM-Richtlinie auszuführen, die entweder `"*"` das `Resource` Element „Alle Ressourcen zulassen“ oder einen ARN enthält, der die Syntax für ein eigenständiges Konto verwendet.
- Wenn Sie einen Vorgang im Organisationsmodus ausführen, müssen Sie berechtigt sein, den Vorgang mit einer IAM-Richtlinie auszuführen, die entweder `"*"` das `Resource` Element „Alle Ressourcen zulassen“ oder einen ARN enthält, der die Syntax für ein Mitgliedskonto in einer Organisation verwendet.

Erteilen von Berechtigungen zum Aktualisieren von Kontoattributen

Wie bei den meisten AWS Vorgängen gewähren Sie Berechtigungen zum Hinzufügen, Aktualisieren oder Löschen von Kontoattributen mithilfe AWS-Konten von IAM-Berechtigungsrichtlinien. Wenn Sie einem IAM-Prinzipal (entweder einem Benutzer oder einer Rolle) eine IAM-Berechtigungsrichtlinie zuordnen, geben Sie an, welche Aktionen dieser Principal auf welchen Ressourcen und unter welchen Bedingungen ausführen kann.

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

Format des Amazon-Ressourcennamens für AWS-Konten

- Der Amazon-Ressourcenname (ARN) für einen AWS-Konto , den Sie in das `resource` Element einer Grundsatzerklärung aufnehmen können, ist unterschiedlich aufgebaut, je nachdem, ob es sich bei dem Konto, auf das Sie verweisen möchten, um ein eigenständiges Konto oder um ein Konto innerhalb einer Organisation handelt. Weitere Informationen finden Sie im vorherigen Abschnitt unterGrundlegendes zu API-Betriebsmodi.

- Ein Konto-ARN für ein eigenständiges Konto:

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

  Sie müssen dieses Format verwenden, wenn Sie einen Vorgang mit Kontoattributen im eigenständigen Modus ausführen, ohne den `AccountID` Parameter einzubeziehen.

- 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 den `AccountID` Parameter einbeziehen.

Kontextschlüssel für IAM-Richtlinien

Der Kontoverwaltungsdienst bietet auch mehrere für den Kontoverwaltungsdienst spezifische Bedingungsschlüssel, mit denen Sie die von Ihnen erteilten Berechtigungen detailliert steuern können.

`account:AccountResourceOrgPaths`

Mit dem Kontextschlüssel `account:AccountResourceOrgPaths` können Sie einen Pfad durch die Hierarchie Ihrer Organisation zu einer bestimmten Organisationseinheit (OU) angeben. Nur Mitgliedskonten, die in dieser Organisationseinheit enthalten sind, erfüllen die Bedingung. Der folgende Beispielausschnitt schränkt die Richtlinie so ein, dass sie nur für Konten gilt, die sich in einem der beiden angegebenen Konten befinden. OUs

Da `account:AccountResourceOrgPaths` es sich um eine Zeichenfolge mit mehreren Werten handelt, müssen Sie die Operatoren `ForAnyValueoder ForAllValues` eine Zeichenfolge mit mehreren Werten verwenden. Beachten Sie außerdem, dass das Präfix auf dem Bedingungsschlüssel lautet`account`, obwohl Sie auf Pfade OUs in einer Organisation verweisen.

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

```
        ]
    }
}
```

`account:AccountResourceOrgTags`

Mit dem Kontextschlüssel `account:AccountResourceOrgTags` können Sie auf die Tags verweisen, die einem Konto in einer Organisation zugeordnet 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 zum Tagging finden Sie im Benutzerhandbuch unter Tag-Editor.AWS Resource Groups Informationen zur Verwendung von Tags als Teil einer attributbasierten Zugriffskontrollstrategie finden Sie unter Wofür ist ABAC AWS im IAM-Benutzerhandbuch. Der folgende Beispielausschnitt schränkt die Richtlinie so ein, dass sie nur für Konten in einer Organisation gilt, die das Tag mit dem Schlüssel und dem Wert entweder oder haben. `project` `blue` `red`

Da `account:AccountResourceOrgTags` es sich um eine Zeichenfolge mit mehreren Werten handelt, müssen Sie die Operatoren `ForAnyValue`oder `ForAllValues` für mehrwertige Zeichenketten verwenden. Beachten Sie außerdem, dass das Präfix auf dem Bedingungsschlüssel lautet`account`, obwohl Sie auf die Stichwörter im Mitgliedskonto einer Organisation verweisen.

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

> **Note**
>
> Sie können Stichwörter nur an ein Konto in einer Organisation anhängen. Sie können keine Tags an ein eigenständiges Gerät anhängen AWS-Konto.

Konfiguriere deine AWS-Konto

Dieser Abschnitt enthält Themen, in denen beschrieben wird, wie Sie Ihre verwalten AWS-Konto.

> **Note**
>
> Wenn Ihre in Indien mithilfe von Amazon Web Services India Private Limited (AWS Indien) erstellt AWS-Konto wurde, gibt es zusätzliche Überlegungen. Weitere Informationen finden Sie unter Konten in Indien verwalten.

Themen

- Erstellen Sie einen AWS-Konto Alias
- AWS-Regionen In Ihrem Konto aktivieren oder deaktivieren
- Aktualisieren Sie die Abrechnung für Ihre AWS-Konto
- Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers,
- Root-Benutzerpasswort aktualisieren
- Aktualisiere deinen AWS-Konto Namen
- Aktualisieren Sie die alternativen Kontakte für Ihre AWS-Konto
- Aktualisieren Sie den Hauptansprechpartner für Ihren AWS-Konto
- AWS-Konto Identifikatoren anzeigen

Erstellen Sie einen 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 unter Verwenden eines Alias für Ihre AWS-Konto ID im IAM-Benutzerhandbuch.

AWS-Regionen In Ihrem Konto aktivieren oder deaktivieren

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. Amazon S3 und Amazon EC2 unterstützen beispielsweise 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 EC2 Amazon-Instances in Europa starten, um Ihren europäischen Kunden näher 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 aktiviert.

Name	Code
USA Ost (Nord-Virginia)	`us-east-1`
USA Ost (Ohio)	`us-east-2`
USA West (Nordkalifornien)	`us-west-1`
USA West (Oregon)	`us-west-2`
Asien-Pazifik (Tokio)	`ap-northeast-1`
Asien-Pazifik (Seoul)	`ap-northeast-2`

Name	Code
Asien-Pazifik (Osaka)	`ap-northeast-3`
Asia Pacific (Mumbai)	`ap-south-1`
Asien-Pazifik (Singapur)	`ap-southeast-1`
Asien-Pazifik (Sydney)	`ap-southeast-2`
Kanada (Zentral)	`ca-central-1`
Europa (Frankfurt)	`eu-central-1`
Europa (Stockholm)	`eu-north-1`
Europa (Irland)	`eu-west-1`
Europa (London)	`eu-west-2`
Europe (Paris)	`eu-west-3`
Südamerika (São Paulo)	`sa-east-1`

