aws

User Guide

AWS Organizations

AWS Organizations: User Guide

Table of Contents

Was ist AWS Organizations? 1
AWS Organizations-Merkmale 1
AWS Organizations – Preise 4
Zugriff auf AWS Organizations 4
Support und Feedback zu AWS Organizations 5
Sonstige AWS-Ressourcen 5
Erste Schritte mit AWS Organizations 7
Informationen über... 7
Terminologie und Konzepte von AWS Organizations 7
Tutorials 14
Praktische Anleitung: Erstellen und Konfigurieren einer Organisation 14
Voraussetzungen 16
Schritt 1: Erstellen Ihrer Organisation 16
Schritt 2: Erstellen der Organisationseinheiten 19
Schritt 3: Erstellen von Service-Kontrollrichtlinien 22
Schritt 4: Testen der Organisationsrichtlinien 27
Tutorial: Überwachen mit Amazon EventBridge 28
Voraussetzungen 29
Schritt 1: Konfigurieren einer Trail- und Ereignisauswahl 30
Schritt 2: Konfigurieren einer Lambda-Funktion 31
Schritt 3: Erstellen Sie ein Amazon-SNS-Thema, das E-Mails an Abonnenten sendet 32
Schritt 4: Erstellen einer Amazon-EventBridge-Regel 33
Schritt 5: Testen Ihrer Amazon-EventBridge-Regel 33
Bereinigung: Entfernen der nicht mehr benötigten Ressourcen 35
Bewährte Methoden für die Verwaltung mehrerer Konten 37
Verwalten von Konten in einer einzigen Organisation 37
Verwenden eines sicheren Passworts für den Root-Benutzer 38
Dokumentieren der Prozesse für die Verwendung der Root-Benutzer-Anmeldeinformationen 38
Aktivieren von MFA für die Anmeldedaten für Ihren Root-Benutzer 39
Anwenden von Steuerelementen zur Überwachung des Zugriffs auf die Anmeldeinformationen 40
Kontakt-Telefonnummer auf dem neuesten Stand halten 40
Verwenden einer Gruppen-E-Mail-Adresse für Root-Konten 41
Gruppieren der Workloads nach Geschäftszweck statt nach Firmenhierarchie 41

Organisieren von Workloads mithilfe mehrerer Konten ... 41
Aktivieren von AWS-Services auf Organisationsebene über die Servicekonsole oder über API/CLI-Vorgänge ... 42
Verwenden von Abrechnungstools zur Verfolgung der Kosten und Optimierung der Ressourcennutzung ... 42
Planen der Tagging-Strategie und Durchsetzen von Tags für alle Organisationsressourcen ... 42
Bewährte Methoden für das Verwaltungskonto ... 43
Beschränken des Zugriffs auf das Verwaltungskonto auf bestimmte Personen ... 43
Überprüfen und Verfolgen des Zugriffs von Personen ... 43
Verwenden Sie das Verwaltungskonto nur für Aufgaben, die das Verwaltungskonto erfordern ... 44
Vermeiden der Bereitstellung von Workloads im Verwaltungskonto der Organisation ... 44
Delegieren von Aufgaben außerhalb des Verwaltungskontos zur Dezentralisierung ... 44
Bewährte Methoden für Mitgliedskonten ... 45
Definieren des Kontonamens und der Attribute ... 45
Effizientes Skalieren Ihrer Umgebung und Kontonutzung ... 45
Verwenden Sie einen SCP, um einzuschränken, was der Stammbenutzer in Ihren Mitgliedskonten tun kann ... 46
Erstellen und Verwalten einer Organisation ... 48
Erstellen einer Organisation ... 49
Erstellen einer Organisation ... 49
Verifizierung der E-Mail-Adresse ... 52
Aktivieren aller Funktionen ... 53
Bevor Sie alle Funktionen aktivieren ... 53
Beginn des Prozesses zur Aktivierung aller Funktionen ... 55
Genehmigung der Anforderung zum Aktivieren aller Funktionen oder zum Neuanlegen der servicegebundenen Rolle ... 58
Abschließen des Prozesses der Aktivierung aller Funktionen ... 62
Anzeigen der Organisationsdetails ... 65
Anzeigen von Details zu einer Organisation vom Verwaltungskonto aus ... 65
Anzeigen der Details des Root-Containers ... 66
Anzeigen von Details zu einer OU ... 68
Anzeigen von Details zu einem Konto ... 70
Anzeigen der Details einer Richtlinie ... 72
Löschen einer Organisation ... 74
Löschen einer Organisation ... 76

Verwalten von AWS-Konten in Ihrer Organisation 78
Auswirkungen der Mitgliedschaft in einer Organisation 78
Auswirkungen auf ein AWS-Konto, das einer Organisation beitritt? 78
Auswirkungen auf ein AWS-Konto, das Sie in einer Organisation erstellen? 79
Einladen eines Kontos zu Ihrer Organisation 80
Senden von Einladungen an AWS-Konten 82
Verwalten schwebender Einladungen für Ihre Organisation 86
Akzeptieren oder Ablehnen einer Einladung von einer Organisation 91
Erstellen eines Mitgliedskontos 95
Erstellen eines AWS-Konto, das Teil Ihrer Organisation ist 96
Zugreifen auf Mitgliedskonten 100
Zugreifen auf ein Mitgliedskonto als Root-Benutzer 101
Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto 102
Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt . 104
Exportieren von Kontodetails 107
Exportieren einer Liste aller AWS-Konten in Ihrer Organisation 107
Entfernen eines Mitgliedskontos 108
Überlegungen vor dem Entfernen eines Kontos aus einer Organisation 109
Entfernen eines Mitgliedskontos aus Ihrer Organisation 111
Verlassen einer Organisation in Ihrem Mitgliedskonto 115
Schließen eines Mitgliedskontos 119
So schließen Sie ein Mitgliedskonto 120
Schützen von Mitgliedskonten vor der Schließung 121
Schließen eines Verwaltungskontos 123
So schließen Sie ein Verwaltungskonto 123
Aktualisieren von alternativen Kontakten 124
Aktualisierung der primären Kontaktinformationen 124
Aktualisieren aktivierter AWS-Regionen 125
Verwalten von Organisationsrichtlinien 126
Richtlinientypen 126
Autorisierungsrichtlinien 126
Management-Richtlinien 126
Verwenden von Richtlinien in Ihrer Organisation 127
Aktivieren und Deaktivieren von Richtlinientypen 128
Aktivieren eines Richtlinientyps 128
Deaktivieren eines Richtlinientyps 129

Abrufen von Richtliniendetails ... 131
Auflisten aller Richtlinien ... 132
Angefügte Richtlinien auflisten ... 133
Alle Anhänge auflisten ... 135
Abrufen von Details zu einer Richtlinie ... 137
Delegierter Administrator für AWS Organizations ... 138
Erstellen oder Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie ... 139
Anzeigen einer ressourcenbasierte Delegierungsrichtlinie ... 144
Löschen einer ressourcenbasierte Delegierungsrichtlinie ... 145
Beispiel für Delegierungsrichtlinien ... 146
Management-Richtlinien ... 149
Grundlegendes zur Richtlinienvererbung ... 150
Richtlinien zur Abmeldung von KI-Services ... 167
Backup-Richtlinien ... 192
Tag-Richtlinien ... 245
Service-Kontrollrichtlinien ... 305
Testen der Auswirkungen von SCPs ... 307
Maximalgröße von SCPs ... 307
Anfügen von SCPs an verschiedene Ebenen in der Organisation ... 307
SCP-Auswirkungen auf Berechtigungen ... 307
Verwenden von Zugriffsdaten zur Verbesserung von SCPs ... 309
Aufgaben und Einheiten, die nicht durch SCPs eingeschränkt sind ... 310
Erstellen, Aktualisieren und Löschen ... 310
Anfügen und Trennen ... 323
SCP-Bewertung ... 327
SCP-Syntax ... 335
SCP-Beispiele ... 347
Verwalten von Organisationseinheiten (OUs) ... 373
Navigieren in der Struktur ... 373
Erstellen einer OU ... 375
Umbenennen einer OU ... 377
Markieren einer Organisationseinheit ... 379
Verschieben von Konten zwischen OUs ... 381
Löschen einer OU ... 383
Markieren von Ressourcen ... 385
Verwenden von Markierungen ... 386

Hinzufügen, Aktualisieren und Entfernen von Tags ... 386
Hinzufügen von Tags zu einer Ressource beim Erstellen ... 386
Hinzufügen oder Aktualisieren von Tags für eine vorhandene Ressource ... 387
Nutzung anderer AWS-Services ... 390
Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs ... 391
Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs ... 393
So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff ... 394
AWS Organizations und serviceverknüpfte Rollen ... 397
Services, die mit Organizations funktionieren ... 398
AWS Account Management ... 458
AWS Application Migration Service ... 462
AWS Artifact ... 467
AWS Audit Manager ... 471
AWS Backup ... 475
AWS CloudFormation-Stacksets ... 477
AWS CloudTrail ... 482
AWS Compute Optimizer ... 487
AWS Config ... 491
AWS Cost Optimization Hub ... 494
AWS Control Tower ... 497
Amazon Detective ... 500
Amazon DevOps Guru ... 504
AWS Directory Service ... 509
AWS Firewall Manager ... 511
Amazon GuardDuty ... 516
AWS Health ... 519
Amazon Inspector ... 523
AWS License Manager ... 528
Amazon Macie ... 531
AWS Marketplace ... 534
AWS Marketplace Private Marketplace ... 537
AWS Network Manager ... 541
AWS Resource Access Manager ... 545
AWS Ressourcen Explorer ... 549
AWS Security Hub ... 553
Amazon-S3-Storage-Lens ... 555

Amazon Security Lake ... 559
AWS Service Catalog ... 564
Service Quotas ... 568
AWS IAM Identity Center ... 570
AWS Systems Manager ... 574
Tag-Richtlinien ... 579
AWS Trusted Advisor ... 581
AWS Well-Architected Tool ... 584
Amazon VPC IP Address Manager (IPAM) ... 588
Amazon VPC Reachability Analyzer ... 592
Delegierter Administrator für integrierte AWS-Services ... 596
An Konten für delegierte Administratoren erteilte Berechtigungen ... 597
Sicherheit ... 599
AWS PrivateLink ... 600
Einschränkungen und Einschränkungen von für AWS PrivateLinkAWS Organizations ... 600
Erstellung eines VPC-Endpunkts ... 601
Erstellen einer VPC-Endpunktrichtlinie für AWS Organizations ... 601
IAM und Organizations ... 602
Authentifizierung ... 603
Zugriffskontrolle ... 604
Verwaltung von Zugriffsberechtigungen für Ihre AWS-Organisation ... 605
Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Organizations ... 614
Attributbasierte Zugriffskontrolle mit Tags ... 619
Protokollierung und Überwachung ... 624
Protokollierung von AWS Organizations-API-Aufrufen mit AWS CloudTrail ... 624
Amazon EventBridge ... 635
Compliance-Validierung ... 635
Ausfallsicherheit ... 636
Sicherheit der Infrastruktur ... 637
AWS Organizations-Referenz ... 638
Kontingente für AWS Organizations ... 638
Vorgaben für die Benennung ... 638
Höchst- und Mindestwerte ... 638
Drosselungsgrenzen ... 643
Verwaltete Richtlinien ... 646
AWS-verwaltete IAM-Richtlinien ... 646

Verwaltete AWS-Service-Kontrollrichtlinien 652
Fehlerbehebung bei AWS Organizations 653
Fehlerbehebung bei allgemeinen Problemen 653
Ich erhalte eine "Zugriff verweigert"-Meldung, wenn ich eine Anfrage an AWS Organizations stelle. 654
Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle 654
Ich erhalte eine „Zugriff verweigert“-Meldung, wenn ich versuche, eine Organisation als Mitgliedskonto zu verlassen oder ein Mitgliedskonto als Verwaltungskonto zu entfernen 655
Ich erhalte eine Meldung „Kontingent überschritten“, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen. 655
Ich erhalte die Meldung "Diese Operation benötigt eine Wartezeit", wenn ich Konten hinzufüge oder entferne. 656
Ich erhalte eine Meldung, dass die Organisation immer noch initialisiert wird, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen. 656
Ich erhalte die Meldung „Einladungen sind deaktiviert“, wenn ich versuche, ein Konto zu meiner Organisation einzuladen. 656
Änderungen, die ich vornehme, sind nicht immer direkt sichtbar 656
Fehlerbehebung bei -Richtlinien 657
Service-Kontrollrichtlinien 657
Erstellen von HTTP-Abfrageanforderungen 661
Endpunkte 662
HTTPS erforderlich 662
Signieren von AWS Organizations-API-Anforderungen 662
Dokumentverlauf 663
AWS-Glossar 676
..... dclxxvii

Was ist AWS Organizations?

AWS Organizations ist ein Kontoverwaltungsservice, mit dem Sie mehrere AWS-Konten in einer zentral erstellten und verwalteten Organisation konsolidieren können. AWS Organizations umfasst Kontoverwaltungs- und konsolidierte Fakturierungsservices, die es Ihnen ermöglichen, die Budget-, Sicherheits- und Compliance-Anforderungen Ihres Unternehmens besser zu erfüllen. Als Administrator einer Organisation können Sie Konten in Ihrer Organisation anlegen und bestehende Konten einladen, der Organisation beizutreten.

Dieses Benutzerhandbuch definiert wichtige Konzepte für AWS Organizations, stellt Tutorials zur Verfügung und erklärt, wie eine Organisation erstellt und verwaltet wird.

Themen

- AWS Organizations-Merkmale
- AWS Organizations – Preise
- Zugriff auf AWS Organizations
- Support und Feedback zu AWS Organizations

AWS Organizations-Merkmale

AWS Organizations bietet folgende Funktionen:

Zentrale Verwaltung Ihrer gesamten AWS-Konten

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.

Konsolidierte Fakturierung für alle Mitgliedskonten

Die konsolidierte Fakturierung ist eine Funktion von AWS Organizations. Sie können das Verwaltungskonto Ihrer Organisation zur Konsolidierung und Zahlung für alle Mitgliedskonten nutzen. Bei der konsolidierten Fakturierung können Verwaltungskonto auch auf die Fakturierungsdaten, Kontoinformationen und Kontoaktivitäten von Mitgliedskonten in ihrer Organisation zugreifen. Diese Informationen können für Services wie Cost Explorer verwendet werden, mit denen bei Verwaltungskonto die Kostenleistung ihrer Organisation verbessert werden kann.

Hierarchische Gruppierung Ihrer Konten zur Umsetzung Ihrer Budget-, Sicherheits- und Compliance-Anforderungen

Sie können Ihre Konten mit Hilfe von Organisationseinheiten (OUs) gruppieren und an jede OU andere Zugriffsrichtlinien anhängen. Wenn Sie zum Beispiel Konten nutzen, die nur auf die AWS-Services mit bestimmten gesetzlichen Anforderungen zugreifen sollen, dann können Sie diese Konten in einer Organisationseinheit zusammenfassen. Dann hängen Sie eine Richtlinie an die OU an, die den Zugriff auf Services ohne die erforderlichen gesetzlichen Anforderungen blockiert. OUs können in anderen OUs verschachtelt werden. Es sind 5 Verschachtelungsebenen möglich. So können Sie Ihre Kontogruppen flexibler strukturieren.

Richtlinien zur Zentralisierung der Kontrolle über die AWS-Services und API-Aktionen, auf die jedes Konto zugreifen kann

Als Administrator des Verwaltungskonto einer Organisation können Sie Service-Kontrollrichtlinien (SCPs) verwenden, um die maximalen Berechtigungen für Mitgliedskonten in der Organisation anzugeben. In den SCPs können Sie einschränken, auf welche AWS-Services, -Ressourcen und einzelne API-Aktionen die Benutzer und Rollen in jedem Mitgliedskonto zugreifen dürfen. Sie können auch Bedingungen für den Zeitpunkt festlegen, wann der Zugriff auf die AWS-Services, -Ressourcen und API-Aktionen eingeschränkt werden soll. Diese Einschränkung überschreibt sogar die Administratoren von Mitgliedskonten in der Organisation. Wenn der Zugriff auf einen Service, eine Ressource oder eine API-Aktion für ein Mitgliedskonto in AWS Organizations blockiert, hat ein Benutzer oder eine Rolle in diesem Konto keinen Zugriff darauf. Diese Blockierung bleibt auch dann bestehen, wenn ein Administrator eines Mitgliedskontos solche Berechtigungen mittels einer IAM-Richtlinie explizit erteilt.