- Sie können alle Zielregionen in einer regionsübergreifenden Inferenzgeografie verwenden, unabhängig vom Region-Opt-Status — Bestimmte AWS generative KI-Services wie Amazon Bedrock (siehe Durchsatz durch regionsübergreifende Inferenz erhöhen) und Amazon Q Developer (siehe Regionsübergreifende Verarbeitung in Amazon Q Developer) verwenden regionsübergreifende Inferenz. Wenn Sie diese Dienste verwenden, wählen sie automatisch die optimalen Optionen AWS-Region— einschließlich Regionen, die Sie nicht für Ressourcen und IAM-Daten aktiviert haben — innerhalb der von Ihnen ausgewählten Region aus. Dies verbessert das Kundenerlebnis, indem die verfügbare Rechenleistung und die Modellverfügbarkeit maximiert werden.
- Sie können IAM-Berechtigungen verwenden, um den Zugriff auf Regionen zu kontrollieren. 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 unter AWS: Ermöglicht das Aktivieren und Deaktivieren AWS-Regionen im IAM-Benutzerhandbuch. Sie können den `aws:RequestedRegion`Bedingungsschlüssel auch verwenden, um den Zugriff auf einen zu AWS-Services 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 die 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. Wenn Sie beispielsweise eine Region deaktivieren, die EC2 Amazon-Instances enthält, müssen Sie trotzdem die Gebühren für diese Instances zahlen, obwohl auf die Instances nicht zugegriffen werden kann.
- 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` `AWSOrganizationsFullAccess` wurden aktualisiert und gewähren nun Zugriff auf die AWS Kontoverwaltung, APIs sodass Sie über die AWS Organizations Konsole auf Kontodaten zugreifen können. 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"
  }
```

Aktualisieren Sie die Abrechnung für Ihre AWS-Konto

Sie können alle Ihre AWS-Konto Abrechnungseinstellungen mithilfe der AWS Billing und der Cost Management-Konsole aktualisieren. Informationen zum Aktualisieren der abrechnungsbezogenen Einstellungen für Ihr Konto finden Sie im AWS Fakturierung und Kostenmanagement Benutzerhandbuch:

Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers,

Es gibt verschiedene geschäftliche Gründe, warum Sie möglicherweise die Root-Benutzer-E-Mail-Adresse aktualisieren müssen AWS-Konto. Zum Beispiel Sicherheit und administrative Belastbarkeit. In diesem Thema werden Sie Schritt für Schritt durch den Prozess der Aktualisierung Ihrer Root-Benutzer-E-Mail-Adresse von sowohl für eigenständige Konten als auch für Mitgliedskonten geführt.

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

Sie können die E-Mail-Adresse des Root-Benutzers unterschiedlich aktualisieren, 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 die des Root-Benutzers mithilfe der AWS Management Console aktualisieren. Informationen dazu finden Sie unter Aktualisieren der Root-Benutzer-E-Mail von für eine eigenständige Version AWS-Konto.
- AWS-Konten innerhalb einer Organisation — Für Mitgliedskonten, die Teil einer AWS Organisation sind, kann ein Benutzer des Verwaltungskontos oder des delegierten Administratorkontos die Root-Benutzer-E-Mail von des Mitgliedskontos zentral über die AWS Organizations Konsole oder programmgesteuert über die AWS CLI & aktualisieren. SDKs Informationen dazu finden Sie unter Aktualisieren der Root-Benutzer-E-Mail von für alle Benutzer AWS-Konto in Ihrer Organisation.

Themen

- Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für einen eigenständigen Benutzer AWS-Konto
- Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für alle Benutzer AWS-Konto in Ihrer Organisation

Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für einen eigenständigen Benutzer AWS-Konto

Gehen Sie wie folgt vor, um die für einen eigenständigen AWS-Konto Benutzer zu bearbeiten.

AWS Management Console

> **Note**
>
> Sie müssen sich als anmelden Root-Benutzer des AWS-Kontos, wofür keine zusätzlichen IAM-Berechtigungen erforderlich sind. Sie können diese Schritte nicht als IAM-Benutzer oder -Rolle ausführen.

1. Verwenden Sie Ihre AWS-Konto E-Mail-Adresse und Ihr Passwort, um sich AWS Management Consoleals Ihr Root-Benutzer des AWS-Kontos Konto anzumelden.
2. Wählen Sie oben rechts in der Konsole Ihren Kontonamen oder Ihre Kontonummer und dann Account (Konto) aus.

3. Wählen Sie auf der Kontoseite neben Kontodetails die Option Aktionen und dann E-Mail-Adresse und Passwort aktualisieren aus.
4. Wählen Sie auf der Seite mit den Kontodetails neben E-Mail-Adresse die Option Bearbeiten aus.
5. Füllen Sie auf der Seite Konto-E-Mail bearbeiten die Felder für Neue E-Mail-Adresse, Neue E-Mail-Adresse bestätigen und bestätigen Sie Ihr aktuelles Passwort. Wählen Sie dann Speichern und fortfahren. Ein Bestätigungscode wird von an Ihre neue E-Mail-Adresse gesendet`no-reply@verify.signin.aws`.
6. Geben Sie auf der Seite Konto-E-Mail bearbeiten unter Bestätigungscode den Code ein, den Sie mit Ihrer E-Mail erhalten haben, und wählen Sie dann Updates bestätigen aus.

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

AWS CLI & SDKs

Diese Aufgabe wird im AWS CLI oder durch einen API-Vorgang von einem der AWS SDKs nicht unterstützt. Sie können diese Aufgabe nur mit dem ausführen AWS Management Console.

Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für alle Benutzer AWS-Konto in Ihrer Organisation

Gehen Sie wie folgt vor, um die für ein Mitgliedskonto in Ihrer Organisation mithilfe der AWS Organizations Konsole zu bearbeiten.

> **Note**
>
> Bevor Sie die E-Mail-Adresse des Root-Benutzers () für ein Mitgliedskonto aktualisieren, empfehlen wir Ihnen, sich mit den Auswirkungen dieses Vorgangs vertraut zu machen. Weitere Informationen finden Sie unter Aktualisieren der E-Mail-Adresse des Root-Benutzers () für ein Mitgliedskonto mit AWS Organizations im AWS Organizations Benutzerhandbuch.

Sie können die E-Mail-Adresse des Root-Benutzers () für ein Mitgliedskonto auch direkt auf der Kontoseite aktualisieren, AWS Management Console nachdem Sie sich als Root-Benutzer angemeldet haben. Folgen Sie den Schritten unter, um step-by-step Anweisungen zu erhaltenAktualisieren Sie die E-Mail-Adresse des Root-Benutzers () für einen eigenständigen Benutzer AWS-Konto.

AWS Management Console

> **Hinweise**
>
> - Um dieses Verfahren über das Verwaltungskonto oder ein delegiertes Administratorkonto in einer Organisation anhand von Mitgliedskonten durchzuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoverwaltungsdienst aktivieren.
> - Sie können dieses Verfahren nicht verwenden, um auf ein Konto zuzugreifen, das sich von der Organisation unterscheidet, mit der Sie den Vorgang aufgerufen haben.

Um die E-Mail-Adresse des Root-Benutzers () für ein Mitgliedskonto mithilfe der AWS Organizations Konsole zu aktualisieren

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich als IAM-Benutzer oder als Root-Benutzer (nicht empfohlen) im Verwaltungskonto der Organisation anmelden.
2. Wählen Sie auf der AWS-KontenSeite das Mitgliedskonto aus, für das Sie die E-Mail-Adresse des Root-Benutzers und die E-Mail-Adresse von aktualisieren möchten.
3. Wählen Sie im Bereich Kontodetails die Schaltfläche Aktionen und dann E-Mail-Adresse aktualisieren aus.
4. Geben Sie unter E-Mail die neue E-Mail-Adresse für den Root-Benutzer ein und wählen Sie dann Speichern aus. Dadurch wird ein Einmalkennwort (OTP) an die neue E-Mail-Adresse gesendet.

> **Note**
>
> Wenn Sie diese Seite in der Organisationskonsole schließen müssen, während Sie auf den Code warten, können Sie innerhalb von 24 Stunden nach dem Senden des Codes zurückkehren und den OTP-Vorgang abschließen. Wählen Sie dazu auf der

Seite mit den Kontodetails die Schaltfläche Aktionen und dann Vollständige E-Mail-Aktualisierung aus.

5. Geben Sie unter Bestätigungscode den Code ein, der im vorherigen Schritt an die neue E-Mail-Adresse gesendet wurde, und wählen Sie dann Bestätigen. Dadurch wird das Update an den Root-Benutzer für das Konto übergeben.

AWS CLI & SDKs

Sie können die E-Mail-Adresse des Root-Benutzers (auch als primäre E-Mail-Adresse bezeichnet) abrufen oder aktualisieren, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

Hinweise

- Um diese Vorgänge über das Verwaltungskonto oder ein delegiertes Administratorkonto in einer Organisation für Mitgliedskonten auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontoverwaltungsdienst aktivieren.
- Sie können nicht auf ein Konto zugreifen, das sich von der Organisation unterscheidet, mit der Sie den Vorgang aufrufen.

Mindestberechtigungen

Für jeden Vorgang benötigen Sie die Berechtigung, die diesem Vorgang zugeordnet ist:

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern die Möglichkeit geben, nur die E-Mail-Adresse des Root-Benutzers zu lesen, die , und anderen Benutzern sowohl Lese- als auch Schreibberechtigungen gewähren.

Um den Prozess für die E-Mail-Adresse des Root-Benutzers von abzuschließen, müssen Sie die primäre E-Mail-Adresse APIs zusammen in der Reihenfolge verwenden, in der sie in den folgenden Beispielen gezeigt wird.

Example **`GetPrimaryEmail`**

Im folgenden Beispiel wird die E-Mail-Adresse des Root-Benutzers () vom angegebenen Mitgliedskonto in einer Organisation abgerufen. Die verwendeten Anmeldeinformationen müssen entweder aus dem Verwaltungskonto der Organisation oder aus dem delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

Im folgenden Beispiel wird der Aktualisierungsprozess für die E-Mail-Adresse des Root-Benutzers von gestartet, die neue E-Mail-Adresse identifiziert und ein Einmalkennwort (OTP) an die neue E-Mail-Adresse für das angegebene Mitgliedskonto in einer Organisation gesendet. Die verwendeten Anmeldeinformationen müssen entweder aus dem Verwaltungskonto der Organisation oder aus dem delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

Im folgenden Beispiel wird der OTP-Code akzeptiert und die neue E-Mail-Adresse dem angegebenen Mitgliedskonto in einer Organisation zugewiesen. Die verwendeten Anmeldeinformationen müssen entweder vom Verwaltungskonto der Organisation oder vom delegierten Administratorkonto der Kontoverwaltung stammen.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Root-Benutzerpasswort aktualisieren

Gehen Sie wie folgt vor, um Ihr AWS-Konto Root-Benutzerkennwort zu bearbeiten.

AWS Management Console

Um Ihr Root-Benutzerpasswort zu bearbeiten

> **Note**
>
> Sie müssen sich als anmelden Root-Benutzer des AWS-Kontos, wofür keine zusätzlichen IAM-Berechtigungen erforderlich sind. Sie können diese Schritte nicht als IAM-Benutzer oder -Rolle ausführen.

1. Verwenden Sie Ihre AWS-Konto E-Mail-Adresse und Ihr Passwort, um sich AWS Management Consoleals Ihr Root-Benutzer des AWS-Kontos Konto anzumelden.
2. Wählen Sie oben rechts in der Konsole Ihren Kontonamen oder Ihre Kontonummer und dann Account (Konto) aus.
3. Wählen Sie auf der Kontoseite neben Kontodetails die Option Aktionen und dann E-Mail-Adresse und Passwort aktualisieren aus.
4. Wählen Sie auf der Seite mit den Kontodetails neben Passwort die Option Bearbeiten aus.
5. Füllen Sie auf der Seite „Passwort bearbeiten“ die Felder für Aktuelles Passwort, Neues Passwort und Neues Passwort bestätigen aus. Wählen Sie dann Passwort aktualisieren aus. Weitere Anleitungen, einschließlich bewährter Methoden für die Einrichtung von Root-Benutzerkennwörtern, finden Sie unter Ändern des Kennworts für Root-Benutzer des AWS-Kontos im IAM-Benutzerhandbuch.

AWS CLI & SDKs

Diese Aufgabe wird in der AWS CLI oder von einer API-Operation von einer der AWS SDKs nicht unterstützt. Sie können diese Aufgabe nur mit dem ausführen AWS Management Console.

Aktualisiere deinen AWS-Konto Namen

Verwenden Sie bei der Verwaltung mehrerer AWS-Konten Dateien klare Benennungskonventionen, die auf die Geschäftsbereiche und Anwendungen abgestimmt sind, um sie zu identifizieren

und zu organisieren. Bei Umstrukturierungen, Fusionen, Übernahmen oder Aktualisierungen von Namenskonventionen müssen Sie möglicherweise Konten umbenennen, um einheitliche Identifikations- und Verwaltungsstandards aufrechtzuerhalten.

Der Name eines Accounts wird an verschiedenen Stellen angezeigt, 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 Ihre Kontonamen leicht zu erkennen sind. Erwägen Sie, für Unternehmenskonten einen Benennungsstandard wie Organisation — Zweck — Umgebung zu verwenden (z. B. Vertrieb — Katalog — Produktion). Vermeiden Sie aus Datenschutz- und Sicherheitsgründen die Verwendung von Kontonamen, die personenbezogene Daten (PII) enthalten.

- Eigenständig AWS-Konten — Wenn Sie keiner Organisation angehören, können Sie Ihren Kontonamen mit dem AWS Management Console, oder dem AWS CLI und SDKs aktualisieren. AWS-Konten Weitere Informationen zur Vorgehensweise finden Sie unter Aktualisieren Sie Ihren Kontonamen für ein eigenständiges AWS-Konto.
- AWS-Konten innerhalb einer Organisation — Bei Mitgliedskonten, die Teil einer sind AWS Organizations, kann ein Benutzer des Verwaltungskontos oder des delegierten Administratorkontos den Kontonamen eines beliebigen Mitgliedskontos in der Organisation zentral über die AWS Organizations Konsole oder programmgesteuert über und aktualisieren. AWS CLI SDKs Weitere Informationen zur Vorgehensweise finden Sie unter Aktualisieren Sie Ihren Kontonamen für alle Konten AWS-Konto in Ihrer Organisation.

> **Note**
>
> Es AWS-Konto kann bis zu vier Stunden dauern, bis Änderungen an einer überall wirksam werden.

Themen

- Aktualisieren Sie Ihren Kontonamen für ein eigenständiges AWS-Konto
- Aktualisieren Sie Ihren Kontonamen für alle Konten AWS-Konto in Ihrer Organisation

Aktualisieren Sie Ihren Kontonamen für ein eigenständiges AWS-Konto

Gehen Sie wie folgt vor AWS-Konto, um den Kontonamen für ein eigenständiges Gerät zu ändern.

AWS Management Console

> **Mindestberechtigungen**
>
> Sie können Ihren Kontonamen mithilfe des Root-Benutzers, eines IAM-Benutzers oder einer IAM-Rolle aktualisieren. Wenn Sie den Root-Benutzer verwenden, sind keine zusätzlichen IAM-Berechtigungen erforderlich, um einen Kontonamen zu aktualisieren. Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, benötigen Sie mindestens die folgenden IAM-Berechtigungen:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Um den Kontonamen für ein eigenständiges Konto zu aktualisieren

1. Verwenden Sie Ihre AWS-Konto E-Mail-Adresse und Ihr Passwort, um sich AWS Management Consoleals Ihr anzumelden Root-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 Kontoseite neben Kontodetails die Option Aktionen und dann Kontonamen aktualisieren aus.
4. Geben Sie unter Name den neuen Kontonamen ein, den Sie aktualisieren möchten, und wählen Sie dann Speichern aus.

AWS CLI & SDKs

> **Mindestberechtigungen**
>
> Sie können Ihren Kontonamen mithilfe des Root-Benutzers, eines IAM-Benutzers oder einer IAM-Rolle aktualisieren. Um die folgenden Schritte ausführen zu können, muss Ihr IAM-Benutzer oder Ihre IAM-Rolle mindestens über die folgenden IAM-Berechtigungen verfügen:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Um den Kontonamen für ein eigenständiges Konto zu aktualisieren

Sie können eine der folgenden Operationen verwenden:

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Aktualisieren Sie Ihren Kontonamen für alle Konten AWS-Konto in Ihrer Organisation

Im Modus „ AWS Organizations Mit allen Funktionen“ können autorisierte IAM-Benutzer oder IAM-Rollen sowohl in Verwaltungs- als auch in delegierten Administratorkonten Kontonamen zentral verwalten.

Gehen Sie wie folgt vor, um den Kontonamen für ein Mitgliedskonto in Ihrer Organisation zu ändern.

Voraussetzungen

Um einen Kontonamen mit der AWS Organizations Konsole zu aktualisieren, müssen Sie einige vorläufige Einstellungen vornehmen:

- Ihre Organisation muss alle Funktionen aktivieren, um die Einstellungen Ihrer Mitgliedskonten verwalten zu können. 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 für eine Organisation aktivieren.
- Sie müssen den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsdienst aktivieren. Informationen zur Einrichtung finden Sie unterVertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

AWS Management Console

> **Mindestberechtigungen**
>
> Um den Kontonamen für ein Mitgliedskonto zu aktualisieren, muss Ihr IAM-Benutzer oder Ihre IAM-Rolle über die folgenden Berechtigungen verfügen:
>
> - `organizations:DescribeOrganization` (nur Konsole)
> - `account:PutAccountName`

Um den Kontonamen für ein Mitgliedskonto zu aktualisieren

1. Öffnen Sie die Organisationskonsole unter https://console.aws.amazon.com/organizations/.
2. Wählen Sie im linken Navigationsbereich die Option AWS-Konten aus.
3. Wählen Sie auf der AWS-KontenSeite das Mitgliedskonto aus, das Sie aktualisieren möchten, wählen Sie das Dropdownmenü Aktionen und dann Kontonamen aktualisieren aus.
4. Geben Sie unter Name den aktualisierten Namen ein und wählen Sie Speichern aus.

AWS CLI & SDKs

> **Mindestberechtigungen**
>
> Um den Kontonamen für ein Mitgliedskonto zu aktualisieren, muss Ihr IAM-Benutzer oder Ihre IAM-Rolle über die folgenden Berechtigungen verfügen:
>
> - `organizations:DescribeOrganization` (nur Konsole)
> - `account:PutAccountName`

Um den Kontonamen für ein Mitgliedskonto zu aktualisieren

Sie können eine der folgenden Operationen verwenden:

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Aktualisieren Sie die alternativen Kontakte für Ihre 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 Hauptkontakt für das Konto erhält weiterhin alle E-Mail-Mitteilungen, die an die E-Mail-Adresse des Root-Kontos gesendet werden.

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

- Ansprechpartner für die Rechnungsstellung
- Ansprechpartner für den operativen Bereich
- Ansprechpartner für Sicherheitsfragen

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

- Eigenständig AWS-Konten — Wenn Sie keiner Organisation angehören, können Sie Ihre eigenen alternativen Kontakte über die AWS Management Console oder über AWS CLI & aktualisieren SDKs. AWS-Konten Informationen zur Vorgehensweise finden Sie unter Aktualisieren der alternativen Kontakte für eine eigenständige Version AWS-Konto.
- AWS-Konten innerhalb einer Organisation — Bei Mitgliedskonten, die Teil einer AWS Organisation sind, kann ein Benutzer des Verwaltungskontos oder des delegierten Administratorkontos jedes Mitgliedskonto in der Organisation zentral über die AWS Organizations Konsole oder programmgesteuert über die AWS CLI & aktualisieren. SDKs Informationen zur Vorgehensweise finden Sie unter Aktualisieren der alternativen Kontakte für alle Kontakte AWS-Konto in Ihrer Organisation.

Themen

- Anforderungen an Telefonnummer und E-Mail-Adresse
- Aktualisieren Sie die alternativen Kontakte für eine eigenständige Version AWS-Konto

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

Anforderungen an Telefonnummer und E-Mail-Adresse

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 alphanumerischen Standardzeichen die folgenden Sonderzeichen im lokalen Teil der E-Mail-Adresse enthalten: "“. `+=.#|!&-_`

Aktualisieren Sie die alternativen Kontakte für eine eigenständige Version AWS-Konto

Gehen Sie wie folgt vor AWS-Konto, um die alternativen Kontakte für ein eigenständiges Gerät hinzuzufügen oder zu bearbeiten. Das unten stehende AWS Management Console Verfahren funktioniert immer nur im eigenständigen Kontext. Sie können den verwenden AWS Management Console , um nur auf die alternativen Kontakte in dem Konto zuzugreifen oder diese zu ändern, mit dem Sie den Vorgang aufgerufen haben.

AWS Management Console

Um alternative Kontakte für ein eigenständiges Gerät hinzuzufügen oder zu bearbeiten AWS-Konto

> **Mindestberechtigungen**
>
> Für die folgenden Schritte sind mindestens folgende IAM-Berechtigungen erforderlich:
>
> - `account:GetAlternateContact`(um die alternativen Kontaktdetails zu sehen)
> - `account:PutAlternateContact`(um einen alternativen Kontakt einzurichten oder zu aktualisieren)

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

1. Melden Sie sich AWS Management Consoleals IAM-Benutzer oder als IAM-Rolle mit den Mindestberechtigungen an.
2. Wählen Sie oben rechts im Fenster Ihren Kontonamen und dann Konto aus.
3. Scrollen Sie auf der Kontoseite nach unten zu Alternative Kontakte und wählen Sie rechts neben dem Titel Bearbeiten aus.

   > **Note**
   >
   > Wenn die Option Bearbeiten nicht angezeigt wird, sind Sie wahrscheinlich nicht als Root-Benutzer für Ihr Konto oder als jemand mit den oben angegebenen Mindestberechtigungen angemeldet.

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

   > **Important**
   >
   > Für Unternehmen hat es sich bewährt AWS-Konten, eine Firmentelefonnummer und eine E-Mail-Adresse einzugeben, anstatt die, die einer Einzelperson gehören.

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

AWS CLI & SDKs

Sie können die alternativen Kontaktinformationen abrufen, aktualisieren oder löschen, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- 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 Kontodienst aktivieren.

Mindestberechtigungen

Für jeden Vorgang benötigen Sie die Berechtigung, die diesem Vorgang zugeordnet ist:

- `GetAlternateContact`(um die alternativen Kontaktdaten zu sehen)
- `PutAlternateContact`(um einen alternativen Kontakt einzurichten 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 Benutzern sowohl Lese- als auch Schreibberechtigungen gewähren.

Example

Im folgenden Beispiel wird der aktuelle alternative Abrechnungskontakt 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 festgelegt.

```
$ 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 mit demselben AWS-Konto Kontakttyp ausführen, wird beim ersten Vorgang der neue Kontakt hinzugefügt, und bei allen aufeinanderfolgenden Anrufen an denselben AWS-Konto Kontakttyp wird der bestehende Kontakt aktualisiert.

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, wird der erste Kontakt im Hintergrund erfolgreich gelöscht. Alle späteren Versuche erzeugen eine `ResourceNotFound` Ausnahme.

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

Gehen Sie wie folgt vor, um alternative Kontaktdetails für beliebige Kontaktadressen AWS-Konto in Ihrer Organisation hinzuzufügen oder zu bearbeiten.

Voraussetzungen

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

- Ihre Organisation muss alle Funktionen aktivieren, 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 für eine Organisation aktivieren.
- Sie müssen den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsdienst aktivieren. Informationen zur Einrichtung finden Sie unterVertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

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

AWS Management Console

Um alternative Kontakte für beliebige Kontakte AWS-Konto in Ihrer Organisation hinzuzufügen oder zu bearbeiten

1. Melden Sie sich mit den Anmeldeinformationen des Verwaltungskontos der Organisation bei der AWS Organizations Konsole an.
2. Wählen Sie unter das Konto aus AWS-Konten, das Sie aktualisieren möchten.

3. Wählen Sie Kontaktinformationen und suchen Sie unter Alternative Kontakte nach dem Kontakttyp: Rechnungskontakt, 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 hat es sich bewährt AWS-Konten, eine Firmentelefonnummer und eine E-Mail-Adresse einzugeben, anstatt die, die einer Einzelperson gehören.

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

AWS CLI & SDKs

Sie können die alternativen Kontaktinformationen abrufen, aktualisieren oder löschen, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- 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 Kontodienst aktivieren.
> - Sie können nicht auf ein Konto zugreifen, das sich von der Organisation unterscheidet, mit der Sie den Vorgang aufrufen.

> **Mindestberechtigungen**
>
> Für jeden Vorgang benötigen Sie die Berechtigung, die diesem Vorgang zugeordnet ist:
>
> - `GetAlternateContact`(um die alternativen Kontaktdaten zu sehen)

- `PutAlternateContact`(um einen alternativen Kontakt einzurichten 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 Benutzern sowohl Lese- als auch Schreibberechtigungen gewähren.