Weitere Informationen finden Sie unter Service-Kontrollrichtlinien (SCPs).

Richtlinien zur Standardisierung von Tags für alle Ressourcen in den Konten Ihrer Organisation

Sie können mit Tag-Richtlinien eine konsistente Tag-Verwaltung sicherstellen, auch in Bezug auf die bevorzugte Fallbehandlung von Tag-Schlüsseln und Tag-Werten.

Weitere Informationen finden Sie unter Tag-Richtlinien.

Richtlinien zur Steuerung, wie AWS-Services für künstliche Intelligenz (KI) und Machine Learning Daten erfassen und speichern können.

Sie können die Deaktivierungsrichtlinien für KI-Services verwenden, um die Datenerfassung und -speicherung für alle AWS-KI-Services abzulehnen, die Sie nicht verwenden möchten.

Weitere Informationen finden Sie unter Richtlinien zur Abmeldung von KI-Services.

Richtlinien zum Konfigurieren der automatischen Backups für die Ressourcen in den Konten Ihrer Organisation

Sie können Backup-Richtlinien verwenden, um AWS Backup-Pläne zu konfigurieren und automatisch auf Ressourcen in allen Konten Ihrer Organisation anzuwenden.

Weitere Informationen finden Sie unter Backup-Richtlinien.

Integration und Unterstützung für AWS Identity and Access Management (IAM)

IAM ermöglicht eine genaue Kontrolle über die Benutzer und Rollen in den einzelnen Konten. AWS Organizations erweitert diese Kontrolle auf die Kontoebene. Sie erhalten die Kontrolle darüber, was Benutzer und Rollen in einem Konto oder einer Kontengruppe durchführen können. Die so entstehenden Berechtigungen ergeben sich aus der Schnittmenge der Berechtigungen, die von AWS Organizations auf Kontoebene zugelassen wurden, und der explizit per IAM auf Endbenutzer- oder Rollenebene des Kontos gewährten Berechtigungen. Der Benutzer kann also nur auf das zugreifen, was in den AWS Organizations-Richtlinien und IAM-Richtlinien zugelassen ist. Wenn eine Operation in einem der Elemente blockiert ist, kann der Benutzer diese nicht durchführen.

Integration in andere AWS-Services

Sie können die in AWS Organizations verfügbaren Services für die Multikontenverwaltung für bestimmte AWS-Services nutzen, um Aufgaben für alle Konten auszuführen, die Mitglied Ihrer Organisation sind. Eine Liste der Services und die Vorteile der Verwendung der einzelnen Services auf unternehmensweiter Ebene finden Sie unter AWS Dienste, die Sie mit verwenden können AWS Organizations.

Wenn Sie einen AWS-Service aktivieren, um in Ihrem Namen Aufgaben in den Mitgliedskonten Ihrer Organisation auszuführen, erstellt AWS Organizations in jedem Mitgliedskonto eine serviceverknüpfte IAM-Rolle für diesen Service. Die servicegebundene Rolle hat vordefinierte IAM-Berechtigungen, die es dem anderen AWS-Service ermöglichen, bestimmte Aufgaben in Ihrer Organisation und deren Konten auszuführen. Damit dies funktioniert, verfügen alle Konten in einer Organisation automatisch über eine serviceverknüpfte Rolle. Diese Rolle gestattet dem AWS Organizations-Service die Erstellung der serviceverknüpften Rollen, die für AWS-Services erforderlich sind, für die Sie den vertrauenswürdigen Zugriff aktivieren. Diese zusätzlichen serviceverknüpften Rollen sind an IAM-Berechtigungsrichtlinien angehängt, die es dem angegebenen Service ermöglichen, nur die Aufgaben auszuführen, die für Ihre Konfigurationsoptionen erforderlich sind. Weitere Informationen finden Sie unter Verwenden von AWS Organizations mit anderen AWS-Services.

Globaler Zugriff

AWS Organizations ist ein globaler Service mit einem einzelnen Endpunkt, der von allen AWS-Regionen aus arbeiten kann. Sie müssen keine Region explizit auswählen, in der Sie arbeiten möchten.

Eventually-Consistent-Datenreplikation

Wie viele andere AWS-Services, arbeitet auch AWS Organizations mit einem Eventually Consistency-Konzept. AWS Organizations erreicht eine Hochverfügbarkeit, indem die Daten über mehrere AWS-Rechenzentren in seiner Region repliziert werden. Wenn eine Anforderung zur Änderung von Daten erfolgreich ist, wird die Änderung übernommen und sicher gespeichert. Die Änderung muss dann jedoch auf die verschiedenen Server repliziert werden. Weitere Informationen finden Sie unter Änderungen, die ich vornehme, sind nicht immer direkt sichtbar.

Kostenlos

AWS Organizations ist eine Funktion Ihres AWS-Konto, die ohne zusätzliche Kosten angeboten wird. Ihnen werden nur dann Gebühren in Rechnung gestellt, wenn Sie über die Konten in Ihrer Organisation auf andere AWS-Services zugreifen. Für Informationen zu den Preisen anderer AWS-Produkte finden Sie in der Amazon-Web-Services-Preisseite.

AWS Organizations – Preise

AWS Organizations wird ohne Aufpreis angeboten. Ihnen werden nur die AWS-Ressourcen berechnet, die die Benutzer und Rollen in Ihren Mitgliedskonten verwenden. Ihnen werden zum Beispiel die Standardgebühren für Amazon-EC2-Instances berechnet, die von den Benutzern oder Rollen in Ihren Mitgliedskonten verwendet werden. Informationen zu den Preisen anderer AWS-Services finden Sie unter AWS-Preise.

Zugriff auf AWS Organizations

Sie können AWS Organizations auf folgende Art und Weise nutzen:

AWS Management Console

Die AWS Organizations-Konsole ist eine browserbasierte Schnittstelle, über die Sie Ihre Organisation und Ihre AWS-Ressourcen verwalten können. Sie können mithilfe der Konsole sämtliche Aufgaben in Ihrer Organisation ausführen.

AWS-Befehlszeilen-Tools

Mit den Befehlszeilen-Tools von AWS können Sie Befehle in der Befehlszeile Ihres Systems ausgeben und AWS Organizations- und AWS-Aufgaben durchführen. Die Arbeit mit der Befehlszeile kann schneller und bequemer sein als die Verwendung der Konsole. Die Befehlszeilen-Tools sind auch hilfreich, wenn Sie Skripts erstellen möchten, die AWS-Aufgaben ausführen.

AWS bietet zwei Sätze an Befehlszeilen-Tools:

- AWS Command Line Interface (AWS CLI). Informationen zum Installieren und Verwenden von AWS CLI finden Sie im AWS Command Line Interface-Benutzerhandbuch.
- AWS Tools for Windows PowerShell. Informationen zum Installieren und Verwenden der Tools for Windows PowerShell finden Sie im AWS Tools for Windows PowerShell-Benutzerhandbuch.

AWS-SDKs

Die AWS-SDKs bestehen aus Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen (beispielsweise Java, Python, Ruby, .NET, iOS und Android). Mit den SDKs lassen sich unter anderem Anforderungen kryptografisch signieren, Fehler verwalten und Anforderungen automatisch wiederholen. Weitere Informationen über die AWS-SDKs, inkl. Herunterladen und Installation, finden Sie unter Tools für Amazon Web Services.

AWS Organizations-HTTPS-Query-API

Die AWS Organizations-HTTPS-Query-API bietet programmgesteuerten Zugriff auf AWS Organizations 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 über die HTTP-Query-Anforderungen und im AWS OrganizationsAPI-Referenz.

Support und Feedback zu AWS Organizations

Wir freuen uns über Ihr Feedback. Senden Sie Ihre Kommentare an feedback-awsorganizations@amazon.com. Sie können Ihr Feedback und Ihre Fragen auch im AWS Organizations-Support-Forum posten. Weitere Informationen zu den AWS-Support-Foren finden Sie unter Forenhilfe.

Sonstige AWS-Ressourcen

- AWS Training und Kurse – Links zu rollenbasierten und speziellen Kursen sowie Übungseinheiten zum Selbststudium zur Verbesserung der AWS-Kompetenzen und für praktische Erfahrung.
- AWS-Entwicklertools – Links zu Entwicklertools und -Ressourcen mit Dokumentationen, Codebeispielen, Versionshinweisen und sonstigen Informationen für die Entwicklung innovativer Anwendungen mit AWS.
- AWS Support-Center – Der zentrale Ort für die Erstellung und Verwaltung Ihrer AWS Support-Fälle. Bietet außerdem Links zu hilfreichen Ressourcen wie z. B. Foren, technischen Fragen und Antworten, Übersicht zum Servicestatus und AWS Trusted Advisor.
- AWS-Support – Die Hauptwebsite mit Informationen zum AWS-Support ist ein persönlicher und reaktionsschneller Support-Kanal, der Sie beim Konfigurieren und Ausführen von Anwendungen in der Cloud unterstützt.
- Kontakt – Zentraler Kontaktpunkt für Fragen zu AWS-Abrechnung, Konten, Ereignissen Missbrauch und anderen Problemen.
- Nutzungsbedingungen für die AWS-Website – Detaillierte Informationen zu unseren Copyright- und Markenbestimmungen, Ihrem Konto, den Lizenzen und anderen Themen.

Erste Schritte mit AWS Organizations

Die folgenden Themen enthalten Informationen, die Sie bei den ersten Schritten mit AWS Organizations unterstützen.

Informationen über...

[Terminologie und Konzepte von AWS Organizations]

Informieren Sie sich über die Terminologie und zentralen Konzepte zu AWS Organizations. Dieser Abschnitt beschreibt die einzelnen Komponenten einer Organisation und die Grundlagen ihrer Zusammenarbeit, um ein neues Level der Kontrolle darüber zu ermöglichen, was Benutzer in diesen Konten tun können.

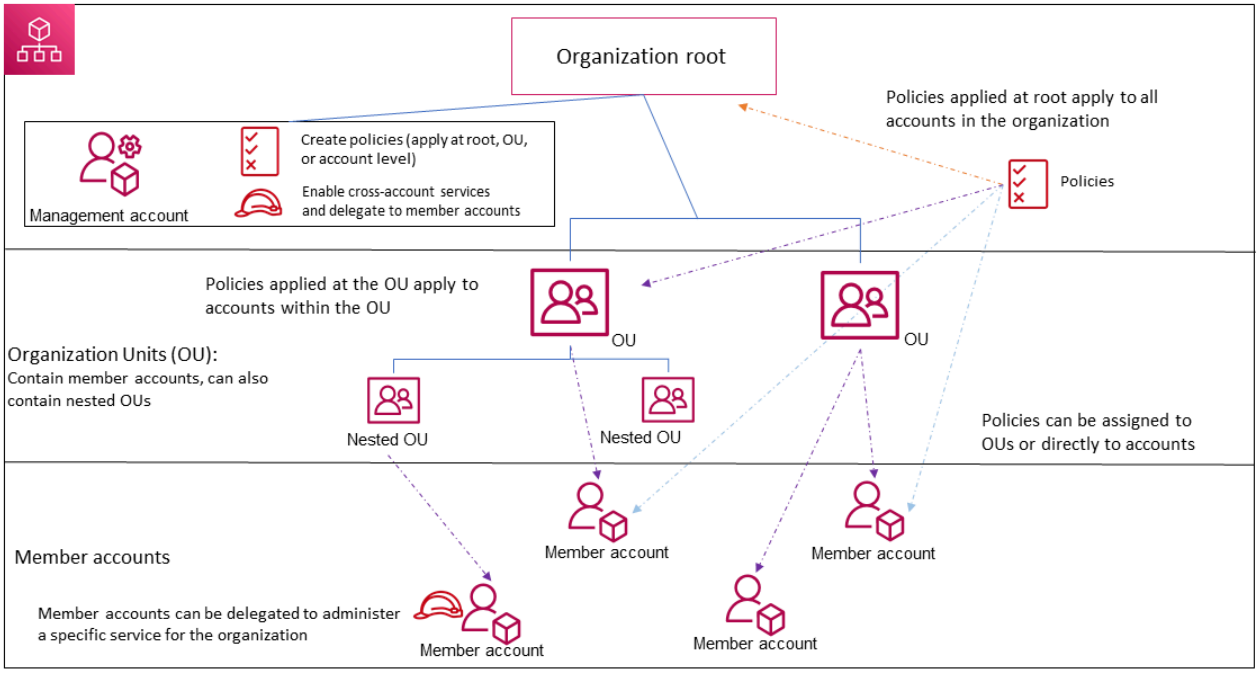
[Konsolidierte Fakturierung für Organisationen]

Eine der wichtigsten Funktionen von AWS Organizations ist die Konsolidierung der Abrechnung aller Konten in Ihrer Organisation. Erfahren Sie mehr darüber, wie die Fakturierung in einer Organisation abgewickelt wird und wie verschiedene Rabatte funktionieren, wenn sie über mehrere Konten verteilt werden. Dieser Inhalt ist im AWS Billing-Benutzerhandbuch.

Terminologie und Konzepte von AWS Organizations

In diesem Thema werden die wichtigsten Konzepte vorgestellt, um Ihnen den Einstieg in AWS Organizations zu erleichtern.

Das folgende Diagramm zeigt eine einfache Organisation, die aus fünf Konten in vier Organisationseinheiten (OU) unterhalb des Roots besteht. Außerdem gibt es in der Organisation mehrere Richtlinien, die einigen der OUs oder aber den Konten direkt zugeordnet wurden. Eine Beschreibung der einzelnen Elemente finden Sie in den Definitionen in diesem Thema.



Organisation

Eine Entität, die Sie erstellen, um Ihre AWS-Konten zu konsolidieren, damit Sie sie als einzelne Einheit verwalten können. In der AWS Organizations-Konsole können Sie alle Konten der Organisation zentral anzeigen und verwalten. Eine Organisation besteht aus einem Verwaltungskonto und gegebenenfalls mehreren Mitgliedskonten. Die Konten lassen sich in einer hierarchischen Baumstruktur mit dem Root an der Spitze und Organisationseinheiten unterhalb des Roots anordnen. Jedes Konto kann sich direkt unterhalb des Roots oder in einer OUs in der Hierarchie befinden. Eine Organisation verfügt über die Funktionalität, die vom aktivierten Featuresatz bestimmt wird.

Root

Der übergeordnete Container für alle Konten Ihrer Organisation. Wenn Sie einem Root eine Richtlinie zuordnen, gilt diese für alle Organisationseinheiten und Konten in der Organisation.

> **Note**
>
> Derzeit ist nur ein Root möglich. AWS Organizations erstellt diesen automatisch bei der Einrichtung der Organisation.

Organisationseinheit (OU)

Ein Container für Konten in einem Root. Eine Organisationseinheit kann weitere OUs enthalten; so entsteht eine Ebenenhierarchie, die an einen umgekehrten Baum erinnert – mit der Wurzel (Root) an der Spitze, von der Äste (Organisationseinheiten) abgehen, die in Blätter (Konten) münden. Wenn Sie einem der Knoten in der Hierarchie eine Richtlinie zuordnen, gilt diese für nachgeordnete Entitäten und wirkt sich auf alle folgenden Organisationseinheiten und Konten aus. Eine Organisationseinheit kann nur ein übergeordnetes Element haben und derzeit kann jedes Konto genau einer Organisationseinheit angehören.

Account

Ein Konto in Organizations ist ein Standard-AWS-Konto, das Ihre AWS-Ressourcen und die Identitäten enthält, die auf diese Ressourcen zugreifen können.

> **Tip**
>
> Ein AWS-Konto ist nicht das Gleiche wie ein „Benutzerkonto“. Ein AWSBenutzer ist eine Identität, die Sie mit AWS Identity and Access Management (IAM) erstellen und die entweder die Form eines IAM-Benutzer mit langfristigen Anmeldeinformationen, oder einer IAM-Rolle mit kurzfristigen Anmeldeinformationen einnimmt. Ein einzelnes AWS-Konto kann und enthält in der Regel viele Benutzer und Rollen.

Es gibt zwei Arten von Konten in einer Organisation: ein einzelnes Konto, das als Verwaltungskonto festgelegt ist, und ein oder mehrere Mitgliedskonten.

- Das Verwaltungskonto ist das Konto, das Sie zur Erstellung der Organisation verwenden. Über das Verwaltungskonto der Organisation haben Sie folgende Möglichkeiten:
  - Erstellen von Konten in der Organisation
  - Einladen anderer vorhandener Konten zur Organisation
  - Entfernen von Konten aus der Organisation
  - Festlegen von Konten für delegierte Administratoren
  - Verwalten von Einladungen
  - Anwenden von Richtlinien auf Entitäten (Roots, OUs oder Konten) innerhalb der Organisation
  - Aktivieren Sie die Integration mit unterstützten AWS-Services, um Service-Funktionen für alle Konten in der Organisation bereitzustellen.

Das Verwaltungskonto hat die Aufgabe eines Zahlungskontos; von ihm gehen sämtliche Gebühren ab, die auf den Mitgliedskonten anfallen. Sie können das Verwaltungskonto einer Organisation nicht ändern.

- Mitgliedskonten bilden alle übrigen Konten in einer Organisation. Ein Konto kann jeweils nur einer Organisation angehören. Sie können einem Konto eine Richtlinie zuordnen und damit eine bestimmte Steuerung nur auf dieses Konto anwenden.

> **Note**
>
> Sie können einige Mitgliedskonten als Konten für delegierte Administratoren festlegen. Siehe Delegierter Administrator unten.

Delegated Administrator

Wir empfehlen, das Verwaltungskonto von Organizations und die zugehörigen Benutzer und Rollen nur für Aufgaben zu verwenden, die über dieses Konto ausgeführt werden müssen. Die AWS-Ressourcen sollten Sie in anderen Mitgliedskonten in der Organisation speichern und aus dem Verwaltungskonto heraushalten. Der Grund dafür ist, dass Sicherheitsfeatures wie die Service-Kontrollrichtlinien (SCPs) von Organizations keine Benutzer oder Rollen im Verwaltungskonto einschränken. Durch die Trennung der Ressourcen vom Verwaltungskonto können Sie außerdem die Kosten auf Ihren Rechnungen leichter nachvollziehen. Zur Umsetzung dieser Empfehlung können Sie über das Verwaltungskonto der Organisation ein oder mehrere Mitgliedskonten als Konto für einen delegierten Administrator festlegen. Es gibt zwei Arten von delegierten Administratoren:

- Delegierter Administrator für Organizations: Über diese Konten können Sie Organisationsrichtlinien verwalten und Richtlinien an Entitäten (Roots, Organisationseinheiten oder Konten) in der Organisation anfügen. Über das Verwaltungskonto lassen sich Delegierungsberechtigungen auf granularer Ebene festlegen. Weitere Informationen finden Sie unter Delegierter Administrator für AWS Organizations.
- Delegierter Administrator für einen AWS-Service: Über diese Konten können Sie AWS-Services verwalten, die in Organizations integriert sind. Über das Verwaltungskonto können verschiedene Mitgliedskonten nach Bedarf als delegierte Administratoren für verschiedene Services registriert werden. Diese Konten verfügen über Administratorberechtigungen für einen bestimmten Service sowie über reine Leseberechtigungen für Organizations. Weitere Informationen finden Sie unter Delegierter Administrator für AWS-Services, die mit Organizations zusammenarbeiten.

Einladung

Hiermit ist der Prozess der Einladung eines anderen Kontos zum Beitritt zu Ihrer Organisation gemeint. Eine Einladung kann nur vom Verwaltungskonto der Organisation ausgehen. Die Einladung wird entweder auf die Konto-ID oder die E-Mail-Adresse erweitert, die dem eingeladenen Konto zugeordnet ist. Wenn das eingeladene Konto eine Einladung annimmt, wird es zum Mitgliedskonto in der Organisation. Einladungen können auch an alle aktuellen Mitgliedskonten gesendet werden – nämlich dann, wenn alle Mitglieder den Wechsel von der Unterstützung der Funktionen für konsolidierte Fakturierung zur Unterstützung aller Funktionen genehmigen sollen. Die Verarbeitung von Einladungen erfolgt durch den Austausch von Handshakes durch die Konten. Möglicherweise werden beim Arbeiten in der AWS Organizations-Konsole keine Handshakes angezeigt. Wenn Sie aber die AWS CLI oder AWS Organizations-API verwenden, müssen Sie direkt mit Handshakes arbeiten.

Handshake

Ein aus mehreren Schritten bestehender Prozess des Informationsaustauschs zwischen zwei Parteien. In AWS Organizations dienen Handshakes hauptsächlich als Grundlage für Einladungen. Handshake-Nachrichten werden zwischen dem Handshake-Initiator und dem Empfänger übergeben, und beide Parteien reagieren darauf. Die Nachrichten werden so übergeben, dass beide Parteien den aktuellen Status kennen. Handshakes werden auch eingesetzt, wenn die Organisation einen Wechsel von der Unterstützung der Funktionen für konsolidierte Abrechnung zur Unterstützung aller von bereitgestellten FunktionenAWS Organizations plant. Im Allgemeinen haben Sie es nur dann direkt mit Handshakes zu tun, wenn Sie mit der AWS Organizations-API oder Befehlszeilen-Tools wie der AWS CLI arbeiten.

Verfügbare Featuresätze

- Alle Features – Der standardmäßige Featuresatz für AWS Organizations. Dieser enthält jede Funktionalität der konsolidierten Fakturierung sowie erweiterte Funktionen, mit denen Sie die Konten in Ihrer Organisation besser steuern können. Wenn alle Funktionen aktiviert sind, hat das Verwaltungskonto der Organisation die vollständige Kontrolle über die Aktionen der Mitgliedskonten. Das Verwaltungskonto kann durch Zuweisung von SCPs die Services und Aktionen beschränken, auf die Benutzer (einschließlich des Root-Benutzers) und Rollen in einem Konto zugreifen dürfen. Das Verwaltungskonto kann zudem verhindern, dass Mitgliedskonten die Organisation verlassen. Sie können auch die Integration mit unterstützten AWS-Services aktivieren, damit diese Services Funktionen für alle Konten in Ihrer Organisation bereitstellen.

Sie können entweder eine Organisation erstellen, in der alle Funktionen bereits aktiviert sind, oder alle Funktionen in einer Organisation aktivieren, die ursprünglich nur die konsolidierte Fakturierung unterstützt hat. Wenn Sie alle Funktionen aktivieren möchten, müssen alle eingeladen Mitgliedskonten die Änderung genehmigen und die Einladung annehmen, die bei der Initiierung des Prozesses durch das Verwaltungskonto gesendet wurde.

- Konsolidierte Fakturierung – Dieser Featuresatz enthält gemeinsame Abrechnungsfunktionen, nicht jedoch die erweiterten Features von AWS Organizations. Sie können beispielsweise nicht aktivieren, dass andere AWS-Dienste in Ihre Organisation integriert werden, um über alle Konten hinweg zu funktionieren, oder Richtlinien verwenden, um einzuschränken, was Benutzer und Rollen in verschiedenen Konten tun können. Zur Verwendung der erweiterten AWS Organizations-Funktionen müssen Sie alle Funktionen in Ihrer Organisation aktivieren.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie mit einer Liste der Services und Aktionen, die Benutzer und Rollen in den von der SCP betroffenen Konten ausführen dürfen. SCPs ähneln den IAM-Berechtigungsrichtlinien; sie gewähren allerdings keine Berechtigungen. Stattdessen sind in SCPs die maximalen Berechtigungen für eine Organisation, eine Organisationseinheit (OU) oder ein Konto angegeben. Wenn Sie eine SCP an den Stamm Ihrer Organisation oder eine Organisationseinheit anfügen, beschränkt die SCP die Berechtigungen für die Entitys in den Mitgliedskonten.

Whitelists im Vergleich zu Sperrlisten

Whitelists und Sperrlisten sind ergänzende Strategien bei der Anwendung von SCPs, um die Berechtigungen zu filtern, die für Konten verfügbar sind.

- Whitelist-Strategie – Hier geben Sie explizit an, dass ein bestimmter Zugriff erlaubt ist. Alle anderen Zugriffe werden stillschweigend blockiert. Standardmäßig weist AWS Organizations allen Roots, OUs und Konten eine verwaltete AWS-Richtlinie namens `FullAWSAccess` zu. Auf diese Weise wird sichergestellt, dass bei der Erstellung der Organisation keine Zugriffe blockiert werden, wenn Sie es nicht wünschen. Mit anderen Worten, standardmäßig sind alle Berechtigungen zugelassen. Wenn Sie die Berechtigungen beschränken möchten, ersetzen Sie die `FullAWSAccess`-Richtlinie durch eine Richtlinie, die die gewünschten Einschränkungen enthält. Benutzer und Rollen in den betroffenen Konten können dann nur in diesem Maß auf Services und Aktionen zugreifen, auch wenn gemäß ihren IAM-Richtlinien alle Aktionen zugelassen sind. Wenn Sie die Standardrichtlinie für den Root-Benutzer ersetzen, wirken sich die Einschränkungen auf alle Konten in der Organisation aus. Es ist nicht möglich,

Berechtigungen auf einer unteren Hierarchieebene wieder hinzuzufügen, denn eine SCP gewährt Berechtigungen nicht, sondern filtert sie nur.

- Sperrlisten-Strategie – Hier geben Sie explizit an, dass ein bestimmter Zugriff nicht erlaubt ist. Alle anderen Zugriffe sind möglich. In diesem Szenario werden alle Berechtigungen gewährt, es sei denn, sie werden explizit gesperrt. Dies ist das Standardverhalten von AWS Organizations. Standardmäßig weist AWS Organizations allen Roots, OUs und Konten eine verwaltete AWS-Richtlinie namens `FullAWSAccess` zu. Auf diese Weise kann jedes Konto uneingeschränkt auf alle AWS Organizations-Services und -Operationen zugreifen. Anders als bei den oben beschriebenen Whitelists bleibt bei Verwendung von Sperrlisten die `FullAWSAccess`-Standardrichtlinie („Alle zulassen“) aktiv. Sie fügen dann aber zusätzliche Richtlinien hinzu, die den Zugriff auf unerwünschte Services und Aktionen explizit verweigern. Ähnlich wie bei IAM-Berechtigungsrichtlinien wird eine Zugriffserlaubnis durch eine explizite Zugriffsverweigerung überschrieben.

Richtlinie zur Abmeldung von Services für künstliche Intelligenz (KI)

Eine Art von Richtlinie, die Ihnen hilft, Ihre Opt-out-Einstellungen für AWS-KI-Services für alle Konten in Ihrer Organisation zu standardisieren. Bestimmte AWS-KI-Services können Kundeninhalte speichern und verwenden, die von diesen Services verarbeitet werden, um die KI-Services und -Technologien von Amazon zu entwickeln und kontinuierlich zu verbessern. Als AWS-Kunde können Sie die Deaktivierungsrichtlinien für KI-Services verwenden, um zu entscheiden, ob Ihre Inhalte gespeichert oder für Serviceverbesserungen verwendet werden.

Backup-Richtlinie

Diese Art von Richtlinie hilft Ihnen, eine Backup-Strategie für die Ressourcen über alle Konten in Ihrer Organisation zu standardisieren und zu implementieren. In einer Backup-Richtlinie können Sie Backup-Pläne für Ihre Ressourcen konfigurieren und bereitstellen.

Tag-Richtlinie

Eine Art von Richtlinie, mit der Sie Tags für alle Ressourcen in allen Konten Ihrer Organisation standardisieren können. In einer Tag-Richtlinie können Sie Tagging-Regeln für bestimmte Ressourcen angeben.

AWS Organizations-Anleitungen

Verwenden Sie die Tutorials in diesem Abschnitt, um zu erfahren, wie Sie Aufgaben mit AWS Organizations durchführen.

Praktische Anleitung: Erstellen und Konfigurieren einer Organisation

Einrichtung mit Schritt-für-Schritt-Anleitungen zum Erstellen Ihrer Organisation, Einladen der ersten Mitgliedskonten, Erstellen einer einfachen Organisationseinheitshierarchie mit Ihren Konten und Anwenden einiger Service-Kontrollrichtlinien (SCPs).

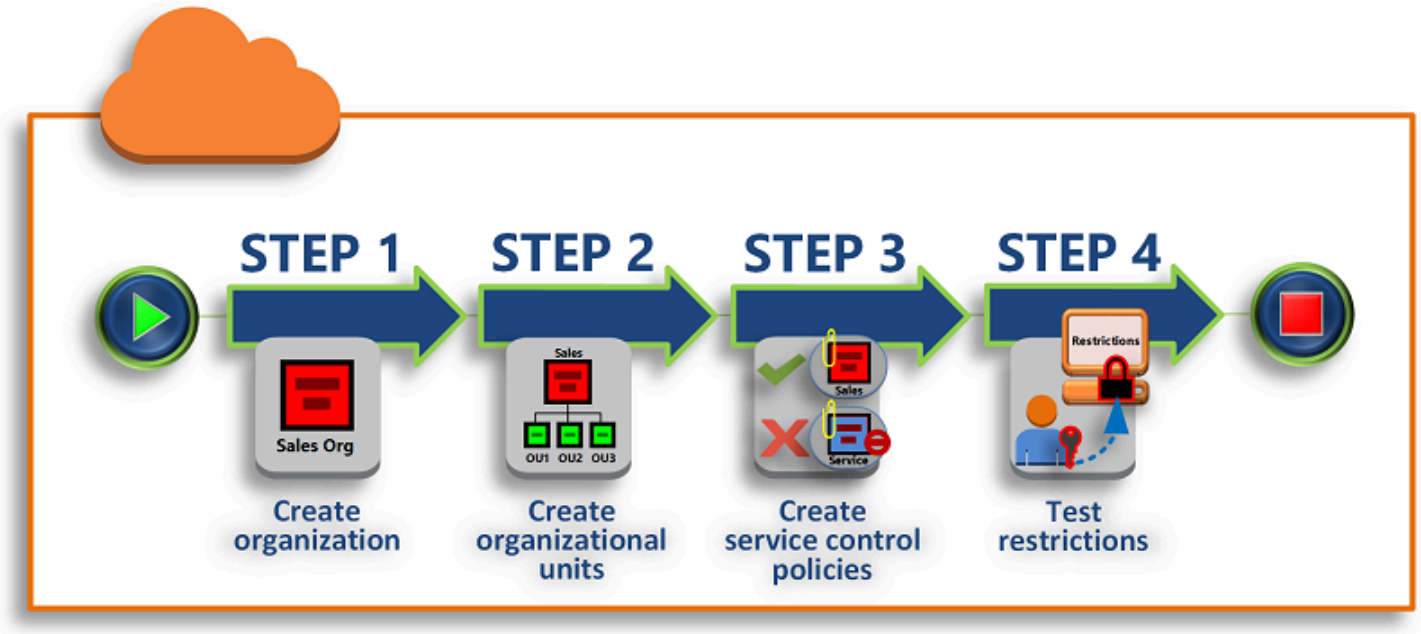
Tutorial: Überwachen wichtiger Änderungen an Ihrer Organisation mit Amazon EventBridge

Überwachen Sie wichtige Änderungen in Ihrer Organisation, indem Sie Amazon EventBridge konfigurieren, sodass bei von Ihnen angegebenen Aktionen in der Organisation ein Alarm in Form einer E-Mail, einer SMS oder eines Protokolleintrags ausgelöst wird. Viele Unternehmen möchten beispielsweise wissen, wann ein neues Konto erstellt wird, oder wann ein Konto versucht, das Unternehmen zu verlassen.