Example

Im folgenden Beispiel wird der aktuelle alternative Abrechnungskontakt für das Konto des Anrufers in einer Organisation abgerufen. Die verwendeten Anmeldeinformationen müssen entweder aus dem Verwaltungskonto der Organisation oder aus dem 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 aus dem Verwaltungskonto der Organisation oder aus dem 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 mit demselben AWS-Konto Kontakttyp ausführen, fügt der erste Kontakt den neuen Kontakt hinzu, und alle nachfolgenden Anrufe an denselben AWS-Konto Kontakttyp 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 aus dem Verwaltungskonto der Organisation oder aus dem 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, gelingt der erste Vorgang automatisch. Alle späteren Versuche erzeugen eine `ResourceNotFound` Ausnahme.

Konto: AlternateContactTypes Kontextschlüssel

Sie können den Kontextschlüssel verwendenaccount:AlternateContactTypes, um anzugeben, welche der drei Abrechnungsarten gemäß der IAM-Richtlinie zulässig (oder verweigert) ist. Das folgende Beispiel für eine IAM-Berechtigungsrichtlinie verwendet diesen Bedingungsschlüssel, um den angehängten Prinzipalen zu ermöglichen, nur den BILLING alternativen Kontakt für ein bestimmtes Konto in einer Organisation abzurufen, aber nicht zu ändern.

Da account:AlternateContactTypes es sich um eine Zeichenfolge mit mehreren Werten handelt, müssen Sie die Operatoren ForAnyValueoder ForAllValues mehrwertige Zeichenketten 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 Sie den Hauptansprechpartner für Ihren AWS-Konto

Sie können die mit Ihrem Konto verknüpften primären Kontaktinformationen aktualisieren, einschließlich des vollständigen Namens, des Firmennamens, der Postanschrift, der Telefonnummer und der Website-Adresse Ihres Kontakts.

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 nicht mit einer Organisation verbunden sind, können Sie Ihren eigenen primären Kontokontakt über die AWS Management Console oder über AWS CLI & aktualisieren SDKs. Informationen dazu finden Sie unter Eigenständigen AWS-Konto Hauptansprechpartner aktualisieren.
- AWS-Konten innerhalb einer Organisation — Bei Mitgliedskonten, die Teil einer AWS Organisation sind, kann ein Benutzer des Verwaltungskontos oder des delegierten Administratorkontos jedes Mitgliedskonto in der Organisation zentral über die AWS Organizations Konsole oder programmgesteuert über die AWS CLI & aktualisieren. SDKs Wie das geht, erfahren Sie unter AWS-Konto Hauptansprechpartner in Ihrer Organisation aktualisieren.

Themen

- Anforderungen an Telefonnummer und E-Mail-Adresse
- Aktualisieren Sie den Hauptkontakt für ein eigenständiges Konto AWS-Konto
- Aktualisieren Sie den Hauptansprechpartner für alle Kontakte AWS-Konto in Ihrer Organisation

Anforderungen an Telefonnummer und E-Mail-Adresse

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 sollten nur Zahlen enthalten.
- Telefonnummern müssen mit einer + und einer Landesvorwahl beginnen und dürfen keine führenden Nullen oder zusätzliche Leerzeichen hinter der Landesvorwahl haben. Zum Beispiel +1 (USA/Kanada) oder +44 (Großbritannien).
- Telefonnummern dürfen keine Bindestriche oder Leerzeichen "-" zwischen der Ortsvorwahl, der Vorwahl und der Ortsvorwahl enthalten. Zum Beispiel +12025550179.
- Aus Sicherheitsgründen müssen Telefonnummern in der Lage sein, SMS von zu empfangen. AWS Gebührenfreie Nummern werden nicht akzeptiert, da die meisten keine SMS unterstützen.
- Für Unternehmen ist es eine bewährte Methode AWS-Konten, eine Firmentelefonnummer und eine E-Mail-Adresse einzugeben, anstatt eine, die einer Einzelperson gehört. Wenn Sie den Root-Benutzer des Kontos mit der E-Mail-Adresse oder Telefonnummer einer Person konfigurieren, kann es schwierig sein, Ihr Konto wiederherzustellen, wenn diese Person das Unternehmen verlässt.

Aktualisieren Sie den Hauptkontakt für ein eigenständiges Konto AWS-Konto

Gehen Sie wie folgt vor AWS-Konto, um Ihre primären Kontaktdaten für ein eigenständiges Unternehmen zu bearbeiten. Das unten stehende AWS Management Console Verfahren funktioniert immer nur im eigenständigen Kontext. Sie können den verwenden AWS Management Console , um nur auf die primären Kontaktinformationen des Kontos zuzugreifen oder diese zu ändern, mit dem Sie den Vorgang aufgerufen haben.

AWS Management Console

Um Ihren Hauptansprechpartner für ein eigenständiges Gerät zu bearbeiten AWS-Konto

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

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

AWS CLI & SDKs

Sie können die primären Kontaktinformationen abrufen, aktualisieren oder löschen, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- GetContactInformation

- PutContactInformation

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

> **Mindestberechtigungen**
>
> Für jeden Vorgang benötigen Sie die Berechtigung, die diesem Vorgang zugeordnet ist:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern nur das Lesen der Kontaktinformationen und anderen Benutzern Lese- und Schreibzugriff gewähren.

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 Sie den Hauptansprechpartner für alle Kontakte AWS-Konto in Ihrer Organisation

Gehen Sie wie folgt vor, um Ihre primären Kontaktdaten AWS-Konto in allen Bereichen Ihrer Organisation zu bearbeiten.

Zusätzliche Anforderungen

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

- Ihre Organisation muss alle Funktionen aktivieren, um die Einstellungen Ihrer Mitgliedskonten verwalten zu können. 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 für eine Organisation aktivieren.
- Sie müssen den vertrauenswürdigen Zugriff für den AWS Kontoverwaltungsdienst aktivieren. Informationen zur Einrichtung finden Sie unterVertrauenswürdigen Zugriff für die AWS Kontoverwaltung aktivieren.

AWS Management Console

So bearbeiten Sie Ihren Hauptansprechpartner für einen beliebigen Ansprechpartner AWS-Konto in Ihrer Organisation

1. Melden Sie sich mit den Anmeldeinformationen für das Verwaltungskonto der Organisation an der AWS Organizations Konsole an.
2. Wählen Sie unter das Konto aus AWS-Konten, das Sie aktualisieren möchten.
3. Wählen Sie Kontaktinformationen und suchen Sie nach Hauptkontakt.
4. Wählen Sie Bearbeiten aus.
5. Ändern Sie die Werte in einem der verfügbaren Felder.
6. Nachdem Sie alle Änderungen vorgenommen haben, wählen Sie Aktualisieren.

AWS CLI & SDKs

Sie können die primären Kontaktinformationen abrufen, aktualisieren oder löschen, indem Sie die folgenden AWS CLI Befehle oder die entsprechenden AWS SDK-Operationen verwenden:

- GetContactInformation
- PutContactInformation

> **Hinweise**
>
> - Um diese Vorgänge über das Verwaltungskonto oder ein delegiertes Administratorkonto in einer Organisation für Mitgliedskonten auszuführen, müssen Sie den vertrauenswürdigen Zugriff für den Kontodienst aktivieren.
> - Sie können nicht auf ein Konto zugreifen, das sich von der Organisation unterscheidet, mit der Sie den Vorgang aufrufen.

> **Mindestberechtigungen**
>
> Für jeden Vorgang benötigen Sie die Berechtigung, die diesem Vorgang zugeordnet ist:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`

Wenn Sie diese individuellen Berechtigungen verwenden, können Sie einigen Benutzern nur das Lesen der Kontaktinformationen und anderen Benutzern Lese- und Schreibzugriff gewähren.

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 aus dem Verwaltungskonto der Organisation oder aus dem 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.

AWS-Konto Identifikatoren anzeigen

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

AWS-Konto ID (ID)

Eine 12-stellige Zahl, z. B. 012345678901, die einen 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. Konten sollten IDs zwar wie alle identifizierenden Informationen sorgfältig verwendet und weitergegeben werden, sie gelten jedoch nicht als geheime, sensible oder vertrauliche Informationen.

Kanonische Benutzer-ID

Ein alphanumerischer Bezeichner, z. B. `79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be` eine verschleierte Form der ID. AWS-Konto Sie können diese ID verwenden, um einen 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 Sie AWS-Konto als Root-Benutzer oder als IAM-Benutzer abrufen.

Sie müssen authentifiziert sein, um diese Identifikatoren sehen AWS zu können.

> **Warning**
>
> Geben Sie Ihre AWS Anmeldeinformationen (einschließlich Passwörter und Zugangsschlüssel) nicht an Dritte weiter, die Ihre AWS-Konto Identifikatoren benötigen, um AWS Ressourcen mit Ihnen zu teilen. Dies würde ihnen den gleichen Zugriff auf die gewähren AWS-Konto , die Sie haben.

Finden Sie Ihren AWS-Konto Ausweis

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

Finden Sie Ihre Konto-ID als Root-Benutzer

AWS Management Console

Um Ihre AWS-Konto ID zu finden, 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 Sicherheitsanmeldedaten 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 Bereich Kontodetails wird die Kontonummer neben der AWS-Konto ID angezeigt.

AWS CLI & SDKs

Um Ihre AWS-Konto ID zu finden, verwenden Sie den 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
```

Finden Sie Ihre 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 Sicherheitsanmeldedaten 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, unter Kontodetails, erscheint die Kontonummer neben der AWS-Konto ID.

AWS CLI & SDKs

Um Ihre AWS-Konto ID zu finden, verwenden Sie den AWS CLI

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

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

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

Finden Sie die kanonische Benutzer-ID für AWS-Konto

Die kanonische Benutzer-ID für Sie finden Sie AWS-Konto mit dem oder dem. AWS Management Console AWS CLI Die kanonische Benutzer-ID für einen AWS-Konto ist spezifisch für dieses Konto. Sie können die kanonische Benutzer-ID für Sie AWS-Konto als Root-Benutzer, Verbundbenutzer oder IAM-Benutzer abrufen.

Suchen Sie die kanonische ID als Root-Benutzer oder IAM-Benutzer

AWS Management Console

So finden Sie die kanonische Benutzer-ID für Ihr Konto, wenn Sie als Root-Benutzer oder IAM-Benutzer an 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, müssen Sie über Folgendes verfügen:
  - `account:GetAccountInformation`

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

   > **Tip**
   > Wenn die Option Sicherheitsanmeldedaten 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.

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

AWS CLI & SDKs

Um die kanonische Benutzer-ID zu finden, verwenden Sie den AWS CLI

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

Verwenden Sie den Befehl list-buckets wie folgt.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Suchen Sie die kanonische ID als Verbundbenutzer mit einer IAM-Rolle

AWS Management Console

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

> **Mindestberechtigungen**
>
> - Sie benötigen die Berechtigung, einen Amazon S3 S3-Bucket aufzulisten und anzuzeigen.

1. Melden Sie sich AWS Management Console als Verbundbenutzer mit einer IAM-Rolle bei der an.
2. Wählen Sie in der Amazon S3 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-Besitzer die kanonische ID für Ihren AWS-Konto Bucket angezeigt.

AWS CLI & SDKs

Um die kanonische Benutzer-ID zu finden, verwenden Sie AWS CLI

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

Verwenden Sie den Befehl list-buckets wie folgt.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Sicherheit in der AWS Kontoverwaltung

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für die Kontoverwaltung gelten, finden Sie unter AWS-Services Umfang nach Compliance-ProgrammAWS-Services und .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung der AWS Kontoverwaltung anwenden können. Es zeigt Ihnen, wie Sie die Kontoverwaltung konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen.
Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Kontoverwaltungsressourcen zu überwachen und zu schützen.

Themen

- Datenschutz in der AWS Kontoverwaltung
- AWS PrivateLink für die AWS Kontoverwaltung
- Identity and Access Management für die AWS Kontoverwaltung
- AWS verwaltete Richtlinien für die AWS Kontoverwaltung
- Konformitätsprüfung für die AWS Kontoverwaltung
- Resilienz im AWS Account Management
- Infrastruktursicherheit in AWS -Kontenverwaltung

Datenschutz in der AWS Kontoverwaltung

Das AWS Modell der mit gilt für den Datenschutz im AWS Account Management. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 Konsole, die API oder arbeiten. AWS CLI AWS SDKs 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 PrivateLink für die AWS Kontoverwaltung

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie von der VPC aus auf den AWS Account Management Service zugreifen, ohne das öffentliche Internet nutzen zu müssen.

Mit Amazon VPC können Sie AWS Ressourcen in einem benutzerdefinierten virtuellen Netzwerk starten. Mit einer VPC können Sie Netzwerkeinstellungen, wie IP-Adressbereich, Subnetze, Routing-Tabellen und Netzwerk-Gateways, steuern. Weitere Informationen VPCs dazu finden Sie im Amazon VPC-Benutzerhandbuch.

Um Ihre Amazon VPC mit Account Management zu verbinden, müssen Sie zunächst einen VPC-Schnittstellen-Endpunkt definieren, über den Sie Ihre VPC mit anderen Diensten verbinden können. AWS 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 einen AWS Account Management-Endpunkt in Ihrer VPC mit dem AWS Management Console, dem AWS Command Line Interface (AWS CLI), einem AWS SDK, der AWS Account Management API oder AWS CloudFormation erstellen.

Informationen zum Erstellen und Konfigurieren eines Endpunkts mithilfe der Amazon VPC-Konsole oder der AWS CLI finden Sie unter Creating an Interface Endpoint im Amazon VPC-Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen Endpunkt erstellen, geben Sie die Kontoverwaltung als den Dienst an, zu dem Ihre VPC eine Verbindung herstellen soll, und verwenden Sie dabei das folgende Format:
>
> ```
> com.amazonaws.us-east-1.account
> ```

Sie müssen die Zeichenfolge genau wie gezeigt verwenden und die `us-east-1` Region angeben. Als globaler Dienst wird Account Management nur in dieser einen AWS Region gehostet.

Informationen zum Erstellen und Konfigurieren eines Endpunkts mithilfe AWS CloudFormation von finden Sie in der VPCEndpoint Ressource AWSEC2:::: im AWS CloudFormation Benutzerhandbuch.

Amazon VPC-Endpunktrichtlinien

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

- Amazon Virtual Private Cloud Cloud-Endpunktrichtlinien für die Kontoverwaltung
- Steuerung des Zugriffs auf Dienste mit VPC-Endpunkten im AWS PrivateLink Handbuch.

Amazon Virtual Private Cloud Cloud-Endpunktrichtlinien für die Kontoverwaltung

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

- Prinzipal, der die Aktionen ausführen kann.
- Die Aktionen, die die Principals 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 Konten abzurufen und zu ändern AWS-Konto, allen IAM-Benutzern jedoch die Erlaubnis verweigert, 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 einem Prinzipal, der sich in einem der Mitgliedskonten der AWS Organisation befindet, Zugriff auf Konten gewähren möchten, die Teil einer Organisation sind, muss das Element das folgende Format verwenden: `Resource`

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

Weitere Informationen zum Erstellen von Endpunktrichtlinien finden Sie im Handbuch unter Steuern des Zugriffs auf Dienste mit VPC-Endpunkten.AWS PrivateLink

Identity and Access Management für die AWS Kontoverwaltung

AWS Identity and Access Management (IAM) ist ein AWS-Service , mit dem ein Administrator den Zugriff auf AWS -Ressourcen sicher steuern kann. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, um Kontoverwaltungsressourcen 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 die AWS Kontoverwaltung mit IAM
- Beispiele für identitätsbasierte Richtlinien für AWS die Kontoverwaltung
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für die Kontoverwaltung AWS
- Problembehebung AWS bei Identität und Zugriff in der Kontoverwaltung

Zielgruppe

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

Service-Benutzer: Wenn Sie den Account Management -Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Kontomitglieder ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Unter finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in der Kontoverwaltung habenProblembehebung AWS bei Identität und Zugriff in der Kontoverwaltung.

Service-Administrator: Wenn Sie in Ihrem Unternehmen für die Kontoverwaltung verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf die Kontoverwaltung. Es ist Ihre Aufgabe, zu bestimmen, auf welche Kontomitglieder und -Ressourcen Ihre Service-Benutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit der Kontomitglieder verwenden kann, finden Sie unterSo funktioniert die AWS Kontoverwaltung mit IAM.

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

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Anmeldeinformationen bei 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. 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 zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Bei AWS programmgesteuerten Zugriff auf AWS bietet ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS -Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS empfiehlt beispielsweise die Verwendung von Multi-Factor Authentication (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto -Stammbenutzer

Wenn Sie ein erstellen AWS-Konto, 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. Um auf den Root-Benutzer zuzugreifen, 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. Verwenden Sie diese nur, 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 Praxis sollten Sie verlangen, dass menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, den Verbund mit einem Identitätsanbieter verwenden, AWS-Services um auf 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 AWS-Services Identitätsquelle bereitgestellt werden, auf zugreift. Wenn Verbundidentitäten auf zugreifen AWS-Konten, 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 -Benutzer ist eine Entität 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 einen Namen geben IAMAdminsund dieser Gruppe 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einem Benutzer zu einer IAM-Rolle (Konsole) 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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 können Sie AWS-Services 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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 verwenden AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung an den, Anforderungen AWS-Service an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. 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 Servicolle, die mit einem verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem angezeigt AWS-Konto und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 — Sie können eine IAM-Rolle nutzen, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS CLI oder AWS -API-Anforderungen durchführen. Das ist empfehlenswerter als Zugriffsschlüssel innerhalb der EC2 Instanz zu speichern. Erstellen Sie ein Instance-Profil, das an die EC2 Instance angefügt ist, um eine AWS -Rolle einer -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 EC2 Amazon-Instances ausgeführt werden 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, einer Identität oder Ressource zugeordnet, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine 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 festzulegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 anfügen können AWS-Konto. Verwaltete

Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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 umfassen. AWS-Services

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

Zugriffskontrolllisten (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 Services, die Unterstützung ACLs bieten. Weitere Informationen ACLs dazu finden Sie unter der Zugriffskontrollliste (ACL) — Übersicht 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 (OU) in angeben AWS Organizations. AWS Organizations ist ein Service für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Funktionen 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 Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbare Zahl von Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource in Ihrem Besitz angefügt sind. Die RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 die AWS Kontoverwaltung mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf die Kontomitglieder verwenden, erfahren Sie, welche IAM-Funktionen Sie mit der Kontomanagement verwenden können.

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

IAM-Feature	Unterstützung bei der Kontoverwaltung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen Überblick über das Zusammenwirken von der Kontoverwaltung und anderen AWS -Services mit den meisten IAM-Funktionen finden Sie unter AWS -Services, 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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 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 umfassen. AWS-Services

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 befinden AWS-Konten, 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für die Kontoverwaltung

Unterstützt Richtlinienaktionen: Ja

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

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 keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Kontoverwaltungsaktionen finden Sie unter Von der AWS Kontoverwaltung definierte Aktionen in der Serviceautorisierungsreferenz.

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. Beispielsweise können Sie alle Aktionen festlegen, die mit den alternativen Kontakten AWS-Konto von an funktionieren, einschließlich der folgenden Aktion:

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

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

Richtlinienressourcen für die Kontoverwaltung

Unterstützt Richtlinienressourcen: Ja

Administratoren können mit AWS -JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Kontoverwaltungsdienst unterstützt die folgenden spezifischen Ressourcentypen im `Resources` Element einer IAM-Richtlinie, sodass Sie die Richtlinie filtern und zwischen diesen Typen unterscheiden können: AWS-Konten

- Konto

  Dieser `resource` Typ eignet sich nur für eigenständige Konten, bei AWS-Konten denen es sich nicht um Mitgliedskonten in einer vom AWS Organizations Service verwalteten Organisation handelt.
- accountInOrganization

Dieser `resource` Typ passt nur zu AWS-Konten , wenn es sich um Mitgliedskonten in einer vom AWS Organizations Dienst verwalteten Organisation handelt.

Eine Liste der Ressourcentypen für die Kontoverwaltung und deren Eigenschaften ARNs finden Sie unter Von der AWS Kontoverwaltung definierte Ressourcen in der Serviceautorisierungsreferenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von der AWS Kontomitglieder definierte Aktionen.

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

Richtlinienbedingungsschlüssel für die Kontoverwaltung

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mit AWS -JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. 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, AWS wertet 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 AWS globalen -Bedingungsschlüssel finden Sie unter AWS Globale - Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Der Account Management -Service unterstützt die folgenden Bedingungsschlüssel, die Sie verwenden können, um eine feinabgestimmte Filterung für Ihre IAM-Richtlinien bereitzustellen:

- Konto: TargetRegion

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

- Konto: AlternateContactTypes

  Dieser Bedingungsschlüssel enthält eine Liste alternativer Kontakttypen:

  - ABRECHNUNG
  - OPERATIONEN
  - SECURITY

  Mithilfe dieses Schlüssels können Sie die Anfrage nur auf die Aktionen filtern, die auf die angegebenen alternativen Kontakttypen abzielen.

- Konto: AccountResourceOrgPaths

  Dieser Bedingungsschlüssel verwendet ein Argument, das aus einer Liste von Pfaden durch die Hierarchie Ihrer Organisation zu bestimmten Organisationseinheiten (OU) besteht. Damit können Sie die Richtlinie so filtern, dass sie sich nur auf Zielkonten in einer passenden Organisationseinheit auswirkt.

  ```
  o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- Konto: AccountResourceOrgTags

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

Eine Liste von -Bedingungsschlüsseln finden Sie unter Bedingungsschlüssel für die AWS Kontoverwaltung in der Service-Autorisierung. Informationen zu den Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von der AWS Kontomitglieder definierte Aktionen.

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

Zugriffskontrolllisten in der 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 Account Management

Unterstützt ABAC (Tags in Richtlinien): Nein

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.

Für die AWS Kontoverwaltung wird die tagbasierte Zugriffskontrolle nur über den `account:AccountResourceOrgTags/key-name` Bedingungsschlüssel unterstützt. Der `aws:ResourceTag/key-name` Standardbedingungsschlüssel wird APIs im Kontonamespace nicht unterstützt.

Beispiel für eine JSON-Richtlinie, die den unterstützten Bedingungsschlüssel verwendet

Die folgende Beispielrichtlinie ermöglicht den Zugriff auf Kontaktinformationen für Konten, die mit dem Schlüssel "" und entweder dem Wert „CostCenter12345" oder „67890" in Ihrer Organisation gekennzeichnet sind.

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

```
            "Effect":"Allow",
            "Action":[
               "account:GetContactInformation",
               "account:GetAlternateContact"
            ],
            "Resource":"*",
            "Condition":{
               "ForAnyValue:StringEquals":{
                  "account:AccountResourceOrgTags/CostCenter":[
                     "12345",
                     "67890"
                  ]
               }
            }
         }
      ]
   }
```

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen auf der Grundlage von Attributen mit ABAC-Autorisierung und IAM-Tutorial: Definieren von Berechtigungen für den Zugriff auf AWS Ressourcen auf der Grundlage von Tags im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit der Kontoverwaltung

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche mit temporären Anmeldeinformationen AWS-Services funktionieren, finden Sie unter, AWS-Services die mit IAM funktionieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort bei der anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On (SSO) -Link Ihres Unternehmens auf 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 von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der - AWS CLI oder AWS -API manuell temporäre Anmeldeinformationen erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden

AWS. 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 verwenden AWS, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anforderung an den, Anforderungen AWS-Service an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. 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: Ja

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 angezeigt AWS-Konto 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 haben standardmäßig nicht die Berechtigung, -Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von der Kontoverwaltung definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für die AWS Kontoverwaltung in der Service-Autorisierung.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden Sie die Kontoseite im AWS Management Console
- Gewährt schreibgeschützten Zugriff auf die Kontoseite in AWS Management Console
- Bereitstellung des vollen Zugriffs auf die Kontoseite im AWS Management Console

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand -Ressourcen 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 verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden

Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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, verwendet werden AWS CloudFormation. 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 mit 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 erfordert AWS-Konto, 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

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

Verwenden Sie die Kontoseite im AWS Management Console

Um auf die Kontoseite in der zugreifen zu können AWS Management Console, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details über Ihre aufzulisten und anzuzeigen AWS-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 Kontomanagement-Konsole verwenden können, können Sie den Entitäten entweder die `AWSAccountManagementReadOnlyAccess` oder die `AWSAccountManagementFullAccess` AWS -verwaltete Richtlinie 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. Stattdessen können Sie in vielen Fällen nur Zugriff auf die Aktionen zulassen, die den API-Operationen entsprechen, die Sie ausführen möchten.

Gewährt schreibgeschützten Zugriff auf die Kontoseite in AWS Management Console

Im folgenden Beispiel möchten Sie einem IAM-Benutzer in Ihrem AWS-Konto schreibgeschützten Zugriff auf die Kontenseite in der gewähren. AWS Management Console Benutzer, denen diese Richtlinie zugewiesen ist, können keine Änderungen vornehmen.

Die `account:GetAccountInformation` Aktion gewährt Zugriff auf die meisten Einstellungen auf der Kontoseite. Um die derzeit aktivierten AWS Regionen zu sehen, müssen Sie die `account:ListRegions` Aktion jedoch auch angeben.

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

Bereitstellung des vollen Zugriffs auf die Kontoseite im AWS Management Console

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

Diese Beispielrichtlinie baut auf der vorherigen Beispielrichtlinie auf, indem alle verfügbaren Schreibberechtigungen (mit Ausnahme von CloseAccount) hinzugefügt werden, sodass 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 Kontoverwaltung AWS

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

Eine Anleitung zum Aktualisieren von kundenverwalteten Richtlinien finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

AWS Richtlinien für Aktionen in der Kontoverwaltung

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

> **Note**
>
> Um IAM-Benutzern Schreibzugriff auf eine bestimmte Kontoeinstellung auf der Kontoseite von zu gewähren AWS Management Console, müssen Sie zusätzlich zu den `GetAccountInformation` Berechtigungen (oder Berechtigungen), die Sie zum Ändern dieser Einstellung verwenden möchten, auch die entsprechende Berechtigung gewähren.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:ListRegions`	Auflisten	Gewährt die Berechtigung zum Auflisten der verfügbaren Regionen.
`account:GetAccountInformation`	Lesen	Gewährt die Berechtigung zum Abrufen der Kontoinformationen für ein Konto.
`account:GetAlternateContact`	Lesen	Gewährt die Berechtigung zum Abrufen der alternativen Kontakte für ein Konto.
`account:GetContactInformation`	Lesen	Gewährt die Berechtigung zum Abrufen der Hauptkontaktinformationen für ein Konto.
`account:GetPrimaryEmail`	Lesen	Gewährt die Berechtigung zum Abrufen der primären E-Mail-Adresse eines Kontos.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:GetRegionOptStatus`	Lesen	Gewährt die Berechtigung zum Abrufen des Opt-in-Status einer Region.
`account:AcceptPrimaryEmailUpdate`	Schreiben	Erteilt die Erlaubnis, die Aktualisierung der primären E-Mail-Adresse des Mitgliedskontos in einer AWS Organisation zu akzeptieren.
`account:CloseAccount`	Schreiben	Gewährt die Berechtigung, ein Konto zu schließen. **Note** Diese Berechtigung gilt nur für die Konsole. Für diese Berechtigung ist kein API-Zugriff verfügbar.
`account:DeleteAlternateContact`	Schreiben	Gewährt die Berechtigung zum Löschen der alternativen Kontakte für ein Konto.
`account:DisableRegion`	Schreiben	Gewährt die Berechtigung, die Verwendung einer Region zu deaktivieren.
`account:EnableRegion`	Schreiben	Gewährt die Berechtigung, die Verwendung einer Region zu aktivieren.
`account:PutAccountName`	Schreiben	Gewährt die Berechtigung, den Namen für ein Konto zu aktualisieren.

Berechtigungsname	Zugriffsebene	Beschreibung
`account:PutAlternateContact`	Schreiben	Gewährt die Berechtigung, die alternativen Kontakte für ein Konto zu ändern.
`account:PutContactInformation`	Schreiben	Gewährt die Berechtigung, die primären Kontaktinformationen für ein Konto zu aktualisieren.
`account:StartPrimaryEmailUpdate`	Schreiben	Erteilt die Erlaubnis, die Aktualisierung der primären E-Mail-Adresse des Mitglieds kontos in einer AWS Organisation einzuleiten.

Problembehebung AWS bei Identität und Zugriff in der Kontoverwaltung

Diagnostizieren und beheben Sie mithilfe der folgenden Informationen gängige Probleme, die bei der Verwendung von der Kontoverwaltung und IAM auftreten können.

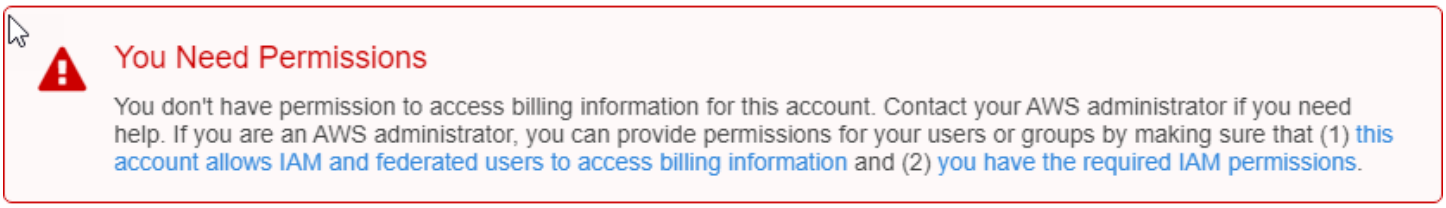
Themen

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

Ich bin nicht autorisiert, eine Aktion auf der Kontoseite auszuführen

Wenn die Ihnen AWS Management Console 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 zum Anzeigen von Details zu seinem AWS-Konto auf der Kontoseite von zu verwenden, AWS Management Console jedoch 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 zum Durchführen 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 Service, sodass keine neue Servicolle 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 Kontomitglieder 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 s Zugriff AWS-Konto auf meine Kontoinformationen 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 Services, die ressourcenbasierte Richtlinien

oder Zugriffskontrolllisten (ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob die Kontoverwaltung diese Funktionen unterstützt, finden Sie unterSo funktioniert die AWS Kontoverwaltung mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle AWS-Konten Ihre finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto Ihrer im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie -Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen AWS-Konten, finden Sie unter Gewähren des Zugriffs für im AWS-Konten Besitz Dritter 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für die AWS Kontoverwaltung

AWS Die Kontoverwaltung bietet derzeit zwei AWS verwaltete Richtlinien, die Ihnen zur Verfügung stehen:

- AWS verwaltete Richtlinie: AWSAccount ManagementReadOnlyAccess
- AWS verwaltete Richtlinie: AWSAccount ManagementFullAccess
- Aktualisierungen der AWS verwalteten Richtlinien durch die Kontoverwaltung

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur

Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

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

AWS verwaltete Richtlinie: AWSAccount ManagementReadOnlyAccess

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

Diese Richtlinie gewährt nur Leseberechtigungen, sodass nur die folgenden Elemente angezeigt werden können:

- Die Metadaten über Ihre AWS-Konten
- Die AWS-Regionen , die für aktiviert oder deaktiviert sind AWS-Konto (Sie können den Status der Regionen in Ihrem Konto nur über die AWS Konsole einsehen)

Dazu wird die Erlaubnis erteilt, alle `List*` Operationen `Get*` oder auszuführen. Es bietet keine Möglichkeit, die Konto-Metadaten zu ändern oder AWS-Regionen für das Konto zu aktivieren oder zu deaktivieren.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `account`— Ermöglicht Prinzipalen das Abrufen der Metadateninformationen über AWS-Konten. Außerdem können Prinzipale die auflisten AWS-Regionen , die für das Konto aktiviert sind, in der. AWS Management Console