Praktische Anleitung: Erstellen und Konfigurieren einer Organisation

In dieser praktischen Anleitung erstellen Sie Ihre Organisation und konfigurieren diese mit zwei AWS-Mitgliedskonten. Sie erstellen eines der Mitgliedskonten in Ihrer Organisation und laden das andere Konto zum Beitritt Ihrer Organisation ein. Als Nächstes geben Sie mithilfe der Whitelist-Technik an, dass die Kontoadministratoren nur explizit aufgelistete Services und Aktionen delegieren können. So können Administratoren jeden neuen Service, den AWS einführt, überprüfen, bevor sie den Benutzern in Ihrem Unternehmens erlauben, ihn zu verwenden. Wenn AWS einen neuen Service einführt, bleibt dieser auf diese Weise verboten, bis ein Administrator den Service der Whitelist in der entsprechenden Richtlinie hinzufügt. Die praktische Anleitung zeigt Ihnen außerdem, wie Sie mithilfe von Sperrlisten sicherstellen, dass kein Benutzer in einem Mitgliedskonto die Konfiguration für die Audit-Protokolle, die von AWS CloudTrail erstellt werden, ändert.

Die folgende Abbildung zeigt die wichtigsten Schritte der praktischen Anleitung.



Schritt 1: Erstellen Ihrer Organisation

In diesem Schritt erstellen Sie eine Organisation mit Ihrem aktuellen AWS-Konto als Verwaltungskonto. Sie laden außerdem ein AWS-Konto zum Beitritt Ihrer Organisation ein und erstellen ein zweites Konto als Mitgliedskonto.

Schritt 2: Erstellen der Organisationseinheiten

Als Nächstes erstellen Sie zwei Organisationseinheiten in der neuen Organisation und platzieren Sie die Mitgliedskonten in diese Organisationseinheiten.

Schritt 3: Erstellen von Service-Kontrollrichtlinien

Sie können die Aktionen, die an Benutzer und Rollen in den Mitgliedskonten delegiert werden, anhand der Service-Kontrollrichtlinien (SCPs) einschränken. In diesem Schritt erstellen Sie zwei SCPs und ordnen Sie den Organisationseinheiten in Ihrer Organisation zu.

Schritt 4: Testen der Organisationsrichtlinien

Sie können sich als Benutzer eines der Testkonten anmelden und die Auswirkungen ansehen, die die Service-Kontrollrichtlinien auf die Konten haben.

Bei keinem der Schritte in dieser praktischen Anleitung fallen Kosten an, die auf Ihre AWS-Rechnung gesetzt werden. AWS Organizations ist ein kostenloser Service.

Voraussetzungen

In dieser praktischen Anleitung wird davon ausgegangen, dass Sie Zugriff auf zwei vorhandene AWS-Konten haben (ein drittes Konto erstellen Sie im Rahmen dieser Anleitung) und dass Sie sich an beiden als Administrator anmelden können.

Die praktische Anleitung bezieht sich auf folgende Konten:

- `111111111111` – Das Konto, das Sie zur Erstellung der Organisation verwenden. Dieses Konto wird zum Verwaltungskonto. Der Inhaber dieses Kontos hat die E-Mail-Adresse `OrgAccount111@example.com`.
- `222222222222` – Ein Konto, das Sie zum Beitritt zur Organisation als Mitgliedskonto einladen. Der Inhaber dieses Kontos hat die E-Mail-Adresse `member222@example.com`.
- `333333333333` – Ein Konto, das Sie als Mitglied der Organisation erstellen. Der Inhaber dieses Kontos hat die E-Mail-Adresse `member333@example.com`.

Ersetzen Sie die obigen Wert mit den Werten für Ihre Testkonten. Wir empfehlen Ihnen, keine Produktionskonten für diese praktische Anleitung zu verwenden.

Schritt 1: Erstellen Ihrer Organisation

In diesem Schritt melden Sie sich am Konto 111111111111 als Administrator an, erstellen eine Organisation mit diesem Konto als Verwaltungskonto und laden ein vorhandenes Konto 222222222222 zum Beitritt zur Organisation als Mitgliedskonto ein.

AWS Management Console

1. Melden Sie sich bei AWS als Administrator von Konto 111111111111 an und öffnen Sie die AWS Organizations-Konsole.
2. Wählen Sie auf der Einführungsseite Create organization (Organisation erstellen) aus.
3. Wählen Sie im Bestätigungsdialogfeld Organisation erstellen.

> **Note**
>
> Standardmäßig wird die Organisation mit allen Funktionen aktiviert erstellt. Sie können auch angeben, dass für die erstellte Organisation nur Funktionen für die konsolidierte Fakturierung aktiviert sein sollen.

AWS erstellt die Organisation und zeigt Ihnen die Seite AWS-Konten. Wenn Sie sich auf einer anderen Seite befinden, wählen Sie AWS-Konten auf der linken Seite des Navigationsbereichs.

Wenn die E-Mail-Adresse des von Ihnen verwendeten Kontos noch nie von AWS verifiziert wurde, wird automatisch eine Verifizierungs-E-Mail an die Adresse gesendet, die Ihrem Verwaltungskonto zugeordnet ist. Es kann eine Verzögerung eintreten, bevor Sie die Verifizierungs-E-Mail erhalten.

4. Überprüfen Sie Ihre E-Mail-Adresse innerhalb von 24 Stunden. Weitere Informationen finden Sie unter Verifizierung der E-Mail-Adresse.

Sie haben nun eine Organisation mit Ihrem Konto als einziges Mitglied. Dies ist das Verwaltungskonto der Organisation.

Einladen eines vorhandenen Kontos zum Beitritt Ihrer Organisation

Nachdem Sie eine Organisation erstellt haben, können Sie Konten hinzufügen. In den Schritten dieses Abschnitts laden Sie ein vorhandenes Konto zum Beitritt zu Ihrer Organisation als Mitglied ein.

AWS Management Console

Einladen eines vorhandenen Kontos zum Beitritt

1. Navigieren Sie zu AWS-Konten und wählen Sie Hinzufügen eines AWS-Konto aus.
2. Wählen Sie auf der Seite Hinzufügen eines AWS-Kontos die Option Einladen eines vorhandenen AWS-Kontos aus.
3. Geben Sie in das Feld E-Mail-Adresse oder Konto-ID eines AWS-Konto einladen die E-Mail-Adresse des Kontoinhabers ein, den Sie einladen möchten, z. B. **`member222@example.com`**. Alternativ können Sie, wenn Sie die AWS-Konto-ID-Nummer kennen, diese stattdessen eingeben.
4. Geben Sie den gewünschten Text in das Feld In die Einladungs-E-Mail-Nachricht einzuschließende Nachricht ein. Dieser Text ist in der E-Mail enthalten, die an den Kontoinhaber gesendet wird.
5. Klicken Sie auf Einladung senden. AWS Organizations sendet die Einladung an den Kontoinhaber.

> **Important**
>
> Erweitern Sie die Fehlermeldung, falls angegeben. Wenn der Fehler darauf hinweist, dass Sie Ihr Kontolimit für die Organisation überschritten haben oder dass Sie kein Konto hinzufügen können, weil Ihre Organisation noch initialisiert wird, warten Sie eine Stunde nach Erstellung der Organisation und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an den AWS-Support.

6. Im Rahmen dieser praktischen Anleitung müssen Sie nun Ihre eigene Einladung annehmen. Führen Sie einen der folgenden Schritte aus, um die Seite Invitations in der Konsole aufzurufen:

   - Öffnen Sie die E-Mail, die von AWS vom Verwaltungskonto gesendet wurde, und wählen Sie den Link zur Annahme der Einladung. Wenn Sie dazu aufgefordert werden, melden Sie sich als Administrator am eingeladenen Mitgliedskonto an.
   - Öffnen Sie die AWS Organizations-Konsole und navigieren Sie zur Seite Einladungen.

7. Wählen Sie auf der Seite AWS-Konten Annehmen und danach Bestätigen.

> **Tip**
>
> Der Eingang der Einladung kann sich verzögern und Sie müssen möglicherweise warten, bis Sie die Einladung annehmen können.

8. Melden Sie sich von Ihrem Mitgliedskonto ab, und melden Sie sich als Administrator an Ihrem Verwaltungskonto an.

Erstellen eines Mitgliedskontos

In den Schritten in diesem Abschnitt erstellen Sie ein AWS-Konto, das automatisch ein Mitglied der Organisation ist. In diesem Tutorial bezeichnen wir dieses Konto als 333333333333.

AWS Management Console

Erstellen eines Mitgliedskontos

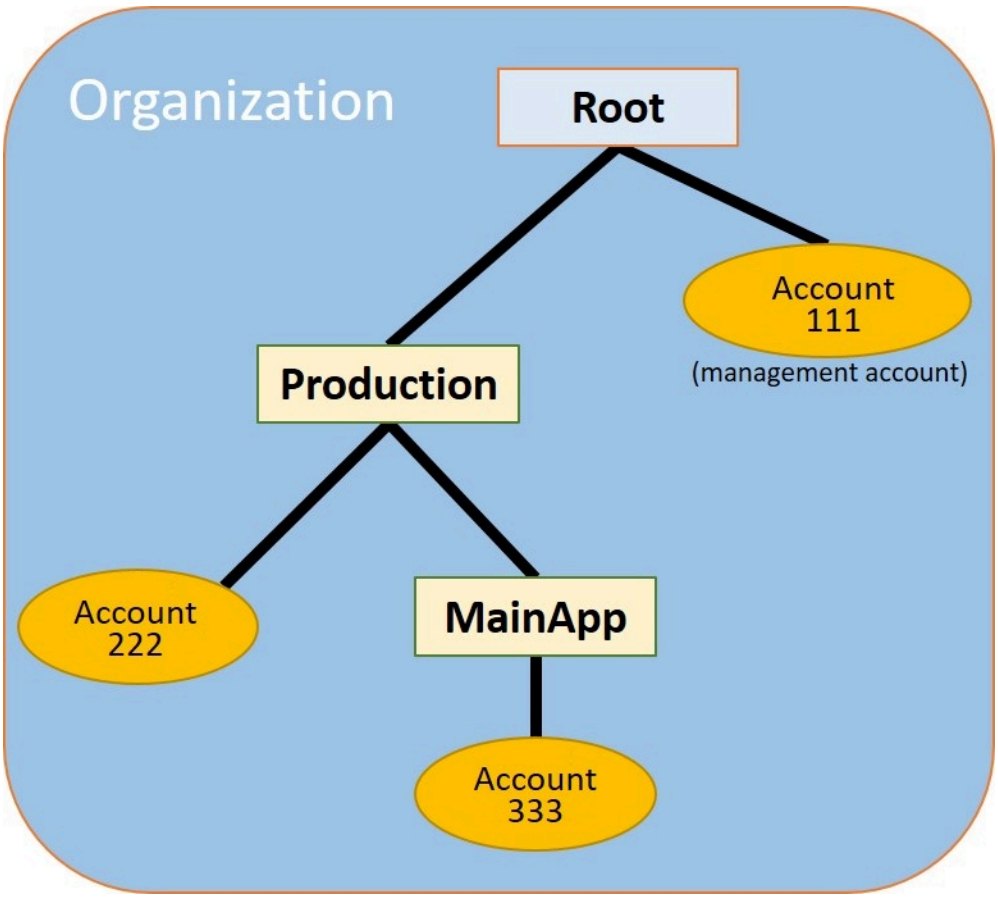
1. Klicken Sie auf der AWS Organizations-Konsole auf die Seite AWS-Konten und wählen Sie dann AWS-Konto hinzufügen aus.

2. Wählen Sie auf der Seite Hinzufügen eines AWS-Konto Erstellen eines AWS-Konto aus.
3. Geben Sie unter AWS-Konto-Name) einen Namen für das Konto ein, z. B. **`MainApp Account`**.
4. Geben Sie unter E-Mail des Stammbenutzerkontos die E-Mail-Adresse der Person ein, die Mitteilungen zu diesem Konto erhalten soll. Dieser Wert muss global eindeutig sein. Zwei Konten können nicht dieselbe E-Mail-Adresse haben. Sie können beispielsweise etwas verwenden wie: **`mainapp@example.com`**.
5. Für IAM role name (IAM-Rollenname) können Sie das Feld leer lassen und automatisch den Standardrollenamen `OrganizationAccountAccessRole` verwenden oder Ihren eigenen Namen angeben. Mit dieser Rolle können Sie auf das neue Mitgliedskonto zugreifen, wenn Sie am Verwaltungskonto als IAM-Benutzer angemeldet sind. Lassen Sie das Feld im Rahmen dieser Anleitung leer, um AWS Organizations anzuweisen, die Rolle mit dem Standardnamen zu erstellen.
6. Wählen Sie Create (Erstellen)AWS-Konto aus. Möglicherweise müssen Sie kurz warten und die Seite aktualisieren, damit das neue Konto auf der Seite AWS-Konten angezeigt wird.

> **Important**
>
> Wenn Sie einen Fehler erhalten, der darauf hinweist, dass Sie Ihr Kontolimit für die Organisation überschritten haben oder dass Sie kein Konto hinzufügen können, weil Ihre Organisation noch initialisiert wird, warten Sie eine Stunde nach Erstellung der Organisation und versuchen Sie es erneut. Wenn das Problem weiterhin besteht, wenden Sie sich bitte an den AWS-Support.

Schritt 2: Erstellen der Organisationseinheiten

In den Schritten in diesem Abschnitt erstellen Sie Organisationseinheiten und platzieren Ihre Mitgliedskonten in diese Einheiten. Sie erhalten am Ende eine Hierarchie, wie in der folgenden Abbildung dargestellt. Das Verwaltungskonto bleibt im Stamm. Ein Mitgliedskonto wird in die Produktionsorganisationseinheit und das andere Mitgliedskonto in die MainApp-Organisationseinheit verschoben, die der Produktion untergeordnet ist.



AWS Management Console

Erstellen und Auffüllen der Organisationseinheiten

> **Note**
>
> In den folgenden Schritten interagieren Sie mit Objekten, für die Sie entweder den Namen des Objekts selbst oder das Optionsfeld neben dem Objekt auswählen können.
>
> - Wenn Sie den Namen des Objekts auswählen, öffnen Sie eine neue Seite, auf der die Objektdetails angezeigt werden.
> - Wenn Sie das Optionsfeld neben dem Objekt auswählen, identifizieren Sie das Objekt, auf das eine andere Aktion angewendet werden soll, z. B. eine Menüoption.
>
> Die folgenden Schritte haben Sie das Optionsfeld zu wählen, so dass Sie dann auf das zugeordnete Objekt reagieren können, indem Sie Menüoptionen vornehmen.

1. Navigieren Sie in der AWS Organizations-Konsole zur Seite AWS-Konten.
2. Aktivieren Sie das
   
   -Kontrollkästchen neben dem Stamm-Container.
3. Wählen Sie auf der Registerkarte untergeordnet die Option Aktionen aus, und wählen Sie dann unter Organisationseinheit die Option Neu erstellen aus.
4. Geben Sie auf der Seite Organisationseinheit im Stamm erstellen für den Namen der Organisationseinheit **`Production`** ein und wählen Sie dann Organisationseinheit erstellen.
5. Aktivieren Sie das Kontrollkästchen
   
   neben der neuen Produktions-OU.
6. Wählen Sie Aktionen und dann unter Organisationseinheit die Option Neu erstellen aus.
7. Geben Sie auf der Seite Organisationseinheit in Produktion erstellen für den Namen der zweiten Organisationseinheit **`MainApp`** ein und wählen Sie dann Organisationseinheit erstellen.

   Nun können Sie Ihre Mitgliedskonten in diese Organisationseinheiten verschieben.
8. Kehren Sie zur Seite AWS-Konten zurück, und erweitern Sie dann den Baum unter Ihrer Produktions-OU, indem Sie das Dreieck
   
   daneben auswählen. Dies zeigt die MainApp-OU als untergeordnetes Element von Produktion an.
9. Aktivieren Sie neben 333333333333 das Kontrollkästchen
   
   (nicht seinen Namen), wählen Sie Aktionen und dann unter AWS-Konto die Option Verschieben.
10. Wählen Sie auf der Seite AWS-Konto „333333333333“ verschieben das Dreieck neben Produktion aus, um es zu erweitern. Wählen Sie neben MainApp das Optionsfeld
    
    (nicht seinen Namen) und dann AWS-Konto verschieben aus.
11. Aktivieren Sie neben 222222222222 das Kontrollkästchen
    
    (nicht seinen Namen), wählen Sie Aktionen und dann unter AWS-Konto die Option Verschieben aus.