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

```
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinie: AWSAccount ManagementFullAccess

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

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

- Die Metadaten über Ihre AWS-Konten
- Die AWS-Regionen , die für aktiviert oder deaktiviert sind AWS-Konto (Sie können den Status anzeigen oder Regionen für Ihr Konto nur über die AWS Konsole aktivieren oder deaktivieren)

Dazu wird die Erlaubnis erteilt, alle `account` Operationen auszuführen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `account`— Ermöglicht Prinzipalen das Anzeigen oder Ändern der Metadateninformationen über AWS-Konten. Es ermöglicht Prinzipalen auch, diejenigen aufzulisten AWS-Regionen , die für das Konto aktiviert sind, und sie in der zu aktivieren oder zu deaktivieren. AWS Management Console

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

Aktualisierungen der AWS verwalteten Richtlinien durch die Kontoverwaltung

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für die Kontoverwaltung, seit dieser Dienst begonnen hat, diese Änderungen nachzuverfolgen. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf der Kontoverwaltungsdokumente.

Änderung	Beschreibung	Datum
AWS Die Kontoverwaltung wurde mit neuen AWS verwalteten Richtlinien eingeführt und begann, Änderungen nachzuverfolgen	Die Kontoverwaltung wurde ursprünglich mit den folgenden AWS verwalteten Richtlinien eingeführt: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30. September 2021

Konformitätsprüfung für die AWS Kontoverwaltung

Externe Prüfer bewerten die Sicherheit und Konformität 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 im Rahmen bestimmter Compliance-Programme finden Sie unter AWS-Services Umfang nach Compliance-Programmen AWS-Services . Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

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

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung von Diensten in Ihrem AWS-Konto Unternehmen hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

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

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- Bewertung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren Sicherheitsstatus AWS , anhand dessen Sie überprüfen können, ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz im AWS Account Management

Die AWS globale Infrastruktur basiert auf AWS-Regionen 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 zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS -Kontenverwaltung

Als verwaltete Dienste AWS-Konto sind AWS Dienste, die in Ihrem Betrieb laufen, durch die AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in 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 Systeme 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.

Überwachen Sie Ihre AWS-Konto

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Account Management und Ihren anderen AWS Lösungen. AWS bietet 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 wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.
- Amazon EventBridge fügt Ihren AWS Services zusätzliche Automatisierung hinzu, indem es automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit 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.

Protokollieren von API-Aufrufen für die AWS Kontoverwaltung mit AWS CloudTrail

Die AWS Kontoverwaltung APIs ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem Dienst ausgeführten Aktionen bereitstellt, oder in einen AWS Dienst, der einen Kontoverwaltungsvorgang aufruft. CloudTrailerfasst alle API-Aufrufe für die Kontoverwaltung als Ereignisse. Zu den erfassten Anrufen gehören alle Aufrufe der Kontoverwaltungsvorgänge. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Kontoverwaltungsvorgänge. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können Sie ermitteln CloudTrail, welche Anfrage einen Kontoverwaltungsvorgang aufgerufen hat, welche IP-Adresse für die Anfrage verwendet wurde, wer die Anfrage wann gestellt hat, und weitere Informationen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zur Kontoverwaltung in CloudTrail

CloudTrail ist in Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn bei einem Kontoverwaltungsvorgang eine Aktivität auftritt, CloudTrail zeichnet diese Aktivität zusammen mit anderen AWS Serviceereignissen im Ereignisverlauf als Ereignis auf. CloudTrail Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem Unternehmen AWS-Konto, einschließlich der Ereignisse für die Kontoverwaltung, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der erstellen AWS Management Console, gilt der Trail standardmäßig für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Sie können andere AWS Dienste so konfigurieren, dass sie die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter analysieren und darauf reagieren. Weitere Informationen finden Sie hier:

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

AWS CloudTrail protokolliert alle API-Operationen zur Kontoverwaltung, die im Abschnitt API-Referenz dieses Handbuchs zu finden sind. Beispielsweise generieren Aufrufe der `PutAlternateContact` Operationen `CreateAccountDeleteAlternateContact`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

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

- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Protokolleinträgen der Kontoverwaltung

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

Beispiel 1: Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für einen Aufruf des `GetAlternateContact` Vorgangs zum Abrufen des aktuellen `OPERATIONS` alternativen Kontakts für ein Konto. Die vom Vorgang 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 des `PutAlternateContact` Vorgangs zum Hinzufügen eines neuen `BILLING` alternativen Kontakts 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 zur `DeleteAlternateContact` Operation zum Löschen des aktuellen `OPERATIONS` alternativen Kontakts.

```
{
  "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, hilft Ihnen dabei, Ereignisse zu überwachen, die spezifisch für andere sind, und Zielaktionen zu initiieren, die andere verwenden AWS-Services. 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 zur 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 mit den vom und zurückgegebenen Status übereinstimmen: `GetRegionOptStatus` `ListRegions` APIs

- `ENABLED`— Die Region wurde erfolgreich für den angegebenen Status 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"
   ]
}
```

Das folgende Beispiel für ein Ereignismuster erstellt eine Regel, die nur `ENABLED` Ereignisse aus `DISABLED` Regionen erfasst.

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

Beheben Sie Probleme mit Ihrem AWS-Konto

Verwenden Sie die Informationen in den folgenden Themen, um Probleme mit Ihrem zu diagnostizieren und zu beheben AWS-Konto. Hilfe zum Root-Benutzer finden Sie im IAM-Benutzerhandbuch unter Problembehandlung mit dem Root-Benutzer. Hilfe zum Anmeldevorgang finden Sie unter Behebung von AWS-Konto Anmeldeproblemen im AWS Anmelde-Benutzerhandbuch.

Themen zur Fehlerbehebung

- Behebung von Problemen bei der AWS-Konto Erstellung
- Behebung von Problemen beim AWS-Konto Schließen
- Behebung anderer Probleme mit AWS-Konten

Behebung von Problemen bei der AWS-Konto Erstellung

Mithilfe der Referenzlinks in der folgenden Tabelle können Sie Probleme beim Erstellen eines neuen Geräts diagnostizieren und beheben AWS-Konto.

Problem	Referenz-Link	Quelle
Ich weiß nicht, wie ich mich anmelden oder ein Konto erstellen soll	Erstelle eine AWS-Konto	Dieser Leitfaden
Was kann ich tun, wenn ich keinen Anruf AWS zur Bestätigung meines neuen Kontos erhalten habe oder die eingegebene PIN nicht funktioniert?	https://repost. aws/knowledge-center/phone- verify-no-call	AWS re:Post
Wie behebe ich den Fehler „maximale Anzahl fehlgesch lagener Versuche“, wenn ich versuche, meine Versuche	https://repost. aws/knowledge-center/maximum-fehlges chlagene Versuche	AWS re:Post

Problem	Referenz-Link	Quelle
AWS-Konto telefonisch zu verifizieren?		
Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert	https://repost. aws/knowledge-center/create- and-activate-aws-account	AWS re:Post
Ich kann mich nicht in mein neues Konto einloggen, nachdem es erstellt wurde	https://docs.aws.amazon.com /signin/latest/userguide/ troubleshooting- sign-in-i ssues .html	AWS Benutzerleitfaden zur Anmeldung

Wenn Sie weitere Hilfe benötigen, empfehlen wir Ihnen, nach Inhalten zu AWS re:Postsuchen, die sich auf Ihr spezielles Problem beziehen. Wenn Sie weiterhin Unterstützung benötigen, wenden Sie sich an AWS -Support.

Behebung von Problemen beim AWS-Konto Schließen

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Kontoschließung aufgetreten sind. Allgemeine Informationen zur Kontoschließung finden Sie unterSchließe eine AWS-Konto.

Themen

- Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann
- Ich sehe die Schaltfläche „Konto schließen“ auf der Kontoseite 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_EXCEEDED“, wenn ich versuche, ein Mitgliedskonto zu schließen
- Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließe?

Ich weiß nicht, wie ich mein Konto löschen oder kündigen kann

Folgen Sie den Anweisungen unter, um Ihr Konto zu schließenSchließe eine AWS-Konto.

Ich sehe die Schaltfläche „Konto schließen“ auf der Kontoseite nicht

Wenn Sie nicht als Root-Benutzer angemeldet sind, wird die Schaltfläche Konto schließen auf der Kontoseite nicht angezeigt. Sie müssen sich AWS Management Console als Root-Benutzer anmelden, um Ihr Konto zu schließen. Wenn Sie sich nicht anmelden können, finden Sie weitere Informationen unter Probleme mit dem Root-Benutzer beheben.

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 gesendet, die für die AWS-Konto. Wenn Sie diese E-Mail nicht innerhalb weniger Stunden erhalten, können Sie sich 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 darauf hinweist, dass Ihr Konto geschlossen wurde. Wenn es sich bei dem Konto, das Sie geschlossen haben, um ein Mitgliedskonto handelt, können Sie überprüfen, ob das geschlossene Konto `SUSPENDED` in der AWS Organizations Konsole so gekennzeichnet ist, dass es erfolgreich geschlossen wurde. 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 Schließung des Kontos 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 über die AWS Organizations Konsole zu schließen, was nicht möglich ist. Um ein Verwaltungskonto zu schließen, müssen Sie sich AWS Management Console

als Root-Benutzer für das Verwaltungskonto anmelden und es auf der Seite Konten schließen. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Schließen eines Verwaltungskontos in Ihrer Organisation.

Ich erhalte die Fehlermeldung „CLOSE_ACCOUNT_QUOTA_EXCEEDED“, 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 Mindestanzahl für Kontoschließungen beträgt 10 und die Höchstgrenze für Kontoschließungen 1000, auch wenn 10% der Konten 1000 überschreiten. Weitere Informationen zu den Kontingenten für Organizations finden Sie unter Kontingente für AWS Organizations im AWS Organizations Benutzerhandbuch.

Muss ich meine AWS Organisation löschen, bevor ich das Verwaltungskonto schließe?

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.

Behebung anderer Probleme mit AWS-Konten

Verwenden Sie die Informationen hier, um Probleme im Zusammenhang mit Ihrem zu beheben AWS-Konto.

Problembereiche

- Ich muss die Kreditkarte für meine ändern AWS-Konto
- Ich muss betrügerische AWS-Konto Aktivitäten melden
- Ich muss meine schließen AWS-Konto

Ich muss die Kreditkarte für meine ändern AWS-Konto

Um die Kreditkarte für Sie zu ändern AWS-Konto, müssen Sie sich anmelden können. AWS verfügt über Schutzmaßnahmen, nach denen Sie nachweisen müssen, dass Sie der Kontoinhaber sind. Anweisungen finden Sie im AWS Billing Benutzerhandbuch unter Verwaltung Ihrer Kreditkarten-Zahlungsmethoden.

Ich muss betrügerische AWS-Konto Aktivitäten melden

Wenn Sie betrügerische Aktivitäten mit Ihrem vermuten AWS-Konto und dies melden möchten, finden Sie weitere Informationen unter Wie melde ich den Missbrauch von AWS Ressourcen?

Wenn Sie Probleme mit einem Kauf auf Amazon.com haben, wenden Sie sich an den Amazon-Kundenservice.

Ich muss meine schließen AWS-Konto

Hilfe zur Behebung von Problemen beim Schließen Ihres AWS-Konto finden Sie unterSchließe eine AWS-Konto.

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 alle unbezahlten Rechnungen und ausstehenden 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. Weitere Informationen finden Sie unter Aktualisieren Sie die E-Mail-Adresse des Root-Benutzers, .

- 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 Frist 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.

- Nachdem ein Konto geschlossen wurde, versendet AWS wir täglich bis zu fünf Tage lang E-Mails, bevor wir die Domain sperren. Nach der Sperrung der Domain und je nach Registrar der Domain löschen wir die Domain entweder innerhalb von 30 Tagen oder geben die Domain an ihren Registrar weiter. Weitere Informationen finden Sie unter Meine Domain AWS-Konto ist geschlossen oder dauerhaft geschlossen und meine Domain ist bei Route 53 registriert.
- AWS CloudTrail ist ein grundlegender Sicherheitsdienst. Das bedeutet, dass von Benutzern erstellte Trails auch nach dem Schließen eines Trails weiterhin existieren und Ereignisse auslösen können, es sei denn, ein Benutzer löscht die AWS-Konto darin enthaltenen Pfade ausdrücklich, AWS-Konto bevor er ihn schließt. Weitere Informationen darüber, wie du die Löschung eines Trails beantragen kannst, nachdem ein Pfad geschlossen AWS-Konto wurde, findest du im CloudTrail Benutzerhandbuch unter AWS-Konto Sperrung und Trails.

Wie schließt du dein Konto

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 unterBehebung von Problemen beim AWS-Konto Schließen.

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. Wählen Sie auf der Kontoseite die Schaltfläche Konto schließen.

4. Geben Sie Ihre Konto-ID ein (wird oben im Schließungsdialogfeld angezeigt), um zu bestätigen, dass Sie den Vorgang zur Kontoschließung gelesen und verstanden haben.
5. Wählen Sie die Schaltfläche Konto schließen, um den Kontoschließungsprozess einzuleiten.
6. Innerhalb weniger Minuten sollten Sie eine Bestätigung per E-Mail erhalten, dass Ihr Konto geschlossen wurde.

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

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. Diese Option ist nur verfügbar, wenn sich eine AWS Organisation im Modus „Alle Funktionen“ befindet.

   > **Note**
   >
   > Wenn Ihre Organisation den Modus „Konsolidierte Abrechnung“ verwendet, wird die Schaltfläche „Schließen“ in der Konsole nicht angezeigt. Um ein Konto im konsolidierten Abrechnungsmodus zu schließen, melden Sie sich als Root-Benutzer bei dem Konto an, das Sie schließen möchten. Wählen Sie auf der Seite Konten die Schaltfläche Konto schließen, geben Sie Ihre Konto-ID ein und wählen Sie dann die Schaltfläche Konto schließen.

4. Lesen Sie die Hinweise zur Kontoschließung und stellen Sie sicher, dass Sie sie verstanden haben.

5. Geben Sie die Mitgliedskonto-ID ein und wählen Sie dann Konto schließen, um den Vorgang zur Kontoschließung einzuleiten.

> **Note**
>
> Für jedes Mitgliedskonto, das Sie schließen, wird in der AWS Organizations Konsole bis zu 90 Tage nach dem ursprünglichen Schließungsdatum ein `SUSPENDED` Etikett neben dem Kontonamen angezeigt. Nach 90 Tagen wird das Mitgliedskonto nicht mehr in der angezeigt AWS Organizations.

Um ein Mitgliedskonto von der Kontoseite aus zu schließen

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

Um ein Mitgliedskonto mit AWS CLI und zu schließen SDKs

Anweisungen zum Schließen eines Mitgliedskontos mithilfe von AWS CLI und SDKs 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 fungiert AWS Organizations.

> **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. Wählen Sie auf der Kontoseite die Schaltfläche Konto schließen.
5. Geben Sie Ihre Konto-ID ein (wird oben im Schließungsdialogfeld angezeigt), um zu bestätigen, dass Sie den Vorgang zur Kontoschließung gelesen und verstanden haben.
6. Wählen Sie die Schaltfläche Konto schließen, um den Kontoschließungsprozess einzuleiten.
7. Innerhalb weniger Minuten sollten Sie eine Bestätigung per E-Mail erhalten, dass Ihr Konto geschlossen wurde.

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

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 unterBehebung von Problemen beim AWS-Konto Schließen.
- Für jedes Mitgliedskonto, das Sie schließen, wird in der AWS Organizations Konsole bis zu 90 Tage nach dem ursprünglichen Schließungsdatum neben dem Kontonamen ein `SUSPENDED` Etikett angezeigt. Nach 90 Tagen wird das Mitgliedskonto nicht mehr in der AWS Organizations Konsole 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.

Die Kontoschließung erfolgt möglicherweise nicht sofort in allen Regionen und Diensten und kann mehrere Stunden dauern.

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 Inhalte und Ressourcen in deinem Konto (mit Ausnahme von CloudTrail Trails). 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.

> **Note**
>
> Die Gebühren für die Dienste, die auf Ihrem Konto verblieben sind, werden wieder aufgenommen, wenn Sie es erneut öffnen.

API-Referenz

Die API-Operationen im Account Management (`account`) -Namespace ermöglichen es Ihnen, Ihre AWS-Konto zu ändern.

Jeder AWS-Konto unterstützt Metadaten mit Informationen über das Konto, einschließlich Informationen über bis zu drei alternative Kontakte, die dem Konto zugeordnet sind. Diese gelten zusätzlich zu der E-Mail-Adresse, die dem Root-Benutzer des Kontos zugeordnet ist. Sie können jeweils nur einen der folgenden Kontakttypen angeben, die einem Konto zugeordnet sind.

- Ansprechpartner für die Rechnungsstellung
- Ansprechpartner für den operativen Bereich
- Ansprechpartner für Sicherheitsfragen

Standardmäßig gelten die in diesem Handbuch beschriebenen API-Operationen direkt für das Konto, das den Vorgang aufruft. Bei der Identität in dem Konto, das den Vorgang aufruft, handelt es sich in der Regel um eine IAM-Rolle oder einen IAM-Benutzer. Für den Aufruf des API-Vorgangs ist eine entsprechende Genehmigung durch eine IAM-Richtlinie erforderlich. Alternativ können Sie diese API-Operationen von einer Identität in einem AWS Organizations Verwaltungskonto aus aufrufen und die Konto-ID-Nummer für jedes AWS-Konto Mitglied der Organisation angeben.

API-Version

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

> **Note**
>
> Als Alternative zur direkten Verwendung der API können Sie eine der verwenden AWS SDKs, die aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (Java, Ruby, .NET, iOS, Android und mehr) besteht. SDKs Sie bieten eine bequeme Möglichkeit, programmatischen Zugriff auf AWS Organizations zu erstellen. SDKs Sie kümmern sich beispielsweise darum, Anfragen kryptografisch zu signieren, Fehler zu verwalten und Anfragen automatisch zu wiederholen. Weitere Informationen zu den AWS SDKs, einschließlich deren Download und Installation, finden Sie unter Tools für Amazon Web Services.

Wir empfehlen, dass Sie den verwenden AWS SDKs , um programmatische API-Aufrufe an den Account Management Service zu tätigen. Sie können jedoch auch die Account Management Query API verwenden, um direkte Aufrufe an den Account Management-Webdienst zu tätigen. Weitere Informationen zur Account Management Query API finden Sie Aufrufen der API mittels HTTP-Abfrageanforderungen im Account Management User Guide. Organizations unterstützt 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 Mengen erfordern, eine POST-Anforderung.

Signieren von Anforderungen

Wenn Sie HTTP-Anfragen an senden AWS, müssen Sie die Anfragen signieren, damit Sie feststellen AWS können, wer sie gesendet hat. Sie signieren Anfragen mit Ihrem AWS Zugriffsschlüssel, der aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel besteht. Wir empfehlen dringend, keinen Zugriffsschlüssel für Ihr Root-Konto zu erstellen. Jeder, der den Zugriffsschlüssel für Ihr Root-Konto hat, hat uneingeschränkten Zugriff auf alle Ressourcen in Ihrem Konto. Erstellen Sie stattdessen einen Zugriffsschlüssel für einen IAM-Benutzer, der über Administratorrechte verfügt. Als weitere Option können Sie den AWS Security Token Service verwenden, um temporäre Sicherheitsanmeldeinformationen zu generieren und diese Anmeldeinformationen zum Signieren von Anfragen zu verwenden.

Zum Signieren von Anfragen empfehlen wir, Signature Version 4 zu verwenden. Wenn Sie über eine bestehende Anwendung verfügen, 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 AWS API-Anfragen signieren.

Wenn Sie die AWS Befehlszeilenschnittstelle (AWS CLI) oder eine der Schnittstellen verwenden, AWS SDKs um Anfragen zu stellen AWS, 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. Senden Sie Ihre Kommentare an feedback-awsaccounts@amazon.com oder posten Sie Ihr Feedback und Ihre Fragen im Account Management-Supportforum. Weitere Informationen zu den AWS Support-Foren finden Sie in der Foren-Hilfe.

Wie werden Beispiele präsentiert

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

API-Anfragen aufzeichnen

Account Management unterstützt CloudTrail, einen Service, der AWS API-Aufrufe für Sie aufzeichnet AWS-Konto und Protokolldateien an einen Amazon S3 S3-Bucket übermittelt. Anhand der von gesammelten Informationen können Sie feststellen CloudTrail, 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 für CloudTrail finden Sie unterProtokollieren von API-Aufrufen für die AWS Kontoverwaltung mit AWS CloudTrail. Weitere Informationen darüber CloudTrail, wie Sie sie aktivieren und Ihre Protokolldateien finden, finden Sie im AWS CloudTrail Benutzerhandbuch.

Aktionen

Folgende Aktionen werden unterstützt:

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- PutAlternateContact
- PutContactInformation

- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

Akzeptiert die Anfrage StartPrimaryEmailUpdate zur Aktualisierung der primären E-Mail-Adresse (auch bekannt als Root-Benutzer-E-Mail-Adresse) für das angegebene Konto.

Anforderungssyntax

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

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "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. 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 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.

Dieser Vorgang kann nur über das Verwaltungskonto oder das delegierte Administratorkonto einer Organisation für ein Mitgliedskonto aufgerufen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben.

Typ: Zeichenfolge

Pattern: `\d{12}`

Erforderlich: Ja

Otp

Der OTP-Code, der an den beim `StartPrimaryEmailUpdate` API-Aufruf `PrimaryEmail` angegebenen Benutzer gesendet wurde.

Typ: Zeichenfolge

Pattern: `[a-zA-Z0-9]{6}`

Erforderlich: Ja

PrimaryEmail

Die neue primäre E-Mail-Adresse zur Verwendung mit dem angegebenen Konto. Dies muss mit `PrimaryEmail` dem `StartPrimaryEmailUpdate` API-Aufruf übereinstimmen.

Typ: Zeichenfolge

Längenbeschränkungen: Mindestlänge von 5. Maximale Länge beträgt 64 Zeichen.

Erforderlich: Ja

Antwortsyntax

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

{
   "Status": "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.

Status

Ruft den Status der akzeptierten primären E-Mail-Aktualisierungsanfrage ab.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | ACCEPTED`

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 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 bearbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT), oder wenn Sie versuchen, die Root-Benutzer-E-Mail-Adresse eines Kontos in eine E-Mail-Adresse zu ändern, die bereits verwendet wird.

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

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

DeleteAlternateContact

Löscht den angegebenen alternativen Kontakt aus einem AWS-Konto.

Vollständige Informationen zur Verwendung der alternativen Kontaktfunktionen finden Sie unter Aktualisieren der alternativen Kontakte für Ihre AWS-Konto.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren können AWS-Konto , die von verwaltet wird AWS 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 und optional 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}`

Erforderlich: Nein

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

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

AccessDeniedException

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

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagen AWS. 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

{
   "AccountName":"MyAccount"
}
```

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for 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 das Amazon Web Services Services-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. Bei der angegebenen Konto-ID muss es sich 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 = 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 bearbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT), oder wenn Sie versuchen, die Root-Benutzer-E-Mail-Adresse eines Kontos in eine E-Mail-Adresse zu ändern, die bereits verwendet wird.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- 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 das Amazon Web Services Services-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. Bei der angegebenen Konto-ID muss es sich 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 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. Maximale Länge = 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 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 bearbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT), oder wenn Sie versuchen, die Root-Benutzer-E-Mail-Adresse eines Kontos in eine E-Mail-Adresse zu ändern, die bereits verwendet wird.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetAccountInformation

Ruft Informationen über das angegebene Konto ab, einschließlich seines Kontonamens, seiner Konto-ID sowie des Datums und der Uhrzeit der Kontoerstellung. Um diese API verwenden zu können, muss ein IAM-Benutzer oder eine IAM-Rolle über die `account:GetAccountInformation` IAM-Berechtigung verfügen.

Anforderungssyntax

```
POST /getAccountInformation 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 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 und optional 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}`

Erforderlich: Nein

Antwortsyntax

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

{
   "AccountCreatedDate": "string",
   "AccountId": "string",
   "AccountName": "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.

AccountCreatedDate

Datum und Uhrzeit der Kontoerstellung.

Typ: Zeitstempel

AccountId

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

Dieser Vorgang kann nur über das Verwaltungskonto oder das delegierte Administratorkonto einer Organisation für ein Mitgliedskonto aufgerufen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben.

Typ: Zeichenfolge

Pattern: `\d{12}`

AccountName

Der Name des Kontos.

Typ: Zeichenfolge

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

Pattern: `[ -;=?-~]+`

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 aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

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

Beispiele

Beispiel 1

Im folgenden Beispiel werden die Kontoinformationen für das Konto abgerufen, dessen Anmeldeinformationen zum Aufrufen des Vorgangs verwendet werden.

Beispielanforderung

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

{}
```

Beispielantwort

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

{
   "AccountId": "123456789012",
```

```
   "AccountName": "MyAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

Beispiel 2

Im folgenden Beispiel werden die Kontoinformationen 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.GetAccountInformation

{
   "AccountId": "123456789012"
}
```

Beispielantwort

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

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

Weitere Informationen finden Sie unter:

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

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for 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 Aktualisieren der alternativen Kontakte für Ihre AWS-Konto.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren können AWS-Konto , die von verwaltet wird AWS 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, 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 und optional 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}`

Erforderlich: Nein

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

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

AccessDeniedException

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

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagen AWS. 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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- AWS -Befehlszeilenschnittstelle

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetContactInformation

Ruft die primären Kontaktinformationen eines AWS-Konto ab.

Vollständige Informationen zur Verwendung der primären Kontaktfunktionen finden Sie unter Aktualisieren des primären Kontakts für Ihren AWS-Konto.

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 das Amazon Web Services Services-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. Die angegebene Konto-ID muss ein Mitgliedskonto in derselben Organisation sein. 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

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 sind AWS-Konto.

Typ: ContactInformation Objekt

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 anrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

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

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

GetPrimaryEmail

Ruft die primäre E-Mail-Adresse für das angegebene Konto ab.

Anforderungssyntax

```
POST /getPrimaryEmail 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 an, auf AWS-Konto die Sie mit diesem Vorgang zugreifen oder die Sie ändern möchten. 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 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.

Dieser Vorgang kann nur über das Verwaltungskonto oder das delegierte Administratorkonto einer Organisation für ein Mitgliedskonto aufgerufen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben.

Typ: Zeichenfolge

Pattern: `\d{12}`

Erforderlich: Ja

Antwortsyntax

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

{
   "PrimaryEmail": "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.

PrimaryEmail

Ruft die primäre E-Mail-Adresse ab, die dem angegebenen Konto zugeordnet ist.

Typ: Zeichenfolge

Längenbeschränkungen: Mindestlänge von 5. Maximale Länge beträgt 64 Zeichen.

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 aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

InternalServerException

Der Vorgang ist aufgrund eines internen Fehlers von fehlgeschlagen AWS. 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for 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 das Amazon Web Services Services-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. Bei der angegebenen Konto-ID muss es sich 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`). Diese Funktion gibt den Status der Region zurück, die Sie an diesen Parameter übergeben.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge = 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. Maximale Länge = 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

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, 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 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for 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 das Amazon Web Services Services-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. Die angegebene Konto-ID muss ein Mitgliedskonto in derselben Organisation sein. 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

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.

Erforderlich: Nein

NextToken

Ein Token, mit dem angegeben wird, wo mit der Paginierung begonnen werden soll. Dies ist das Ergebnis `NextToken` 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.

Erforderlich: Nein

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: Zeichenfolgen-Array

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

Erforderlich: Nein

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

Weitere Informationen zu den allgemeinen Fehlern, die bei allen Aktionen zurückgegeben werden, 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 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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutAccountName

Aktualisiert den Kontonamen des angegebenen Kontos. Um diese API verwenden zu können, müssen IAM-Prinzipale über die `account:PutAccountName` IAM-Berechtigung verfügen.

Anforderungssyntax

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

{
   "AccountId": "string",
   "AccountName": "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 in der 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}`

Erforderlich: Nein

AccountName

Der Name des Kontos.

Typ: Zeichenfolge

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

Pattern: `[ -;=?-~]+`

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 aufrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

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

Beispiele

Beispiel 1

Im folgenden Beispiel wird der Name des Kontos aktualisiert, dessen Anmeldeinformationen zum Aufrufen des Vorgangs verwendet werden.

Beispielanforderung

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

{
   "AccountName":"MyAccount"
}
```

Beispielantwort

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

Beispiel 2

Im folgenden Beispiel wird der Kontoname für das angegebene Mitgliedskonto in einer Organisation aktualisiert. 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.PutAccountName

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
}
```

Beispielantwort

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

Weitere Informationen finden Sie unter:

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

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3

- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for 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 Aktualisieren der alternativen Kontakte für Ihre AWS-Konto.

> **Note**
>
> Bevor Sie die alternativen Kontaktinformationen für eine Person aktualisieren können AWS-Konto , die von verwaltet wird AWS 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 und optional 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}`

Erforderlich: Nein

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 beträgt 1 Zeichen. Die maximale Länge beträgt 254.

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

Erforderlich: Ja

Name

Gibt einen Namen für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 64 Zeichen.

Erforderlich: Ja

PhoneNumber

Gibt eine Telefonnummer für den alternativen Kontakt an.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. 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. Maximale Länge = 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 anrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

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

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 einer der sprachspezifischen Sprachen finden Sie im AWS SDKs Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

PutContactInformation

Aktualisiert die primären Kontaktinformationen eines AWS-Konto.

Vollständige Informationen zur Verwendung der primären Kontaktfunktionen finden Sie unter Aktualisieren des primären Ansprechpartners für Ihren AWS-Konto.

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 das Amazon Web Services Services-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. 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 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

ContactInformation

Enthält die Details der primären Kontaktinformationen, die mit einem verknüpft sind AWS-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

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

AccessDeniedException

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

HTTP Status Code: 403

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

StartPrimaryEmailUpdate

Startet den Vorgang zur Aktualisierung der primären E-Mail-Adresse für das angegebene Konto.

Anforderungssyntax

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

{
   "AccountId": "string",
   "PrimaryEmail": "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. 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 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.

Dieser Vorgang kann nur über das Verwaltungskonto oder das delegierte Administratorkonto einer Organisation für ein Mitgliedskonto aufgerufen werden.

> **Note**
>
> Das Verwaltungskonto kann kein eigenes `AccountId` Konto angeben.

Typ: Zeichenfolge

Pattern: `\d{12}`

Erforderlich: Ja

PrimaryEmail

Die neue primäre E-Mail-Adresse (auch bekannt als Root-Benutzer-E-Mail-Adresse), die für das angegebene Konto verwendet werden soll.

Typ: Zeichenfolge

Längenbeschränkungen: Mindestlänge von 5. Maximale Länge beträgt 64 Zeichen.

Erforderlich: Ja

Antwortsyntax

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

{
   "Status": "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.

Status

Der Status der primären E-Mail-Aktualisierungsanfrage.

Typ: Zeichenfolge

Zulässige Werte: `PENDING | ACCEPTED`

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 anrufende Identität nicht über die erforderlichen Mindestberechtigungen verfügt.

HTTP Status Code: 403

ConflictException

Die Anfrage konnte aufgrund eines Konflikts im aktuellen Status der Ressource nicht bearbeitet werden. Dies ist beispielsweise der Fall, wenn Sie versuchen, eine Region zu aktivieren, die derzeit deaktiviert ist (im Status DEAKTIVIERT), oder wenn Sie versuchen, die Root-Benutzer-E-Mail-Adresse eines Kontos in eine E-Mail-Adresse zu ändern, die bereits verwendet wird.

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

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS -Befehlszeilenschnittstelle
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK für JavaScript V3
- AWS SDK für Kotlin
- AWS SDK for PHP V3
- AWS SDK für Python
- AWS SDK for Ruby V3

Verwandte Aktionen in anderen AWS Diensten

Die folgenden Operationen beziehen sich auf den AWS Organizations Namespace, sind AWS -Kontenverwaltung aber Teil davon:

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

Der `CreateAccount` API-Vorgang kann nur im Kontext einer Organisation verwendet werden, die vom AWS Organizations Dienst verwaltet wird. Die API-Operation ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie unter CreateAccount in der AWS Organizations -API-Referenz.

CreateGovCloudAccount

Der `CreateGovCloudAccount` API-Vorgang kann nur im Kontext einer Organisation verwendet werden, die vom AWS Organizations Dienst verwaltet wird. Die API-Operation ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie unter CreateGovCloudAccount in der AWS Organizations -API-Referenz.

DescribeAccount

Der `DescribeAccount` API-Vorgang kann nur im Kontext einer Organisation verwendet werden, die vom AWS Organizations Dienst verwaltet wird. Die API-Operation ist im Namespace dieses Dienstes definiert.

Weitere Informationen finden Sie unter DescribeAccount in der AWS Organizations -API-Referenz.