12. Wählen Sie auf der Seite AWS-Konto „222222222222“ verschieben neben Produktion das Optionsfeld (nicht seinen Namen) und dann AWS-Konto verschieben aus.

Schritt 3: Erstellen von Service-Kontrollrichtlinien

In den folgenden Schritten erstellen Sie drei Service-Kontrollrichtlinien (SCPs) und hängen sie an den Stamm und die Organisationseinheiten an, um die Aktionen zu beschränken, die Benutzer in den Konten der Organisation ausführen können. Die erste SCP verhindert, dass ein Benutzer in einem der Mitgliedskonten AWS CloudTrail-Protokolle erstellt oder von Ihnen konfigurierte Protokolle ändert. Das Verwaltungskonto wird von keiner SCP beeinflusst. Nachdem Sie die CloudTrail-SCP angewendet haben, müssen Sie Protokolle vom Verwaltungskonto aus erstellen.

Aktivieren des Service-Kontrollrichtlinientyps für die Organisation

Bevor Sie einen Richtlinientyp an einen Root oder eine beliebige Organisationseinheit innerhalb des Roots anfügen können, müssen Sie den Richtlinientyp für die Organisation aktualisieren. Richtlinientypen sind nicht standardmäßig aktiviert. In diesem Abschnitt erfahren Sie, wie Sie den Service-Kontrollrichtlinientyp (SCP) in Ihrer Organisation aktivieren.

AWS Management Console

So aktivieren Sie SCPs für Ihre Organisation

1. Navigieren Sie zu Richtlinien und wählen Sie dann Service-Kontrollrichtlinien aus.
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien Aktivieren von Service-Kontrollrichtlinien aus.

   Es wird ein grünes Banner angezeigt, das Sie darüber informiert, dass Sie jetzt SCPs in Ihrer Organisation erstellen können.

Erstellen Sie SCPs

Nachdem Servicesteuerungsrichtlinien in Ihrer Organisation aktiviert sind, können Sie die drei Richtlinien erstellen, die Sie für dieses Lernprogramm benötigen.

AWS Management Console

Erstellen der ersten SCP, die CloudTrail-Konfigurationsaktionen blockiert

1. Navigieren Sie zu Richtlinien und wählen Sie dann Service-Kontrollrichtlinien aus.
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus.
3. Geben Sie unter Policy name (Richtlinienname) **`Block CloudTrail Configuration Actions`** ein.
4. Wählen Sie im Abschnitt Richtlinie in der Liste der Services auf der linken Seite CloudTrail als den Service aus. Wählen Sie die folgenden Aktionen: AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging und UpdateTrail.
5. Wählen Sie ebenfalls im rechten Bereich Ressource hinzufügen und geben Sie CloudTrail und Alle Ressourcen an. Wählen Sie dann Add resource (Ressource hinzufügen).

   Die Richtlinienanweisung auf der linken Seite sollte in etwa wie folgt aussehen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Wählen Sie Create Policy (Richtlinie erstellen) aus.

Die zweite Richtlinie definiert eine Whitelist aller Services und Aktionen, die Sie für Benutzer und Rollen in der Produktionsorganisationseinheit aktivieren möchten. Wenn Sie fertig sind, können Benutzer in der Organisationseinheit "Production" nur auf die die aufgelisteten Services und Aktionen zugreifen.

AWS Management Console

So erstellen Sie die zweiten Richtlinie zur Aufnahme von genehmigten Services in die Whitelist für die Produktionsorganisationseinheit

1. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus.
2. Geben Sie unter Policy name (Richtlinienname) **`Allow List for All Approved Services`** ein.
3. Positionieren Sie den Cursor im rechten Bereich des Abschnitts Policy (Richtlinie) und fügen Sie eine Richtlinie wie die folgende ein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Wählen Sie Create Policy (Richtlinie erstellen) aus.

Die endgültige Richtlinie bietet eine Sperrliste der Services, die von der Nutzung in der MainApp-Organisationseinheit blockiert sind. Im Rahmen dieser praktischen Anleitung blockieren Sie den Zugriff auf Amazon DynamoDB in allen Konten, die in der MainApp-Organisationseinheit enthalten sind.

AWS Management Console

So erstellen Sie die dritte Richtlinie, die Services sperrt, die in der MainApp-Organisationseinheit nicht verwendet werden können

1. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus.
2. Geben Sie unter Policy name (Richtlinienname) **`Deny List for MainApp Prohibited Services`** ein.
3. Wählen Sie im Abschnitt Policy (Richtlinie) auf der linken Seite Amazon DynamoDB für den Service aus. Wählen Sie für die Aktion All actions (Alle Aktionen) aus.
4. Wählen Sie ebenfalls auf der linken Seite Ressource hinzufügen und geben Sie DynamoDB und Alle Ressourcen an. Wählen Sie dann Add resource (Ressource hinzufügen).

   Die Richtlinienanweisung auf der rechten Seite wird aktualisiert und sieht in etwa wie folgt aus.

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

5. Wählen Sie Create Policy (Richtlinie erstellen), um die SCP zu speichern.

Anfügen der SCPs an Ihre Organisationseinheiten

Nachdem die Service-Kontrollrichtlinien erstellt und für Ihren Root-Benutzer aktiviert sind, können Sie sie an den Root-Benutzer und die Organisationseinheiten anfügen.

AWS Management Console

Anfügen der Richtlinien an den Root und die Organisationseinheiten

1. Navigieren Sie zur Seite AWS-Konten.

2. Wählen Sie auf der Seite AWS-Konten Stamm (seinen Namen, nicht das Optionsfeld) aus, um zur Detailseite zu navigieren.
3. Wählen Sie auf der Seite Stamm-Details die Registerkarte Richtlinien aus, und wählen Sie dann unter Service-Kontrollrichtlinien die Option Anfügen aus.
4. Wählen Sie auf der Seite Service-Kontrollrichtlinie anfügen das Optionsfeld neben dem SCP mit dem Namen `Block CloudTrail Configuration Actions` aus und wählen Sie dann Anfügen aus. In dieser Anleitung hängen Sie die SCP an den Root an, sodass sie sich auf alle Mitgliedskonten auswirkt, um zu verhindern, dass Sie CloudTrail konfiguriert haben.

   Auf der Seite Stamm-Details auf der Registerkarte Richtlinien wird nun angezeigt, dass zwei SCPs mit dem Stamm verbunden sind: der gerade angehängte und der Standard-`FullAWSAccess`-SCP.
5. Navigieren Sie zurück zur Seite AWS-Konten und wählen Sie die Produktions-OU (der Name, nicht das Optionsfeld), um zur Detailseite zu navigieren.
6. Wählen Sie auf der Detailseite der Produktions-OU die Registerkarte Richtlinien aus.
7. Wählen Sie unter Service-Kontrollrichtlinien die Option Anfügen aus.
8. Wählen Sie auf der Seite Service-Kontrollrichtlinie anfügen das Optionsfeld neben `Allow List for All Approved Services` aus und wählen Sie dann Anfügen aus. Dadurch können Benutzer oder Rollen in Mitgliedskonten in der Produktionsorganisationseinheit auf die genehmigten Services zugreifen.
9. Wählen Sie erneut die Registerkarte Richtlinien, um zu sehen, dass zwei SCPs an die OU angehängt sind: der gerade angehängte und der Standard-`FullAWSAccess`-SCP. Da die `FullAWSAccess`-SCP jedoch auch eine Whitelist ist, mit der alle Services und Aktionen freigegeben werden, müssen Sie jetzt die Zuweisung dieser SCP aufheben, um sicherzustellen, dass nur Ihre genehmigten Services zulässig sind.
10. Um die Standardrichtlinie aus der Produktions-OU zu entfernen, wählen Sie das Optionsfeld für FullAWSAccess, wählen Sie Trennen und wählen Sie dann im Bestätigungsdialogfeld Richtlinie trennen.

    Nachdem Sie die Standardrichtlinie entfernt haben, verlieren alle der Produktions-OU untergeordneten Mitgliedskonten den Zugriff auf sämtliche Aktionen und Services, die nicht in der im vorherigen Schritt zugewiesenen Whitelist-SCP enthalten sind. Alle Anforderungen zur Verwendung von Aktionen, die nicht in der Allow List for All Approved Services (Whitelist für alle zugelassenen Services) enthalten sind, werden verweigert. Dies gilt auch dann, wenn

ein Administrator in einem Konto Zugriff auf einen anderen Service gewährt, indem er einem Benutzer in einem der Mitgliedskonten eine IAM-Berechtigungsrichtlinie zuweist.

11. Sie können jetzt die SCP namens `Deny List for MainApp Prohibited services` anhängen, um zu verhindern, dass ein Benutzer in den Konten der MainApp-Organisationseinheit einen der nicht genehmigten Services verwendet.

    Navigieren Sie dazu zur Seite AWS-Konten, wählen Sie das Dreiecksymbol, um den Zweig der Produktions-OU zu erweitern und wählen Sie dann die MainApp-OU (ihren Namen, nicht das Optionsfeld), um zu ihrem Inhalt zu navigieren.
12. Wählen Sie auf der MainApp-Detailseite die Registerkarte Richtlinien.
13. Wählen Sie unter Service-Kontrollrichtlinien die Option Anfügen und wählen Sie dann in der Liste der verfügbaren Richtlinien das Optionsfeld neben Zugriffsverweigerungsliste für verbotene MainApp-Services und wählen Sie dann Richtlinie anfügen.

Schritt 4: Testen der Organisationsrichtlinien

Sie können sich jetzt als Benutzer bei einem der Mitgliedskonten anmelden und versuchen, verschiedene AWS-Aktionen auszuführen:

- Wenn Sie sich als Benutzer am Verwaltungskonto anmelden, können Sie jede Operation ausführen, die Ihre IAM-Berechtigungsrichtlinien zulassen. Die Service-Kontrollrichtlinien wirken sich nicht auf Benutzer oder Rollen im Verwaltungskonto aus, egal in welchem Stamm-Benutzer oder welcher Organisationseinheit sich das Konto befindet.
- Wenn Sie sich als Benutzer beim Konto „222222222222“ anmelden, können Sie sämtliche Aktionen ausführen, die laut Whitelist zulässig sind. AWS Organizations lehnt jede Aktion in allen Services ab, die nicht in der Whitelist enthalten sind. Außerdem lehnt AWS Organizations jeden Versuch ab, eine der CloudTrail-Konfigurationsaktionen auszuführen.
- Wenn Sie sich als ein Benutzer in Konto „333333333333“ anmelden, können Sie sämtliche Aktionen ausführen, die laut Whitelist zulässig und laut Sperrliste nicht blockiert sind. AWS Organizations lehnt jede Aktion ab, die nicht in der Whitelist-Richtlinie enthalten ist, sowie jede Aktion, die in der Sperrlistenrichtlinie aufgeführt ist. Außerdem lehnt AWS Organizations jeden Versuch ab, eine der CloudTrail-Konfigurationsaktionen auszuführen.

Tutorial: Überwachen wichtiger Änderungen an Ihrer Organisation mit Amazon EventBridge

In diesem Tutorial wird gezeigt, wie Amazon EventBridge, früher Amazon CloudWatch Events, zur Überwachung der Änderungen an Ihrer Organisation konfiguriert wird. Konfigurieren Sie zunächst eine Regel, die ausgelöst wird, wenn Benutzer bestimmte AWS Organizations-Operationen aufrufen. Dann konfigurieren Sie Amazon EventBridge so, dass beim Auslösen der Regel eine AWS Lambda-Funktion ausgeführt wird. Zudem konfigurieren Sie Amazon SNS so, dass eine E-Mail mit Details zum Ereignis versendet wird.

Die folgende Abbildung zeigt die wichtigsten Schritte der praktischen Anleitung.

[Schritt 1: Konfigurieren einer Trail- und Ereignisauswahl](#)

Erstellen Sie ein Protokoll namens in Trail in AWS CloudTrail. Es wird auf die Erfassung aller API-Aufrufe konfiguriert.

[Schritt 2: Konfigurieren einer Lambda-Funktion](#)

Erstellen Sie eine AWS Lambda-Funktion, die Details über das Ereignis in einem S3 Bucket protokolliert.

[Schritt 3: Erstellen Sie ein Amazon-SNS-Thema, das E-Mails an Abonnenten sendet](#)

Erstellen Sie ein Amazon-SNS-Thema, das E-Mails an Abonnenten sendet und abonnieren Sie das Thema selbst.

[Schritt 4: Erstellen einer Amazon-EventBridge-Regel](#)

Erstellen Sie eine Regel, die Amazon EventBridge anweist, Details zu bestimmten API-Aufrufen an die Lambda-Funktion und die SNS-Themaabonnenten weiterzuleiten.

Schritt 5: Testen Ihrer Amazon-EventBridge-Regel

Testen Sie die neue Regel, indem Sie eine der überwachten Operationen ausführen. In diesem Tutorial erstellt die überwachte Operation eine Organisationseinheit (OU). Sie zeigen den Protokolleintrag an, den die Lambda-Funktion erstellt, und Sie zeigen die E-Mail an, die von Amazon SNS an Abonnenten gesendet wird.

> **Tipp**
>
> Außerdem können Sie dieses Tutorial als Leitfaden beim Konfigurieren ähnlicher Operationen verwenden, wie z. B. das Senden von E-Mail-Benachrichtigungen, wenn die Kontoerstellung abgeschlossen ist. Da die Erstellung eines Kontos eine asynchrone Operation ist, werden Sie standardmäßig nicht benachrichtigt, wenn sie abgeschlossen ist. Weitere Informationen zur Verwendung von AWS CloudTrail und Amazon EventBridge mit AWS Organizations finden Sie unter Protokollieren und Überwachen in AWS Organizations.

Voraussetzungen

In diesem Tutorial wird von Folgendem ausgegangen:

- Sie können sich in der AWS Management Console als IAM-Benutzer des Verwaltungskontos in Ihrer Organisation anmelden. Der IAM-Benutzer muss über Berechtigungen zum Erstellen und Konfigurieren eines Protokolls in CloudTrail, einer Funktion in Lambda, eines Themas in Amazon SNS und einer Regel in Amazon EventBridge verfügen. Weitere Informationen zum Erteilen von Berechtigungen finden Sie unter Access Management im IAM-Benutzerhandbuch oder im Leitfaden für den Service, für den Sie den Zugriff konfigurieren möchten.
- Sie haben Zugriff auf einen vorhandenen Amazon-S3-Bucket (Amazon Simple Storage Service) (oder verfügen über die Berechtigung zum Erstellen eines Buckets), um das im ersten Schritt erstellte CloudTrail-Protokoll zu erhalten.

> **Important**
>
> Derzeit wird AWS Organizations nur in der Region USA Ost (Nord-Virginia) bereitgestellt (auch wenn es weltweit verfügbar ist). Zum Ausführen der Schritte in diesem Tutorial müssen Sie die AWS Management Console für die Verwendung dieser Region konfigurieren.

Schritt 1: Konfigurieren einer Trail- und Ereignisauswahl

In diesem Schritt melden Sie sich am Verwaltungskonto an und konfigurieren ein Protokoll (namens Trail) in AWS CloudTrail. Außerdem konfigurieren Sie eine Ereignisauswahl auf dem Trail, um alle Lese-/Schreib-API-Aufrufe aufzuzeichnen, damit Amazon EventBridge über Aufrufe als Auslöser verfügt.

Sie erstellen einen Trail wie folgt:

1. Melden Sie sich bei AWS als Administrator des Verwaltungskontos der Organisation an und öffnen Sie die CloudTrail-Konsole unter https://console.aws.amazon.com/cloudtrail/.
2. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke der Konsole die Region USA Ost (Nord-Virginia) aus. Wenn Sie eine andere Region auswählen, wird AWS Organizations nicht als Option in den Amazon-EventBridge-Konfigurationseinstellungen angezeigt, und CloudTrail erfasst keine Informationen zu AWS Organizations.
3. Wählen Sie im Navigationsbereich Trails aus.
4. Wählen Sie Create Trail (Trail erstellen) aus.
5. Geben Sie für Trail name (Trail-Name) den Namen **`My-Test-Trail`** ein.
6. Führen Sie eine der folgenden Optionen aus, um anzugeben, wohin CloudTrail die Protokolle senden soll:

   - Wenn Sie einen Bucket erstellen müssen, wählen Sie Create a new S3 bucket (Neuen S3-Bucket erstellen) und geben Sie dann unter Trail log bucket and folder (Trail–Protokoll-Bucket und -Ordner) einen Namen für den neuen Bucket ein.