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`

Erforderlich: Nein

EmailAddress

Die mit diesem alternativen Kontakt verknüpfte E-Mail-Adresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 254.

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

Erforderlich: Nein

Name

Der Name, der diesem alternativen Kontakt zugeordnet ist.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 64 Zeichen.

Erforderlich: Nein

PhoneNumber

Die diesem alternativen Kontakt zugeordnete Telefonnummer.

Typ: Zeichenfolge

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

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

Erforderlich: Nein

Title

Der Titel, der diesem alternativen Kontakt zugeordnet ist.

Typ: Zeichenfolge

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

Erforderlich: Nein

Weitere Informationen finden Sie unter:

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ContactInformation

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

Inhalt

AddressLine1

Die erste Zeile der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 60.

Erforderlich: Ja

City

Die Stadt der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge = 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 = 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 beträgt 1 Zeichen. Maximale Länge von 20.

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

Erforderlich: Ja

PostalCode

Die Postleitzahl der primären Kontaktadresse.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge von 20.

Erforderlich: Ja

AddressLine2

Die zweite Zeile der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 60.

Erforderlich: Nein

AddressLine3

Die dritte Zeile der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. 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 = 50 Zeichen.

Erforderlich: Nein

DistrictOrCounty

Der Bezirk oder Bezirk der primären Kontaktadresse, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge von 1. Maximale Länge = 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: `USCA`, `GBDE`,`JP`,`IN`, und`BR`.

Typ: Zeichenfolge

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

Erforderlich: Nein

WebsiteUrl

Die URL der Website, die mit den primären Kontaktinformationen verknüpft ist, falls vorhanden.

Typ: Zeichenfolge

Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 256 Zeichen.

Erforderlich: Nein

Weitere Informationen finden Sie unter:

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

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for 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 = 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 einer der sprachspezifischen Sprachen finden Sie im Folgenden: AWS SDKs

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ValidationExceptionField

Die Eingabe erfüllte die vom AWS Dienst in einem angegebenen Feld angegebenen Einschränkungen nicht.

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 einer der sprachspezifischen Sprachen AWS SDKs finden Sie im Folgenden:

- AWS SDK for C++
- AWS SDK for Java V2
- AWS SDK for 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 von AWS API-Anfragen im IAM-Benutzerhandbuch.

Action

Die auszuführende Aktion.

Typ: Zeichenfolge

Erforderlich: Ja

Version

Die API-Version, für die die Anfrage geschrieben wurde, ausgedrückt im Format YYYY-MM-DD.

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 im IAM-Benutzerhandbuch unter Erstellen einer signierten AWS API-Anfrage.

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. Beispielsweise ist die folgende Datums- und Uhrzeitangabe 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-Grundformat angegeben ist, X-Amz-Date ist dies nicht erforderlich. Wenn verwendet X-Amz-Date wird, überschreibt er immer den Wert des Date-Headers. Weitere Informationen finden Sie unter Elemente einer AWS API-Anforderungssignatur im IAM-Benutzerhandbuch.

Typ: Zeichenfolge

Required: Conditional

X-Amz-Security-Token

Das temporäre Sicherheitstoken, das durch einen Aufruf von AWS Security Token Service (AWS STS) abgerufen wurde. Eine Liste der Services, die temporäre Sicherheits-Anmeldeinformationen von AWS STS unterstützen, finden Sie im IAM-Benutzerhandbuch unter AWS-Services , die mit IAM funktionieren.

Bedingung: Wenn Sie temporäre Sicherheitsanmeldedaten von verwenden AWS STS, müssen Sie das Sicherheitstoken angeben.

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 signierten AWS 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 werden die Fehler aufgeführt, die bei den API-Aktionen aller AWS Dienste häufig 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 angegebene AWS Zugriffsschlüssel-ID ist in unseren Aufzeichnungen nicht vorhanden.

HTTP Status Code: 403

NotAuthorized

Sie haben keine Berechtigung zum Ausführen dieser Aktion.

HTTP Status Code: 400

OptInRequired

Für die AWS Zugriffsschlüssel-ID ist ein Abonnement für den Dienst erforderlich.

HTTP Status Code: 403

RequestExpired

Die Anfrage erreichte den Service mehr als 15 Minuten nach dem Datumsstempel auf der Anfrage oder mehr als 15 Minuten nach dem Ablaufdatum der Anfrage (z. B. bei vorsignierter Anfrage URLs), oder der Datumsstempel auf der Anfrage liegt mehr als 15 Minuten in der future.

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 Dienst angegebenen Einschränkungen.

HTTP Status Code: 400

Aufrufen der API mittels HTTP-Abfrageanforderungen

Dieser Abschnitt enthält allgemeine Informationen zur Verwendung der Query API für die AWS Kontoverwaltung. Weitere Informationen über die API-Vorgänge und Fehler finden Sie in der API-Referenz.

> **Note**
>
> Anstatt die Abfrage-API für die AWS Kontoverwaltung direkt aufzurufen, können Sie eine der folgenden verwenden AWS SDKs. Sie AWS SDKs bestehen aus Bibliotheken und Beispielcode für verschiedene Programmiersprachen und Plattformen (Java, Ruby, .NET, iOS, Android und mehr). SDKs Sie bieten eine bequeme Möglichkeit, programmatischen Zugriff auf die AWS Kontoverwaltung und AWS zu erstellen. SDKs Sie kümmern sich beispielsweise um Aufgaben wie das kryptografische Signieren von Anfragen, das Verwalten von Fehlern und das automatische Wiederholen von Anfragen. Informationen zu den AWS SDKs, einschließlich deren Download und Installation, finden Sie unter Tools für Amazon Web Services.

Mit der Query API for AWS Account Management können Sie Serviceaktionen aufrufen. Abfrage-API-Anfragen sind HTTPS-Anfragen, die einen `Action` Parameter enthalten müssen, der den auszuführenden Vorgang angibt. AWS Die Kontoverwaltung unterstützt `GET` und `POST` fordert alle Vorgänge an. Das heißt, Sie müssen die API `GET` für einige Aktionen und `POST` für andere nicht verwenden. `GET`Anfragen unterliegen jedoch der Größenbeschränkung einer URL. Obwohl dieses Limit vom Browser abhängt, liegt ein typisches Limit bei 2.048 Byte. Daher müssen Sie für Query API-Anfragen, die größere Größen erfordern, eine `POST` Anfrage verwenden.

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
- API-Anfragen für die AWS Kontoverwaltung signieren

Endpunkte

AWS Account 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 Dienste finden Sie unter Regionen und Endpunkte in der. Allgemeine AWS-Referenz

HTTPS erforderlich

Da die Abfrage-API vertrauliche Informationen wie Sicherheitsanmeldedaten zurückgeben kann, müssen Sie HTTPS verwenden, um alle API-Anfragen zu verschlüsseln.

API-Anfragen für die AWS Kontoverwaltung signieren

Anforderungen müssen über eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel signiert werden. Wir empfehlen dringend, dass Sie Ihre AWS Root-Kontoanmeldeinformationen nicht für die tägliche Arbeit mit der AWS Kontoverwaltung verwenden. Sie können die Anmeldeinformationen für einen AWS Identity and Access Management (IAM-) Benutzer oder temporäre Anmeldeinformationen verwenden, wie Sie sie für eine IAM-Rolle verwenden.

Um Ihre API-Anfragen zu signieren, müssen Sie AWS Signature Version 4 verwenden. Informationen zur Verwendung von Signature Version 4 finden Sie unter Signieren von AWS API-Anfragen 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 Nutzung des IAM-Dienstes zum Schutz Ihrer AWS Ressourcen, einschließlich der Ressourcen in der AWS Kontoverwaltung.
- Temporäre Sicherheitsanmeldeinformationen in IAM – Beschreibt die Erstellung und Verwendung von temporären Sicherheitsanmeldeinformationen.

Kontingente für AWS -Kontenverwaltung

Ihr AWS-Konto hat Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Dienst. 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
Maximale Anzahl von `StartPrimaryEmailUpdate` Anfragen pro Zielkonto	3 pro 30 Sekunden
Anzahl der alternativen Kontakte in einem AWS-Konto	3 — jeweils einer für `BILLING``SECURITY`, und `OPERATIONS`
Anzahl gleichzeitiger Region-Opt-Anfragen pro Konto	6
Anzahl gleichzeitiger Region-Opt-Anfragen pro Organisation	50
Rate der `AcceptPrimaryEmailUpdate` Anfragen pro Anruferkonto	1 pro Sekunde, Burst auf 1 pro Sekunde
Rate der `DeleteAlternateContact` Anfragen pro Konto	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 `GetAccountInformation` Anfragen pro Anruferkonto	3 pro Sekunde, Burst auf 3 pro Sekunde
Rate der `GetAlternateContact` Anfragen pro Konto	10 pro Sekunde, Burst auf 15 pro Sekunde

Ressource	Kontingent
Rate der `GetContactInformation` Anfragen pro Konto	10 pro Sekunde, Burst auf 15 pro Sekunde
Rate der `GetPrimaryEmail` Anfragen pro Anruferkonto	3 pro Sekunde, Burst auf 3 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 `PutAccountName` Anfragen pro Anruferkonto	1 pro Sekunde, Burst auf 1 pro Sekunde
Rate der `PutAlternateContact` Anfragen pro Konto	5 pro Sekunde, Burst auf 8 pro Sekunde
Rate der `PutContactInformation` Anfragen pro Konto	5 pro Sekunde, Burst auf 8 pro Sekunde
Rate der `StartPrimaryEmailUpdate` Anfragen pro Anruferkonto	1 pro Sekunde, Burst auf 1 pro Sekunde

Konten in Indien verwalten

Wenn Sie sich für ein neues Konto registrieren AWS-Konto und Indien als Kontakt- und Rechnungsadresse wählen, gilt Ihre Benutzervereinbarung mit Amazon Web Services India Private Limited (AWS Indien), einem lokalen AWS Verkäufer in Indien. AWS Indien verwaltet Ihre Abrechnung, und Ihre Rechnungssumme wird in indischen Rupien (INR) statt in US-Dollar (USD) aufgeführt. Informationen zur Verwaltung eines AWS-Konto finden Sie unter. Konfiguriere deine AWS-Konto

Wenn Ihr Konto bei AWS Indien geführt wird, folgen Sie den Anweisungen in diesem Thema, um Ihr Konto zu verwalten. In diesem Thema wird erklärt, wie Sie sich für ein AWS indisches Konto registrieren, Informationen zu Ihrem AWS Indien Konto bearbeiten, die Kundenverifizierung verwalten und Ihre permanente Kontonummer (PAN) hinzufügen oder bearbeiten.

Im Rahmen der Kreditkartenverifizierung bei der Anmeldung belastet AWS Indien Ihre Kreditkarte mit 2 INR. AWS Indien erstattet die 2 INR nach erfolgter Überprüfung zurück. Sie werden möglicherweise bei der Verifizierung zu Ihrer Bank umgeleitet.

Themen

- Erstelle eine AWS-Konto mit AWS Indien
- Verwalte deine Informationen zur Kundenverifizierung

Erstelle eine AWS-Konto mit AWS Indien

AWS Indien ist ein lokaler Verkäufer von AWS in Indien. Wenn sich Ihre Kontakt- und Rechnungsadresse in Indien befindet und Sie ein Konto erstellen möchten, gehen Sie wie folgt vor, um ein AWS indisches Konto zu eröffnen.

Um ein Konto in AWS Indien zu eröffnen

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 „Neues

Konto erstellen“ AWS-Konto immer noch nicht angezeigt wird, wählen Sie „Bei einem anderen Konto anmelden“ und anschließend „Neues Konto erstellen AWS-Konto“.

3. Geben Sie Ihre Kontoinformationen ein, überprüfen Sie Ihre E-Mail-Adresse und wählen Sie ein sicheres Passwort für Ihr Konto.
4. Wählen Sie Geschäftlich oder Persönlich. Privatkonten und Geschäftskonten haben dieselben Merkmale und Funktionen.
5. Geben Sie Ihre Unternehmens- oder persönlichen Kontaktinformationen ein. Wenn Ihre Kontakt- oder Rechnungsadresse in Indien ansässig ist, ist es gemäß den Vorschriften des Indian Computer Emergency Response Team (Cert-In) AWS erforderlich, Ihre Identitätsinformationen zu sammeln und zu validieren, bevor Ihnen der Zugriff auf AWS Dienste gewährt wird.

   Der Name, den Sie zwischen Ihren Kontakt- oder Rechnungsinformationen gewählt haben, muss genau mit dem Namen übereinstimmen, der auf dem Dokument steht, das Sie zur Kundenverifizierung verwenden möchten. Wenn Sie beispielsweise beabsichtigen, ein Geschäftskonto mithilfe einer Gründungsurkunde zu verifizieren, müssen Sie den Firmennamen angeben, der auf dem Dokument steht. Eine Liste der akzeptierten Dokumenttypen finden Sie unter the section called “Akzeptierte indische Dokumente zur Kundenverifizierung”.
6. Nachdem Sie die Kundenvereinbarung gelesen haben, aktivieren Sie das Kontrollkästchen für die Allgemeinen Geschäftsbedingungen und klicken Sie dann auf Weiter.
7. Geben Sie auf der Seite Fakturierungsinformationen die Zahlungsart ein, die Sie verwenden möchten. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben.
8. Unter Haben Sie eine PAN? , wählen Sie Ja aus, wenn Sie eine permanente Kontonummer (PAN) haben, die auf Ihren Steuerrechnungen angezeigt werden soll, und geben Sie dann Ihre PAN ein. Wenn Sie keine PAN haben oder diese nach der Registrierung hinzufügen möchten, wählen Sie Nein.
9. Wählen Sie Verifizieren und fahren Sie fort. AWS Indien belastet Ihre Karte im Rahmen des Überprüfungsprozesses mit 2 INR. AWS Indien erstattet die 2 INR nach erfolgter Überprüfung zurück.
10. Wählen Sie auf der Seite „Bestätigen Sie Ihre Identität“ den Hauptzweck der Kontoregistrierung aus.
11. Wählen Sie die Art der Inhaberschaft, die dem Kontoinhaber am besten entspricht. Wenn Sie ein Unternehmen, eine Organisation oder eine Partnerschaft als Eigentümertyp wählen, geben Sie den Namen einer wichtigen Führungspersönlichkeit ein. Bei der wichtigsten Führungskraft

kann es sich um einen Direktor, einen Betriebsleiter oder eine Person handeln, die für den Geschäftsbetrieb in Ihrem Unternehmen verantwortlich ist.

12. Wählen Sie je nach der von Ihnen ausgewählten Eigentümerart einen für Indien akzeptierten Dokumenttyp aus, den Sie zur Überprüfung verwenden möchten, und geben Sie Ihre Dokumentinformationen ein.

> **Note**
>
> Wenn Sie ein persönliches Konto haben und planen, einen Führerschein zu verwenden, der nicht von der Union of Indien ausgestellt wurde, empfehlen wir, zur Überprüfung einen anderen persönlichen Dokumenttyp zu verwenden.

13. Wählen Sie den Namen, den Sie für die Kundenverifizierung verwenden möchten.

    Die Namen aus Ihren Rechnungs- und Kontaktinformationen werden zur Auswahl angezeigt, wenn sie mit einer indischen Adresse verknüpft sind. Stellen Sie sicher, dass der von Ihnen gewählte Name mit dem Namen auf dem Dokumenttyp übereinstimmt, den Sie für die Kundenverifizierung verwenden möchten. Wenn Sie Änderungen an dem Namen vornehmen müssen, der mit Ihrer Rechnungs- oder Kontaktadresse verknüpft ist, können Sie dies tun, nachdem Sie die Kontoregistrierung abgeschlossen haben.

14. Geben Sie Ihr Einverständnis, die Informationen zur Überprüfung einzureichen, und wählen Sie dann Weiter.

    Sie werden nach Abschluss der Kontoregistrierung per E-Mail über das Ergebnis der Kundenverifizierung informiert. Sie können den Status auch später auf der Kundenbestätigungsseite in Ihren Kontoeinstellungen oder im AWS Health Dashboard überprüfen. Sie müssen die Kundenverifizierung bestehen, um auf die AWS Dienste zugreifen zu können.