     > **Note**
     >
     > S3-Bucket-Namen müssen global eindeutig sein.

   - Wenn Sie bereits einen Bucket haben, wählen Sie Use existing S3 bucket (Vorhandenen S3-Bucket verwenden) und anschließend den Bucket-Namen aus der Liste S3 bucket (S3-Bucket).
7. Wählen Sie Weiter aus.
8. Wählen Sie auf der Seite Choose log events (Protokollereignisse auswählen) im Abschnitt Management events (Verwaltungsereignisse) die Optionen Read (Lesen) und Write (Schreiben) aus.

9. Wählen Sie Weiter aus.
10. Prüfen Sie Ihre Auswahlen und wählen Sie dann Create trail (Trail erstellen).

Mit Amazon EventBridge können Sie zwischen verschiedenen Möglichkeiten zum Senden von Warnungen wählen, wenn eine Alarmregel mit einem eingehenden API-Aufruf übereinstimmt. In diesem Tutorial werden zwei Methoden gezeigt: das Aufrufen einer Lambda-Funktion, die den API-Aufruf protokollieren kann, und das Senden von Informationen an ein Amazon-SNS-Thema, das eine E-Mail oder Textnachricht an die Abonnenten des Themas sendet. In den nächsten zwei Schritten erstellen Sie die erforderlichen Komponenten: die Lambda-Funktion und das Amazon-SNS-Thema.

Schritt 2: Konfigurieren einer Lambda-Funktion

In diesem Schritt erstellen Sie eine Lambda-Funktion für die Protokollierung der API-Aktivität, die sie von der später noch zu konfigurierenden Amazon-EventBridge-Regel erhält.

So erstellen Sie eine Lambda-Funktion für die Protokollierung von Amazon–EventBridge-Ereignissen

1. Öffnen Sie die AWS Lambda-Konsole unter https://console.aws.amazon.com/lambda/.
2. Wenn Sie Lambda zum ersten Mal verwenden, wählen Sie auf der Willkommensseite Get Started Now (Erste Schritte); wählen Sie andernfalls Create function (Funktion erstellen) aus.
3. Wählen Sie auf der Seite Create function (Funktion erstellen) die Option Use a blueprint (Blueprint verwenden) aus.
4. Geben Sie im Suchfeld Blueprints den Suchbegriff **`hello`** für den Filter ein und wählen Sie den Blueprint hello-world aus.
5. Wählen Sie Konfigurieren aus.
6. Führen Sie auf der Seite Basic information (Grundlegende Informationen) folgende Schritte aus:
    a. Geben Sie für den Lambda-Funktionsnamen den Namen **`LogOrganizationEvents`** in das Textfeld Name ein.
    b. Wählen Sie unter Role (Rolle) die Option Create a new role with basic Lambda permissions (Eine neue Rolle mit den grundlegenden Lambda-Berechtigungen erstellen) aus. Diese Rolle gewährt Ihrer Lambda-Funktion die Berechtigung für den Zugriff auf die erforderlichen Daten zum Schreiben des Ausgabeprotokolls.
7. Bearbeiten Sie den Code für die Lambda-Funktion wie im folgenden Beispiel:

```
console.log('Loading function');
```

```
exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

Mit diesem Beispiel-Code wird das Ereignis mit einer **`LogOrganizationEvents`**-Markierungsfolge gefolgt von der JSON-Zeichenfolge protokolliert, die das Ereignis ausmacht.

8. Wählen Sie Create function (Funktion erstellen).

Schritt 3: Erstellen Sie ein Amazon-SNS-Thema, das E-Mails an Abonnenten sendet

In diesem Schritt erstellen Sie ein Amazon-SNS-Thema, das Informationen per E-Mail an Abonnenten sendet. Sie machen das Thema zum „Ziel“ der noch zu erstellenden Amazon-EventBridge-Regel.

So erstellen Sie ein Amazon-SNS-Thema zum Senden einer E-Mail an Abonnenten

1. Öffnen Sie die Amazon-SNS-Konsole unter https://console.aws.amazon.com/sns/v3/.
2. Wählen Sie im Navigationsbereich Topics (Themen) aus.
3. Wählen Sie Create new topic (Neues Thema erstellen).
   a. Geben Sie in das Feld Topic name (Themenname) den Namen **`OrganizationsCloudWatchTopic`**.
   b. Geben Sie unter Display name (Anzeigename) **`OrgsCWEvnt`** ein.
   c. Wählen Sie Thema erstellen aus.
4. Jetzt können Sie einen Abonnementen für das Thema erstellen. Wählen Sie die ARN für das Thema aus, das Sie soeben erstellt haben.
5. Klicken Sie auf Create subscription (Abonnement erstellen).
   a. Wählen Sie auf der Seite Create subscription unter Protocol Email aus.
   b. Geben Sie unter Endpunkt Ihre E-Mail-Adresse ein.

c. Wählen Sie Create subscription. AWS sendet eine E-Mail an die im vorherigen Schritt angegebene E-Mail-Adresse. Warten Sie, bis die E-Mail ankommt und wählen Sie dann den Link Confirm subscription darin aus, um den erfolgreichen Erhalt der E-Mail zu bestätigen.

d. Kehren Sie zur Konsole zurück und aktualisieren Sie die Seite. Die Nachricht Pending confirmation wird ausgeblendet und durch die nun gültige Abonnement-ID ersetzt.

Schritt 4: Erstellen einer Amazon-EventBridge-Regel

Nachdem die erforderliche Lambda-Funktion nun in Ihrem Konto vorhanden ist, erstellen Sie eine Amazon-EventBridge-Regel zum Aufruf dieser Funktion, wenn die Kriterien in der Regel erfüllt sind.

So erstellen Sie eine EventBridge-Regel

1. Öffnen Sie die Amazon-EventBridge-Konsole unter https://console.aws.amazon.com/events/.
2. Stellen Sie die Konsole auf die Region USA Ost (Nord-Virginia) ein, da sonst keine Informationen zu Organizations verfügbar sind. Wählen Sie in der Navigationsleiste in der oberen rechten Ecke der Konsole die Region USA Ost (Nord-Virginia) aus.
3. Weitere Informationen zum Erstellen von Amazon-EventBridge-Regeln finden Sie unter Erste Schritte mit Amazon EventBridge im Amazon-EventBridge-Benutzerhandbuch.

Schritt 5: Testen Ihrer Amazon-EventBridge-Regel

In diesem Schritt erstellen Sie eine Organisationseinheit (OU) und beobachten die Amazon-EventBridge-Regel, erstellen einen Protokolleintrag und senden sich selbst eine E-Mail mit Details zu dem Ereignis.

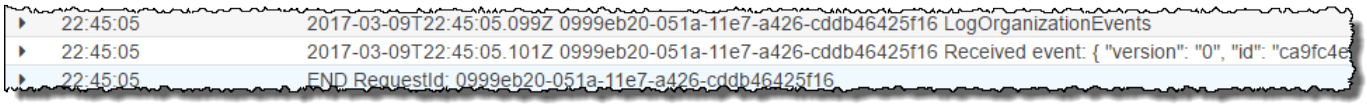
AWS Management Console

So erstellen Sie eine OU

1. Öffnen Sie die Seite AWS Organizations-Konsole auf der AWS-Konten-Seite.
2. Aktivieren Sie das Kontrollkästchen
   ☑
   Root-OU, wählen Sie Aktionen und dann unter Organisationseinheit die Option Neu erstellen.
3. Geben Sie als Namen der Organisationseinheit **`TestCWEOU`** ein und wählen Sie dann Create organizational unit (Organisationseinheit erstellen) aus.

So zeigen Sie den Protokolleintrag „EventBridge“ an

1. Öffnen Sie die CloudWatch-Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie auf der Navigationsseite Logs (Protokolle).
3. Wählen Sie auf der Seite Log Groups (Protokollgruppen) die Gruppe aus, die Ihrer -Funktion zugeordnet ist: /aws/lambda/LogOrganizationEvents.
4. Jede Gruppe enthält mindestens einen Stream. Außerdem sollte eine Gruppe für heute vorhanden sein. Wählen Sie diese aus.
5. Zeigen Sie das Protokoll an. Es sollten Zeilen angezeigt werden, die den folgenden ähneln:



6. Wählen Sie die mittlere Zeile des Eintrags aus, um den vollständigen JSON-Text des erhaltenen Ereignisses anzuzeigen. Sie können alle Details der API-Anforderung in den `requestParameters`- und `responseElements`-Teilen der Ausgabe sehen.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
```

```
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Suchen Sie in Ihrem E-Mail-Konto eine Nachricht von OrgsCWEvnt (der Anzeigename Ihres Amazon-SNS-Themas). Der E-Mail-Text enthält den gleichen JSON-Text als Ausgabe, wie der im vorherigen Schritt gezeigte Protokolleintrag.

Bereinigung: Entfernen der nicht mehr benötigten Ressourcen

Um anfallende Gebühren zu vermeiden, sollten Sie alle für dieses Tutorial erstellten AWS-Ressourcen, die Sie nicht behalten möchten, löschen.

Bereinigen Ihrer AWS-Umgebung

1. Verwenden Sie die CloudTrail-Konsole unter zum Löschen der Funktion namens **`My-Test-Trail`**, die Sie in Schritt 1 erstellt haben.
2. Wenn Sie in Schritt 1 einen Amazon-S3-Bucket erstellt haben, verwenden Sie zum Löschen die Amazon-S3-Konsole.
3. Verwenden Sie die Lambda-Konsole unter zum Löschen der Funktion namens **`LogOrganizationEvents`**, die Sie in Schritt 2 erstellt haben.
4. Verwenden Sie die Amazon-SNS-Konsole, um das Amazon-SNS-Thema mit dem Namen **`OrganizationsCloudWatchTopic`** zu löschen, das Sie in Schritt 3 erstellt haben.
5. Verwenden Sie die CloudWatch-Konsole zum Löschen der EventBridge-Regel namens **`OrgsMonitorRule`**, die Sie in Schritt 4 erstellt haben.
6. Verwenden Sie abschließnd die Organizations-Konsole zum Löschen der Organisationseinheit mit dem Namen **`TestCWEOU`**, die Sie in Schritt 5 erstellt haben.

Das war's. In diesem Tutorial haben Sie EventBridge zur Überwachung der Änderungen an Ihrer Organisation konfiguriert. Sie haben eine Regel konfiguriert, die ausgelöst wird, wenn Benutzer bestimmte AWS Organizations-Operationen aufrufen. Mit der Regel wurde eine Lambda-Funktion ausgeführt, die mit der das Ereignis protokolliert und eine E-Mail mit Details zum Ereignis gesendet wurde.

Bewährte Methoden für die Verwaltung mehrerer Konten

Befolgen Sie die folgenden Empfehlungen, die Ihnen die Einrichtung und Verwaltung einer Umgebung mit mehreren Konten in AWS Organizations erleichtern.

Themen

- Verwalten von Konten in einer einzigen Organisation
- Verwenden eines sicheren Passworts für den Root-Benutzer
- Dokumentieren der Prozesse für die Verwendung der Root-Benutzer-Anmeldeinformationen
- Aktivieren von MFA für die Anmeldedaten für Ihren Root-Benutzer
- Anwenden von Steuerelementen zur Überwachung des Zugriffs auf die Anmeldeinformationen
- Kontakt-Telefonnummer auf dem neuesten Stand halten
- Verwenden einer Gruppen-E-Mail-Adresse für Root-Konten
- Gruppieren der Workloads nach Geschäftszweck statt nach Firmenhierarchie
- Organisieren von Workloads mithilfe mehrerer Konten
- Aktivieren von AWS-Services auf Organisationsebene über die Servicekonsole oder über API/CLI-Vorgänge
- Verwenden von Abrechnungstools zur Verfolgung der Kosten und Optimierung der Ressourcennutzung
- Planen der Tagging-Strategie und Durchsetzen von Tags für alle Organisationsressourcen
- Bewährte Methoden für das Verwaltungskonto
- Bewährte Methoden für Mitgliedskonten

Verwalten von Konten in einer einzigen Organisation

Wir empfehlen, eine einzige Organisation zu erstellen und alle Konten in dieser Organisation zu verwalten. Eine Organisation stellt eine Art Sicherheitsgrenze dar, mit der Sie in allen Konten in Ihrer Umgebung für Einheitlichkeit sorgen können. Sie können zum Beispiel Richtlinien oder Service-Level-Konfigurationen zentral für alle Konten in einer Organisation anwenden. Wenn Sie einheitliche Richtlinien, zentrale Sichtbarkeit und programmgesteuerte Kontrollen in Ihrer Umgebung mit mehreren Konten aktivieren möchten, lässt sich dies am besten in einer einzigen Organisation erreichen.

Verwenden eines sicheren Passworts für den Root-Benutzer

Es empfiehlt sich, ein sicheres und eindeutiges Passwort zu verwenden. Zahlreiche Passwort-Manager sowie Algorithmen und Tools zur Erstellung sicherer Passwörter können Ihnen dabei helfen. Weitere Informationen finden Sie unter Ändern des Passworts für den Root-Benutzer des AWS-Kontos. Nutzen Sie die Informationssicherheitsrichtlinie Ihres Unternehmens, um die Langzeitspeicherung und den Zugriff auf das Passwort des Root-Benutzers zu verwalten. Es empfiehlt sich, das Passwort in einem Passwort-Manager-System oder einem gleichwertigen System zu speichern, das den Sicherheitsanforderungen Ihrer Organisation genügt. Um eine zirkuläre Abhängigkeit zu vermeiden, speichern Sie das Stammbenutzerpasswort nicht mit Tools, die von AWS-Services abhängen, bei denen Sie sich mit dem geschützten Konto anmelden. Unabhängig von der gewählten Methode sollten Sie der Ausfallsicherheit Priorität einräumen und eventuell in Erwägung ziehen, den Zugriff auf diesen Tresor für einen stärkeren Schutz zwingend von mehreren Akteuren autorisieren zu lassen. Zugriffe auf das Passwort oder dessen Speicherort sollten protokolliert und überwacht werden. Weitere Empfehlungen für Root-Benutzerpasswörter finden Sie unter Bewährte Methoden für Root-Benutzer für Ihren AWS-Konto.

Dokumentieren der Prozesse für die Verwendung der Root-Benutzer-Anmeldeinformationen

Dokumentieren Sie die Umsetzung wichtiger Prozesse während der Ausführung, damit Sie ein Protokoll der an den einzelnen Schritten beteiligten Personen haben. Zur Verwaltung des Passworts empfiehlt sich die Verwendung eines sicheren verschlüsselten Passwort-Managers. Außerdem ist es wichtig, etwaige Ausnahmen und unvorhergesehene Ereignisse zu dokumentieren. Weitere Informationen finden Sie unter Problembehandlung bei der AWS Management Console-Anmeldung im AWSAnmelde-Benutzerhandbuch und Aufgaben, für dieRoot-Benutzeranmeldedaten erforderlich sind im IAM-Benutzerhandbuch.

Testen und überprüfen Sie mindestens vierteljährlich, ob Sie weiterhin Zugriff auf den Root-Benutzer haben und ob die Kontakt-Telefonnummer funktioniert. Damit können Sie dem Unternehmen versichern, dass der Prozess funktioniert und dass Sie den Zugriff auf den Root-Benutzer aufrechterhalten können. Außerdem wird damit gezeigt, dass die für den Root-Zugriff verantwortlichen Personen die Schritte verstehen, die sie ausführen müssen, damit der Prozess erfolgreich ist. Um die Reaktionszeit zu verkürzen und erfolgreicher zu sein, müssen Sie sicherstellen, dass alle an einem Prozess beteiligten Personen genau wissen, was sie zu tun haben, falls Zugriff erforderlich ist.

Aktivieren von MFA für die Anmeldedaten für Ihren Root-Benutzer

Es empfiehlt sich, mehrere MFA-Geräte (Multi-Faktor-Authentifizierung) für den Root-Benutzer des AWS-Konto und die IAM-Benutzer in Ihren AWS-Konten zu aktivieren. Damit können Sie die Sicherheitsstandards in Ihren AWS-Konten erhöhen und die Verwaltung des Zugriffs auf hochprivilegierte Benutzer wie den Root-Benutzer des AWS-Konto vereinfachen. Um den unterschiedlichen Kundenanforderungen gerecht zu werden, werden drei Arten von MFA-Geräten für IAM von AWS unterstützt, darunter FIDO-Sicherheitsschlüssel, virtuelle Authenticator (Anwendungen) und TOTP-Hardwaretoken (Time-based One-Time Password, zeitgesteuertes Einmalpasswort).

Jeder Authenticator-Typ hat etwas unterschiedliche physische und sicherheitstechnische Eigenschaften, die für verschiedene Anwendungsfälle unterschiedlich gut geeignet sind. FIDO2-Sicherheitsschlüssel bieten ein Höchstmaß an Sicherheit und sind resistent gegenüber Phishing-Angriffen. Jede Form von MFA bietet wesentlich mehr Sicherheit als die reine Passwortauthentifizierung. Daher empfiehlt es sich dringend, Ihrem Konto eine Form von MFA hinzuzufügen. Wählen Sie den Gerätetyp aus, der Ihren Sicherheits- und Betriebsanforderungen am besten entgegenkommt.

Wenn Sie ein batteriebetriebenes Gerät als primären Authenticator wählen, z. B. ein TOTP-Hardwaretoken, sollten Sie in Erwägung ziehen, als Backup-Mechanismus außerdem einen Authenticator zu registrieren, der nicht mit einer Batterie betrieben wird. Die regelmäßige Überprüfung der Funktionsfähigkeit des Geräts und sein Austausch vor dem Ablaufdatum sind ebenfalls unerlässlich, um einen ununterbrochenen Zugriff zu gewährleisten. Unabhängig davon, für welchen Gerätetyp Sie sich entscheiden, sollten Sie mindestens zwei Geräte registrieren (IAM unterstützt bis zu acht MFA-Geräte pro Benutzer), um die Ausfallsicherheit bei Geräteverlust oder -ausfall zu erhöhen.

Befolgen Sie zur Aufbewahrung des MFA-Geräts die Informationssicherheitsrichtlinie Ihrer Organisation. Es empfiehlt sich, das MFA-Gerät getrennt vom zugehörigen Passwort aufzubewahren. Dadurch wird sichergestellt, dass für den Zugriff auf das Passwort und das MFA-Gerät unterschiedliche Ressourcen (Personen, Daten und Tools) erforderlich sind. Diese Trennung sorgt für ein zusätzliches Maß an Schutz vor unbefugtem Zugriff. Außerdem empfiehlt es sich, Zugriffe auf das MFA-Gerät oder seinen Aufbewahrungsort zu protokollieren und zu überwachen. Dies hilft, unbefugte Zugriffe zu erkennen und darauf zu reagieren.

Weitere Informationen finden Sie unter Absichern Ihrer Root-Benutzer-Anmeldedaten mit der Multi-Faktor-Authentifizierung (MFA) im IAM-Benutzerhandbuch. Anleitungen zur Aktivierung von MFA

finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS und Aktivieren von MFA-Geräten für Benutzer in AWS.

Anwenden von Steuerelementen zur Überwachung des Zugriffs auf die Anmeldeinformationen

Der Zugriff auf die Anmeldeinformationen des Stammbenutzers sollte ein seltenes Ereignis sein. Erstellen Sie Warnungen mit Tools wie Amazon EventBridge, um die Anmeldung und Verwendung der Anmeldeinformationen des Root-Benutzers für das Verwaltungskonto anzukündigen. Diese Warnung sollte u. a. die E-Mail-Adresse umfassen, die für den Root-Benutzer selbst verwendet wird. Sie sollte eindringlich und nicht zu übersehen sein. Ein Beispiel finden Sie unter Überwachen und Benachrichtigen von AWS-Konto-Stammbenutzeraktivitäten. Vergewissern Sie sich, dass die Mitarbeiter, die eine solche Warnung erhalten, wissen, wie sie überprüfen können, ob der Root-Benutzerzugriff erwartet wird, und wie sie den Vorfall melden können, wenn es sich ihrer Meinung nach um einen Sicherheitsvorfall handelt. Weitere Informationen finden Sie unter Verdächtige E-Mails melden oder Meldung von Schwachstellen. Alternativ können Sie sich an AWS wenden, um Unterstützung und zusätzliche Hilfestellung zu erhalten.

Kontakt-Telefonnummer auf dem neuesten Stand halten

Für die Wiederherstellung des Zugriffs auf Ihr AWS-Konto müssen Sie über eine gültige und aktive Kontakt-Telefonnummer verfügen, über die Sie Textnachrichten oder Anrufe empfangen können. Es empfiehlt sich die Nutzung einer speziellen Telefonnummer, damit AWS Sie für Kontosupport und Wiederherstellungszwecke auf jeden Fall erreichen kann. Die Telefonnummern Ihres Kontos können Sie über die AWS Management Console oder über Kontoverwaltungs-APIs problemlos einsehen und verwalten.

Es gibt verschiedene Möglichkeiten, eine spezielle Telefonnummer zu erlangen, über die AWS Sie kontaktieren kann. Wir empfehlen Ihnen dringend, sich eine spezielle SIM-Karte und ein spezielles Mobiltelefon zu besorgen. Bewahren Sie das Telefon und die SIM-Karte sicher und dauerhaft auf, damit die Telefonnummer für die Kontowiederherstellung verfügbar bleibt. Erklären Sie außerdem dem für die Handyrechnung zuständigen Team, wie wichtig diese Telefonnummer ist, selbst wenn sie für längere Zeit inaktiv bleibt. Um zusätzlichen Schutz zu gewährleisten, sollte diese Telefonnummer in Ihrer Organisation unbedingt vertraulich behandelt werden.

Halten Sie die Telefonnummer auf der Seite „Kontaktinformationen“ der AWS-Konsole fest und geben Sie die Details an die jeweiligen Teams in Ihrer Organisation weiter, die davon Kenntnis

haben müssen. Auf diese Weise lässt sich das Risiko minimieren, das mit der Übertragung der Telefonnummer auf eine andere SIM-Karte verbunden ist. Lagern Sie das Telefon gemäß Ihrer bestehenden Informationssicherheitsrichtlinie. Lagern Sie das Telefon jedoch nicht am selben Ort wie die anderen zugehörigen Anmeldeinformationen. Zugriffe auf das Telefon oder dessen Aufbewahrungsort sollten protokolliert und überwacht werden. Für den Fall, dass sich die mit einem Konto verknüpfte Telefonnummer ändert, sollten Sie Prozesse zu ihrer Aktualisierung in der vorhandenen Dokumentation implementieren.

Verwenden einer Gruppen-E-Mail-Adresse für Root-Konten

Verwenden Sie eine E-Mail-Adresse, die von Ihrem Unternehmen verwaltet wird. Nutzen Sie eine E-Mail-Adresse, über die empfangene Nachrichten direkt an eine Gruppe von Benutzern weitergeleitet werden. Für den Fall, dass AWS den Besitzer des Kontos kontaktieren muss, um beispielsweise den Zugriff zu bestätigen, wird die E-Mail-Nachricht an mehrere Parteien gesendet. Dieser Ansatz hilft, das Risiko von Verzögerungen bei der Reaktion zu reduzieren, auch wenn Personen im Urlaub sind, krank sind oder das Geschäft verlassen.

Gruppieren der Workloads nach Geschäftszweck statt nach Firmenhierarchie

Es empfiehlt sich, die Umgebungen und Daten von Produktions-Workloads unter Ihren Workload-orientierten Organisationseinheiten der obersten Ebene zu isolieren. Die Organisationseinheiten sollten auf gemeinsamen Kontrollen basieren, anstatt nur die Hierarchie Ihres Unternehmens widerzuspiegeln. Neben den Organisationseinheiten für die Produktion sollten Sie mindestens eine Organisationseinheit definieren, die nicht für die Produktion bestimmt ist und Konten und Workload-Umgebungen enthält, mit deren Hilfe Workloads entwickelt und getestet werden. Weitere Hilfestellung finden Sie unter Organisieren von Workload-orientierten Organisationseinheiten.

Organisieren von Workloads mithilfe mehrerer Konten

Ein AWS-Konto bietet natürliche Grenzen, was die Sicherheit, den Zugriff und die Abrechnungen für Ihre AWS-Ressourcen betrifft. Die Verwendung mehrerer Konten bietet Vorteile, da Kontokontingente und Limits für API-Anforderungsraten verteilt werden können. Weitere Vorteile sind hier aufgeführt. Es empfiehlt sich, eine Reihe von organisationsweiten Basiskonten zu verwenden, z. B. Konten für Sicherheit, Protokollierung und Infrastruktur. Bei Workload-Konten sollten Sie Produktions-Workloads von Test-/Entwicklungs-Workloads in separaten Konten trennen.

Aktivieren von AWS-Services auf Organisationsebene über die Servicekonsole oder über API/CLI-Vorgänge

Als bewährte Methode sollten Sie Services, die Sie in AWS Organizations integrieren möchten, über die Konsole des jeweiligen Service oder über entsprechende API-Vorgänge bzw. CLI-Befehle aktivieren oder deaktivieren. So kann der AWS-Service alle erforderlichen Initialisierungsschritte für Ihre Organisation ausführen, z. B. die Erstellung von erforderlichen Ressourcen und die Bereinigung von Ressourcen bei Deaktivierung des Service. AWS Account Management ist der einzige Service, für dessen Aktivierung die Konsole von AWS Organizations oder APIs erforderlich sind. Eine Liste der Services, die in AWS Organizations integriert sind, finden Sie unter AWS Dienste, die Sie mit verwenden können AWS Organizations.

Verwenden von Abrechnungstools zur Verfolgung der Kosten und Optimierung der Ressourcennutzung

Wenn Sie eine Organisation verwalten, erhalten Sie eine konsolidierte Rechnung mit allen Kosten für die Konten in Ihrer Organisation. Für geschäftliche Benutzer, die Kostentransparenz benötigen, können Sie im Verwaltungskonto eine Rolle mit eingeschränkten Leseberechtigungen zur Überprüfung von Abrechnungen und für Kostentools einrichten. Sie können beispielsweise einen Berechtigungssatz erstellen, der Zugriff auf Abrechnungsberichte bzw. auf den AWS Cost Explorer Service (ein Tool zur Anzeige langfristiger Kostentrends) und auf Kosteneffizienz-Services wie Amazon S3 Storage Lens und AWS Compute Optimizer gewährt.

Planen der Tagging-Strategie und Durchsetzen von Tags für alle Organisationsressourcen

Wenn Ihre Konten und Workloads größer werden, können Tags ein nützliches Feature für die Kostenverfolgung, die Zugriffssteuerung und die Ressourcenorganisation sein. Hilfestellung zu Benennungsstrategien für das Tagging finden Sie unter Taggen Ihrer AWS-Ressourcen. Tags können Sie nicht nur für Ressourcen erstellen, sondern auch für den Organisations-Root, für Konten, Organisationseinheiten und Richtlinien. Weitere Informationen finden Sie unter Entwickeln einer eigenen Tagging-Strategie.

Bewährte Methoden für das Verwaltungskonto

Befolgen Sie diese Empfehlungen in AWS Organizations, um die Sicherheit des Verwaltungskontos zu schützen. Bei diesen Empfehlungen wird davon ausgegangen, dass Sie sich auch an die bewährte Methode halten, den Stammbenutzer nur für die Aufgaben zu verwenden, die ihn wirklich erfordern.

Themen

- Beschränken des Zugriffs auf das Verwaltungskonto auf bestimmte Personen
- Überprüfen und Verfolgen des Zugriffs von Personen
- Verwenden Sie das Verwaltungskonto nur für Aufgaben, die das Verwaltungskonto erfordern
- Vermeiden der Bereitstellung von Workloads im Verwaltungskonto der Organisation
- Delegieren von Aufgaben außerhalb des Verwaltungskontos zur Dezentralisierung

Beschränken des Zugriffs auf das Verwaltungskonto auf bestimmte Personen

Das Verwaltungskonto ist für alle genannten Verwaltungsaufgaben wie Kontoverwaltung, Richtlinien, Integration in andere AWS-Services, konsolidierte Abrechnungen usw. von zentraler Bedeutung. Daher sollten Sie den Zugriff auf das Verwaltungskonto auf die Admin-Benutzer beschränken, die Rechte benötigen, um Änderungen an der Organisation vornehmen zu können.

Überprüfen und Verfolgen des Zugriffs von Personen

Um sicherzustellen, dass Sie den Zugriff auf das Verwaltungskonto behalten, überprüfen Sie regelmäßig die Mitarbeiter in Ihrem Unternehmen, die Zugriff auf die E-Mail-Adresse, das Passwort, die MFA und die Telefonnummer haben, die damit verknüpft sind. Richten Sie Ihre Überprüfung an bestehenden Geschäftsabläufen aus. Fügen Sie eine monatliche oder vierteljährliche Überprüfung dieser Informationen hinzu, um sicherzustellen, dass nur die richtigen Personen Zugang haben. Stellen Sie sicher, dass der Vorgang zum Wiederherstellen oder Zurücksetzen des Zugriffs auf die Stammbenutzeranmeldeinformationen nicht von einer bestimmten Person abhängig ist. Alle Prozesse sollten die Möglichkeit berücksichtigen, dass Personen nicht verfügbar sein können.

Verwenden Sie das Verwaltungskonto nur für Aufgaben, die das Verwaltungskonto erfordern

Wir empfehlen, das Verwaltungskonto und die zugehörigen Benutzer und Rollen für Aufgaben zu verwenden, die nur über dieses Konto ausgeführt werden müssen. Speichern Sie alle AWS-Ressourcen in anderen AWS-Konten in der Organisation und halten Sie sie aus dem Verwaltungskonto heraus. Ein wichtiger Grund, Ihre Ressourcen in anderen Konten zu belassen, besteht darin, dass Servicesteuerungsrichtlinien (SCPs) von Organisationen keine Benutzer oder Rollen im Verwaltungskonto einschränken. Durch die Trennung der Ressourcen vom Verwaltungskonto können Sie außerdem die Kosten auf Ihren Rechnungen leichter nachvollziehen.

Vermeiden der Bereitstellung von Workloads im Verwaltungskonto der Organisation

Privilegierte Vorgänge können im Verwaltungskonto einer Organisation ausgeführt werden und SCPs gelten nicht für das Verwaltungskonto. Daher sollten Sie nur Cloud-Ressourcen und -Daten in das Verwaltungskonto aufnehmen, die dort verwaltet werden müssen.

Delegieren von Aufgaben außerhalb des Verwaltungskontos zur Dezentralisierung

Nach Möglichkeit sollten Aufgaben und Services außerhalb des Verwaltungskontos delegiert werden. Erteilen Sie den Teams in ihren eigenen Konten Berechtigungen zur Bewältigung der erforderlichen Aufgaben in der Organisation, sodass sie keinen Zugriff auf das Verwaltungskonto benötigen. Darüber hinaus können Sie mehrere delegierte Administratoren für Services registrieren, die diese Funktionalität unterstützen, z. B. AWS Service Catalog für die Freigabe von Software in der gesamten Organisation oder StackSets von AWS CloudFormation für die Erstellung und Bereitstellung von Stacks.

Weitere Informationen finden Sie unter Sicherheitsreferenzarchitektur und Organisieren der AWS-Umgebung mithilfe mehrerer Konten. AWS Dienste, die Sie mit verwenden können AWS Organizations enthält Vorschläge zur Registrierung von Mitgliedskonten als delegierten Administrator für verschiedene AWS-Services. Weitere Informationen zum Einrichten delegierter Administratoren finden Sie unter Aktivieren eines Kontos für einen delegierten Administrator für AWS Account Management und Delegierter Administrator für AWS Organizations.

Bewährte Methoden für Mitgliedskonten

Befolgen Sie diese Empfehlungen, um die Mitgliedskonten in Ihrer Organisation zu schützen. Bei diesen Empfehlungen wird davon ausgegangen, dass Sie sich auch an die bewährte Methode halten, den Stammbenutzer nur für die Aufgaben zu verwenden, die ihn wirklich erfordern.

Themen

- Definieren des Kontonamens und der Attribute
- Effizientes Skalieren Ihrer Umgebung und Kontonutzung
- Verwenden Sie einen SCP, um einzuschränken, was der Stammbenutzer in Ihren Mitgliedskonten tun kann

Definieren des Kontonamens und der Attribute

Verwenden Sie für die Mitgliedskonten eine Benennungsstruktur und eine E-Mail-Adresse, die der Kontonutzung entsprechen. Zum Beispiel `Workloads+fooA+dev@domain.com` für `WorkloadsFooADev` oder `Workloads+fooB+dev@domain.com` für `WorkloadsFooBDev`. Wenn benutzerdefinierte Tags für Ihre Organisation definiert sind, sollten Sie diese Tags in Konten zuweisen, die die Kontonutzung, die Kostenstelle, die Umgebung und das Projekt widerspiegeln. Das erleichtert das Identifizieren und Organisieren von Konten und die Suche danach.

Effizientes Skalieren Ihrer Umgebung und Kontonutzung

Beim Skalieren sollten Sie sich vor der Erstellung neuer Konten vergewissern, dass es nicht bereits Konten für ähnliche Bedürfnisse gibt, um so unnötige Doppelkonten zu vermeiden. AWS-Konten sollten auf gängigen Zugriffsanforderungen basieren. Wenn Sie planen, die Konten wiederzuverwenden (z. B. als Sandbox-Konto oder ähnliches), sollten Sie nicht benötigte Ressourcen oder Workloads in den Konten bereinigen, die Konten jedoch für eine künftige Nutzung aufbewahren.

Beachten Sie vor dem Schließen von Konten, dass sie entsprechenden Kontingentlimits unterliegen. Weitere Informationen finden Sie unter Kontingente für AWS Organizations. Implementieren Sie nach Möglichkeit einen Bereinigungsprozess, um Konten wiederzuverwenden, anstatt sie zu schließen. So vermeiden Sie, dass Kosten für den Betrieb von Ressourcen anfallen und die CloseAccount-API-Limits erreicht werden.

Verwenden Sie einen SCP, um einzuschränken, was der Stammbenutzer in Ihren Mitgliedskonten tun kann

Es wird empfohlen, eine Service-Kontrollrichtlinie (Service Control Policy, SCP) in der Organisation zu erstellen und sie dem Stammverzeichnis der Organisation zuzuordnen, damit sie auf alle Mitgliedskonten angewendet wird. Weitere Informationen finden Sie unter Sichern von Root-Benutzer-Anmeldedaten für Ihr Organizations-Konto.

Sie können alle Root-Aktionen bis auf eine bestimmte, reine Root-Aktion ablehnen, die Sie in Ihrem Mitgliedskonto ausführen müssen. Zum Beispiel verhindert die folgende SCP, dass der Root-Benutzer in einem Mitgliedskonto API-Aufrufe des AWS-Service tätigt, mit Ausnahme von „Aktualisieren einer falsch konfigurierten S3-Bucket-Richtlinie, die allen Prinzipalen den Zugriff verweigert“ (eine der Aktionen, für die Root-Anmeldeinformationen erforderlich sind). Weitere Informationen finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }
```

```
        }

    ]
}
```