15. Wählen Sie aus, ob Sie Ihre Handynummer per Textnachricht (SMS) oder Sprachanruf verifizieren möchten.
16. Wählen Sie Ihre Landes- oder Regionalvorwahl und geben Sie dann Ihre Handynummer ein.
17. Schließen Sie die Sicherheitsprüfung ab.
18. Wählen Sie SMS senden oder Jetzt anrufen aus. Nach wenigen Augenblicken erhalten Sie eine vierstellige PIN in einer SMS oder einem automatisierten Anruf auf Ihrem Handy.
19. Geben Sie auf der Seite Bestätigen Sie Ihre Identität die PIN ein, die Sie erhalten haben, und wählen Sie Weiter.

20. Wählen Sie auf der Seite „Supportplan auswählen“ Ihren Supportplan aus und klicken Sie dann auf Registrierung abschließen. Nachdem Ihre Zahlungsmethode und die Kundenverifizierung bestätigt wurden, wird Ihr Konto aktiviert und Sie erhalten eine E-Mail, in der die Aktivierung Ihres Kontos bestätigt wird.

> **Note**
>
> Wenn Sie die Kundenverifizierung abgeschlossen haben und den Namen, die Adresse oder das Dokument bearbeiten, das zuvor zur Überprüfung Ihrer Identität verwendet wurde, müssen Sie Ihre Kundenverifizierung möglicherweise erneut aktualisieren und abschließen. Weitere Informationen finden Sie unter the section called “Bearbeiten Sie Ihre Kundenbestätigungsinformationen”.

Verwalte deine Informationen zur Kundenverifizierung

Gemäß den Vorschriften des Indian Computer Emergency Response Team (Cert-In) AWS ist es erforderlich, Ihre Identitätsinformationen zu sammeln und zu validieren, bevor wir Ihnen einen neuen oder weiteren Zugriff auf AWS Dienste gewähren können. Ihre Identität muss anhand des Namens der von Ihnen angegebenen Rechnungs- oder Kontaktadresse in Indien verifiziert werden. Bei der Überprüfung AWS wird geprüft, ob die Dokumentennummer gültig ist und ob der von Ihnen angegebene Name mit dem Namen übereinstimmt, der dem Dokument zugeordnet ist, das Sie für die Kundenverifizierung verwenden. Der Name, den Sie zwischen Ihren Kontakt- oder Rechnungsinformationen wählen, muss genau mit dem Namen übereinstimmen, der auf dem Dokument steht.

Informationen zur Aktualisierung Ihres Rechnungsnamens und Ihrer Rechnungsadresse finden Sie auf der Seite mit den Zahlungseinstellungen. Informationen zum Aktualisieren Ihres Kontaktnamens und der Kontaktadresse finden Sie unter the section called “Aktualisieren Sie den Hauptansprechpartner für Ihren AWS-Konto”. Wenn Sie Informationen bearbeiten, die Sie zuvor für die Kundenverifizierung verwendet haben, z. B. den Namen oder die Adresse mit Sitz in Indien aus Ihren Rechnungs- oder Kontaktinformationen, müssen Sie möglicherweise Ihre Kundenverifizierungsinformationen aktualisieren und erneut einreichen.

Überprüfen Sie den Status Ihrer Kundenverifizierung

Sie können den Status Ihrer Kundenverifizierung jederzeit auf der Kundenbestätigungsseite einsehen. Wenn Ihr Bestätigungsstatus „Überprüfung erforderlich“ oder „Überprüfung fehlgeschlagen“

lautet, erstellen oder aktualisieren Sie Ihre Kundenverifizierungsinformationen und reichen Sie sie zur Überprüfung ein.

Erstellen Sie Ihre Informationen zur Kundenverifizierung

Um die Kundenverifizierung abzuschließen, müssen Sie Informationen aus einem akzeptierten Indien Dokument angeben. Eine Liste der akzeptierten Dokumenttypen finden Sie unter the section called "Akzeptierte indische Dokumente zur Kundenverifizierung".

1. Melden Sie sich beim AWS Management Console an.
2. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke Ihren Kontonamen (oder Alias) und dann Konto aus.
3. Wählen Sie unter Andere Einstellungen die Option Kundenverifizierung aus.

   Wenn Sie Ihre Kundenbestätigungsinformationen noch nicht angegeben haben, wird die Seite Kundenverifizierung erstellen angezeigt.
4. Wählen Sie den Namen, der genau mit dem Namen auf dem Dokument übereinstimmt, das Sie für die Kundenverifizierung verwenden möchten. Wenn Sie beispielsweise beabsichtigen, ein Geschäftskonto mithilfe einer Gründungsurkunde zu verifizieren, müssen Sie den Firmennamen angeben, der auf dem Dokument steht.
5. Geben Sie die übrigen auf der Seite angeforderten Informationen ein. Je nach ausgewähltem Dokumenttyp müssen Sie möglicherweise eine Kopie sowohl der Vorder- als auch der Rückseite des Dokuments hochladen. Wenn Sie eine Bilddatei hochladen, stellen Sie sicher, dass alle Informationen im Dokument sichtbar und lesbar sind.
6. Wählen Sie Absenden aus.

   Sie werden per E-Mail oder im AWS Health Dashboard über das Ergebnis der Kundenverifizierung und alle nächsten Schritte informiert.

Bearbeiten Sie Ihre Kundenbestätigungsinformationen

Sie können Ihre Kundenverifizierungsinformationen bearbeiten, z. B. den Hauptzweck der Kontoregistrierung, die Art Ihrer Organisation und den Namen, den Dokumenttyp, das Hochladen von Dokumenten oder die Dokumentinformationen, die Sie zur Überprüfung verwenden möchten.

Wenn Sie den Namen oder den Dokumenttyp bearbeiten, der für die Kundenverifizierung verwendet werden soll, oder Dokumentinformationen aktualisieren, muss Ihre Identität beim Speichern der Änderungen erneut überprüft werden.

1. Melden Sie sich beim AWS Management Console an.
2. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke Ihren Kontonamen (oder Alias) und dann Konto aus.
3. Wählen Sie unter Andere Einstellungen die Option Kundenverifizierung aus.
4. Wählen Sie Bearbeiten und aktualisieren Sie dann die Informationen, die Sie ändern möchten.

   Beachten Sie beim Aktualisieren der Informationen die folgenden Hinweise:

   - Wenn Sie einen anderen Namen wählen, muss der Name genau mit dem Namen auf dem Dokument übereinstimmen, das Sie für die Kundenverifizierung verwenden möchten. Wenn Sie beispielsweise beabsichtigen, ein Geschäftskonto mithilfe einer Gründungsurkunde zu verifizieren, müssen Sie den Firmennamen angeben, der auf dem Dokument steht.
   - Wenn Sie einen anderen Dokumenttyp wählen, müssen Sie eine Kopie der Vorder- und Rückseite (falls zutreffend) des Dokuments hochladen. Alle Informationen im Upload des Dokuments sollten sichtbar und lesbar sein.
   - Wenn Sie ein persönliches Konto haben und planen, einen Führerschein zu verwenden, der nicht von der Union of Indien ausgestellt wurde, empfehlen wir, zur Überprüfung einen anderen persönlichen Dokumenttyp zu verwenden.

     Eine Liste der akzeptierten Dokumenttypen finden Sie unter the section called “Akzeptierte indische Dokumente zur Kundenverifizierung”.
5. Wählen Sie Absenden aus.

   Wenn Ihre Identität aufgrund der Art der von Ihnen gespeicherten Änderungen erneut verifiziert werden muss, werden Sie per E-Mail über das Ergebnis der Kundenverifizierung und alle nächsten Schritte informiert. Sie können sich die Ergebnisse auch ansehen, indem Sie zur Kundenverifizierungsseite oder zum AWS Health Dashboard zurückkehren.

Akzeptierte indische Dokumente zur Kundenverifizierung

Die folgenden von der indischen Regierung ausgestellten Dokumenttypen werden für die Kundenverifizierung akzeptiert.

> **Note**
>
> Die unten aufgeführten Links können von der Regierung geändert werden.

- PAN-Karte — Die PAN-Karte (Permanent Account Number) ist sowohl in digitaler als auch in physischer Form erhältlich und enthält eine eindeutige alphanumerische Kennung, die vom Indien Income Tax Department für Einzelpersonen, Unternehmen und Organisationen ausgestellt wurde. Eine PAN besteht aus zehn Zeichen, einschließlich Buchstaben und Zahlen, im Format **`AAAAA1111A`**. Um dieses Dokument zur Überprüfung verwenden zu können, müssen Sie auch das Geburtsdatum (Einzelperson) oder das Gründungsdatum (Unternehmen) angeben, das auf dem PAN-Dokument angegeben ist, und die Vorderseite der Karte hochladen. Sie können die offizielle Website der Einkommensteuerbehörde aufrufen, um die Gültigkeit Ihrer PAN zu überprüfen.
- Wählerausweis/EPIC — Der Wählerausweis, auch bekannt als Electors Photo Identity Card (EPIC), enthält eine eindeutige Identifikationsnummer, die von der indischen Wahlkommission an Wahlberechtigte in Indien ausgestellt wurde. Eine Wählerausweis-/EPIC-Nummer besteht aus zehn Zeichen, einschließlich Buchstaben und Zahlen. Auf der offiziellen Website der Indien Wahlkommission können Sie die Gültigkeit Ihres Wählerausweises überprüfen. Um dieses Dokument zur Überprüfung zu verwenden, müssen Sie sowohl die Vorder- als auch die Rückseite der Karte hochladen.
- Führerschein — Wenn Ihr Führerschein nicht von der Union of Indien ausgestellt wurde, empfehlen wir, zur Überprüfung einen anderen Dokumenttyp zu verwenden. Eine Führerscheinnummer besteht aus 12 bis 16 Zeichen, einschließlich Buchstaben, Zahlen und einem Leerzeichen oder Bindestrich. Um dieses Dokument zur Überprüfung verwenden zu können, müssen Sie Ihr Geburtsdatum angeben und sowohl die Vorder- als auch die Rückseite der Karte hochladen. Sie können die Gültigkeit Ihres Führerscheins auf der Website des Ministeriums für Straßenverkehr und Autobahnen in Parivahan Sewa überprüfen.
- Reisepass — Ein Reisepass dient als Nachweis der indischen Staatsbürgerschaft und kann als Ausweis für internationale Reisen verwendet werden. In Reisepässen, die von Passport Seva Kendra (PSK) ausgestellt wurden, ist die Reisepassnummer eine eindeutige alphanumerische Kennung, die dem Reisepass einer Person zugeordnet ist. Die Nummer einer Reisepassdatei besteht aus fünfzehn Zeichen, einschließlich Buchstaben und Zahlen. Anders als die Reisepassnummer finden Sie die Nummer der Reisepassdatei auf einer der letzten Seiten Ihres Indien Reisepasses. Um dieses Dokument zur Überprüfung zu verwenden, müssen Sie Ihr Geburtsdatum angeben und sowohl die erste als auch die letzte Seite (mit der

Reisepassnummer) des Reisepasses hochladen. Sie können auf der Website Passport Seva Kendra des Außenministeriums die Gültigkeit Ihrer Reisepassnummer überprüfen.

> **Note**
>
> Für die Kundenverifizierung wird nur eine Reisepassnummer aus einem in Indien ausgestellten indischen Reisepass akzeptiert. Wenn Ihr Indien Reisepass in einem anderen Land ausgestellt wurde, müssen Sie zur Kundenverifizierung ein anderes indisches Dokument verwenden.

- Gründungsurkunde — Eine Gründungsurkunde ist ein vom Ministerium für Unternehmensangelegenheiten (MCA) ausgestelltes Dokument, das die Registrierung eines Unternehmens als juristische Person datiert. Das Zertifikat wird verwendet, um in Indien registrierte Unternehmen eindeutig zu identifizieren und zu verfolgen. Jedes Zertifikat enthält eine Unternehmensidentifikationsnummer (CIN), eine eindeutige alphanumerische Kennung, die aus 21 Zeichen, einschließlich Buchstaben und Zahlen, besteht. Um dieses Dokument zur Überprüfung zu verwenden, müssen Sie die Gründungsurkunde hochladen. Sie können das Portal des Ministeriums für Unternehmensangelegenheiten aufrufen, um die Gültigkeit Ihrer CIN zu überprüfen.

Für Privat- und Geschäftskonten werden verschiedene indische Dokumenttypen akzeptiert:

- Für persönliche Konten - PAN-Karte, Wählerausweis/EPIC, Führerschein und Reisepass.
- Für Geschäftskonten - PAN-Karte und Gründungsurkunde.

Verwalte dein Konto AWS in Indien

Mit Ausnahme der folgenden Aufgaben sind die Verfahren für die Verwaltung Ihres Kontos dieselben wie für Konten, die außerhalb Indien erstellt wurden. Allgemeine Informationen zur Verwaltung Ihres Kontos finden Sie unterKonfiguriere dein Konto.

Verwenden Sie den AWS Management Console , um die folgenden Aufgaben auszuführen:

- Eine permanente Kontonummer hinzufügen oder bearbeiten
- Bearbeiten mehrerer permanenter Kontonummern
- the section called “Verwalte deine Informationen zur Kundenverifizierung”
- Bearbeiten Sie mehrere Steuernummern für Waren und Dienstleistungen (GSTs)

- Eine Steuerrechnung anzeigen

Dokumentenverlauf für das Account Management-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für AWS Account Management beschrieben.

Änderung	Beschreibung	Datum
Neuer Kontoname APIs	Support für neue `GetAccountInformation` und `PutAccountName` APIs zum Anzeigen oder Ändern eines Kontonamens.	22. April 2025
Ende der Unterstützung für die Bearbeitung von Fragen zu Sicherheitsfragen	Das Thema „Fragen zur Sicherheitsabfrage bearbeiten“ wurde aus dem Handbuch entfernt, da der Support eingestellt wurde.	6. Januar 2025
Neue primäre E-Mail-Adresse APIs	Support für neue `GetPrimaryEmail` `StartPrimaryEmailUpdate`, und `AcceptPrimaryEmailUpdate` APIs zentrale Aktualisierung der Root-Benutzer-E-Mail-Adresse für jedes Mitgliedskonto in AWS Organizations. Weitere Informationen finden Sie unter Aktualisieren der E-Mail-Adresse des Root-Benutzers für ein Mitgliedskonto im AWS Organizations Benutzerhandbuch.	6. Juni 2024

Das Thema „Konto schließen“ wurde neu geschrieben	Das gesamte Thema „Konto schließen“ wurde komplett überarbeitet, einschließlich der Hinzufügung von Schritten zum Schließen von Mitglieder- und Verwaltungskonten.	1. Februar 2024
Ende des Supports für das Hinzufügen neuer Fragen zu Sicherheitsproblemen	Es wurden neue Inhalte hinzugefügt, in denen darauf hingewiesen wurde, dass die Option zum Hinzufügen neuer Sicherheitsfragen von der Kontoseite 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 der Standardunterstützung erreicht.	1. Januar 2024
Neufassung des Themas „Regionen“	Das gesamte Thema Regionen wurde komplett überarbeitet, einschließlich der Hinzufügung von Steuerelementen zum Erweitern und Reduzieren.	8. Oktober 2023

Die Themen für Root-Benutzer wurden in das IAM-Benutzerhandbuch verschoben	Die Diskussion über Root-Benutzer wurde zu einem Thema zusammengefasst und es wurden Querverweislinks zu Root-Benutzerthemen hinzugefügt, die in das IAM-Benutzerhandbuch verschoben wurden.	18. September 2023
Dem Hauptkontaktthema des Accounts wurde ein neuer Abschnitt hinzugefügt	Ein neuer Abschnitt mit den Anforderungen an Telefonnummer und E-Mail-Adresse wurde hinzugefügt.	12. September 2023
Neue Kontaktinformationen APIs	Support für neue `GetContactInformation` und `PutContactInformation` 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 aktualisieren, indem Sie die Account-API-Berechtigungen verwenden, die in den aktualisierten AWS Organizations verwalteten Richtlinien bereitgestellt werden.	8. Februar 2022
Erstversion	Erste Version des Referenzleitfadens zur AWS Kontoverwaltung	30. September 2021

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.