In den meisten Fällen können alle Verwaltungsaufgaben von einer IAM-Rolle (AWS Identity and Access Management) im Mitgliedskonto mit entsprechenden Administratorberechtigungen ausgeführt werden. Auf diese Rollen sollten geeignete Kontrollen angewendet werden, um Aktivitäten einzuschränken, zu protokollieren und zu überwachen.

Erstellen und Verwalten einer Organisation

Über die AWS Organizations-Konsole oder durch Ausführen eines AWS Command Line Interface-(AWS CLI)-Befehls oder der entsprechenden AWS-SDK-API-Vorgänge können Sie die folgenden Aufgaben ausführen:

- Erstellen einer Organisation. Sie können Ihre Organisation mit dem aktuellen Konto und dem entsprechenden Verwaltungskonto erstellen. Erstellen Sie Mitgliedskonten in der Organisation und laden Sie andere Konten ein, sich der Organisation anzuschließen.
- Aktivieren aller Funktionen in der Organisation. Für das Arbeiten mit AWS Organizations wird empfohlen, alle Funktionen zu aktiveren. Wenn Sie eine Organisation erstellen, haben Sie die Möglichkeit, alle Funktionen oder nur einen Teil der Funktionen für die konsolidierte Abrechnung zu aktivieren. Standardmäßig sind alle Funktionen aktiviert, auch die Funktionen für die konsolidierte Fakturierung.

  Wenn alle Funktionen aktiviert sind, können Sie die Funktionen der erweiterten Kontoverwaltung von AWS Organizations wie z. B. Service-Kontrollrichtlinien (SCPs) verwenden. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für alle Konten in Ihrer Organisation, sodass Sie sicherstellen können, dass Ihre Konten die Zugriffskontrollrichtlinien Ihrer Organisation einhalten.
- Anzeigen von Details zur Organisation. Sie können Details zu Ihrer Organisation und den Roots, Organisationseinheiten (OUs) und Konten anzeigen.
- Löschen einer Organisation. Eine nicht mehr benötigte Organisation können Sie löschen.

> **Note**
>
> In den Verfahren in diesem Abschnitt werden die Mindestberechtigungen angegeben, die für die Durchführung der Aufgaben erforderlich sind. Diese gelten in der Regel für die API oder den Zugriff auf das Befehlszeilen-Tool.
> Für die Ausführung einer Aufgabe über die Konsole können zusätzliche Berechtigungen erforderlich sein. Sie können beispielsweise allen Benutzern in der Organisation Leseberechtigungen einräumen und später für ausgewählte Benutzer weitere Berechtigungen für die Ausführung bestimmter Aufgaben hinzufügen.

Erstellen einer Organisation

Sie können eine Organisation erstellen, die mit Ihrem AWS-Konto als Verwaltungskonto startet. Wenn Sie eine Organisation erstellen, können Sie auswählen, ob die Organisation nur die Funktionen der konsolidierten Fakturierung oder alle Funktionen (empfohlen) unterstützt.

Nachdem eine Organisation erstellt wurde, können Sie ihr folgendermaßen über das Verwaltungskonto Konten hinzufügen:

- Erstellen Sie andere AWS-Konten, die Ihrer Organisation automatisch als Mitgliedskonten hinzugefügt werden.
- Nachdem Ihre E-Mail-Adresse verifiziert wurde, können Sie bestehende AWS-Konten dazu einladen, Ihrer Organisation als Mitgliedskonten beizutreten.

Erstellen einer Organisation

Sie können eine Organisation erstellen, indem Sie entweder AWS Management Console verwenden oder einen Befehl von AWS CLI oder einer der SDK-APIs verwenden.

> **Mindestberechtigungen**
>
> Um eine Organisation mit Ihrem aktuellen AWS-Konto zu erstellen, benötigen Sie folgende Berechtigungen:
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> Sie können diese Berechtigung nur auf den Serviceprinzipal `organizations.amazonaws.com` beschränken.

AWS Management Console

So erstellen Sie eine -Organisation:

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Standardmäßig wird die Organisation mit allen Funktionen aktiviert erstellt. Sie können jedoch einen der folgenden Schritte ausführen:

   - Um eine Organisation mit allen aktivierten Funktionen zu erstellen, wählen Sie auf der Einführungsseite Organisation erstellen aus.
   - Um eine Organisation nur mit konsolidierten Fakturierungsfunktionen zu erstellen, wählen Sie auf der Einführungsseite und unter Organisation erstellen die Option konsolidierte Fakturierungsfunktionen aus, und wählen Sie dann im Bestätigungsdialogfeld Organisation erstellen aus.

   Wenn Sie versehentlich die falsche Option auswählen, können Sie sofort zur Seite Einstellungen gehen und dann Organisation löschen auswählen und von vorne beginnen.

3. Die Organisation wird erstellt und die Seite AWS-Konten wird angezeigt. Das einzige vorhandene Konto ist Ihr Verwaltungskonto, das derzeit in der Stammorganisationseinheit (OU) gespeichert ist.

   Falls erforderlich, sendet Organizations automatisch eine Bestätigungs-E-Mail an die Adresse, die Ihrem Verwaltungskonto zugeordnet ist. Es kann eine Verzögerung eintreten, bevor Sie die Verifizierungs-E-Mail erhalten. Überprüfen Sie Ihre E-Mail-Adresse innerhalb von 24 Stunden. Weitere Informationen finden Sie unter Verifizierung der E-Mail-Adresse. Sie können Konten erstellen, um Ihre Organisation zu vergrößern, ohne die E-Mail-Adresse Ihres Verwaltungskontos zu überprüfen. Um jedoch vorhandene Konten einzuladen, müssen Sie zuerst die E-Mail-Verifizierung abschließen.

   > **Note**
   >
   > Wenn dieses Konto zuvor seine E-Mail-Adresse verifiziert hat, passiert dies nicht erneut, wenn Sie das Konto verwenden, um eine Organisation zu erstellen.

AWS CLI & AWS SDKs

So erstellen Sie eine -Organisation:

Sie können einen der folgenden Befehle verwenden, um eine Organisation zu erstellen:

- AWS CLI: create-organization

Im folgenden Beispiel wird eine Organisation erstellt und das aktuell angemeldete AWS-Konto zum Verwaltungskonto für die Organisation.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> Die `AvailablePolicyTypes` ist veraltet und enthält keine genauen Informationen zu den in Ihrer Organisation aktivierten Richtlinien. Um die genaue und vollständige Liste der Richtlinientypen anzuzeigen, die tatsächlich für die Organisation aktiviert sind, verwenden Sie den `ListRoots`-Befehl, wie im AWS CLI-Abschnitt des folgenden Abschnitts beschrieben.

- AWS-SDKs: CreateOrganization

Jetzt können Sie Ihrer Organisation wie folgt weitere Konten hinzufügen:

- Informationen zu Erstellen eines AWS-Konto, das automatisch Teil Ihrer AWS-Organisation wird, finden Sie unter Erstellen eines Mitliedskontos Ihrer Organisation.
- Informationen zum Einladen eines vorhandenen Kontos zu Ihrer Organisation finden Sie unter Einen einladen AWS-Konto , Ihrer Organisation beizutreten.

Verifizierung der E-Mail-Adresse

Nachdem Sie eine Organisation erstellt haben, müssen Sie zuerst überprüfen, ob sich die für das Verwaltungskonto in der Organisation bereitgestellte E-Mail-Adresse in Ihrem Besitz befindet, bevor Sie Konten zum Beitritt einladen können.

Wenn Sie eine Organisation erstellen und das Verwaltungskonto noch nicht verifiziert wurde, sendet AWS automatisch eine Verifizierungs-E-Mail an die angegebene E-Mail-Adresse. Es kann eine Verzögerung eintreten, bevor Sie die Verifizierungs-E-Mail erhalten.

Befolgen Sie innerhalb von 24 Stunden die Anweisungen in der E-Mail zum Verifizieren Ihrer E-Mail-Adresse.

Wenn Sie Ihre E-Mail-Adresse nicht innerhalb von 24 Stunden verifizieren, können Sie die Verifizierungsanforderung erneut senden, sodass Sie andere AWS-Konten zu Ihrer Organisation einladen können. Wenn Sie keine Verifizierungs-E-Mail erhalten, überprüfen Sie, ob Ihre E-Mail-Adresse richtig ist, und korrigieren Sie sie ggf.

- Informationen dazu, wie Sie herausfinden, welche E-Mail-Adresse Ihrem Verwaltungskonto zugeordnet ist, finden Sie unter Anzeigen von Details zu einer Organisation vom Verwaltungskonto aus.
- Informationen zum Ändern der Ihrem Verwaltungskonto zugeordneten E-Mail-Adresse finden Sie unter Verwalten eines AWS-Konto im AWS Billing-Benutzerhandbuch.

AWS Management Console

So senden Sie die Verifizierungsanforderung erneut

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zur Seite Einstellungen und wählen Sie dann Verifizierungsanfrage senden. Die Option ist nur vorhanden, wenn das Verwaltungskonto nicht verifiziert ist.
3. Überprüfen Sie Ihre E-Mail-Adresse innerhalb von 24 Stunden.

   Nachdem Ihre E-Mail-Adresse verifiziert wurde, können Sie andere AWS-Konten zu Ihrer Organisation einladen. Weitere Informationen finden Sie unter Einen einladen AWS-Konto , Ihrer Organisation beizutreten.

Wenn Sie die E-Mail-Adresse des Verwaltungskontos ändern, wird der Status des Kontos auf „email unverified“ (E-Mail-Adresse nicht verifiziert) zurückgesetzt und Sie müssen den Verifizierungsprozess für die neue E-Mail-Adresse ausführen.

> **Note**
>
> Wenn Sie Konten zum Beitritt Ihrer Organisation eingeladen haben, bevor Sie die E-Mail-Adresse des Verwaltungskontos geändert haben und diese Einladungen noch nicht akzeptiert wurden, können sie erst akzeptiert werden, wenn Sie die neue E-Mail-Adresse des Verwaltungskontos verifizieren. Verwenden Sie das vorherige Verfahren, um die Verifizierungsanforderung erneut zu senden. Nachdem Sie den Vorgang abgeschlossen haben, indem Sie auf die E-Mail antworten, können Ihre eingeladenen Konten die Einladungen annehmen.

Aktivieren aller Funktionen in der Organisation

AWS Organizations bietet zwei Feature-sätze:

- All features (Alle Funktionen) – Diese Funktionsgruppe ist die bevorzugte Methode für das Arbeiten mit AWS Organizations. Sie umfasst auch die konsolidierte Fakturierung. Wenn Sie eine Organisation erstellen, werden standardmäßig alle Funktionen aktiviert. Wenn alle Funktionen aktiviert sind, können Sie die in AWS Organizations verfügbaren erweiterten Kontoverwaltungsfunktionen verwenden, z. B. die Integration mit unterstützten AWS-Services und Richtlinien zur Organisationsverwaltung.
- Consolidated billing features (Funktionen der konsolidierten Fakturierung) – Diese Funktionen werden von allen Organisationen unterstützt. Sie stellen grundlegende Verwaltungs-Tools bereit, mit denen Sie die Konten in Ihrer Organisation zentral verwalten können.

Wenn Sie eine Organisation nur mit der konsolidierten Fakturierung erstellen, können Sie auch später noch alle Funktionen aktivieren. Auf dieser Seite wird die Aktivierung aller Funktionen beschrieben.

Bevor Sie alle Funktionen aktivieren

Bevor Sie von einer Organisation, die nur die Funktionen für die konsolidierte Fakturierung unterstützt, zu einer Organisation wechseln, die alle Funktionen unterstützt, beachten Sie Folgendes:

- Beim Starten des Aktivierungsprozesses sendet AWS Organizations eine Anforderung an jedes Mitgliedskonto, das Sie zum Beitritt in die Organisation eingeladen haben. Jedes eingeladene Konto muss durch Annahme der Anforderung die Aktivierung aller Funktionen genehmigen. Nur dann können Sie den Vorgang abschließen und alle Funktionen in Ihrer Organisation aktivieren. Wenn ein Konto die Anforderung ablehnt, müssen Sie das Konto entweder aus Ihrer Organisation entfernen oder die Anforderung erneut senden. Die Anforderung muss angenommen werden, bevor Sie den Vorgang abschließen und alle Funktionen aktivieren können. Konten, die Sie mithilfe von erstellt habenAWS Organizations, erhalten keine Anforderung, weil sie die zusätzliche Kontrolle nicht genehmigen müssen.
- Sie können weiterhin Konten in Ihre Organisation einladen und gleichzeitig alle Funktionen aktivieren. Der Besitzer eines eingeladenen Kontos wird durch die Einladung darüber informiert, ob er einer Organisation beitritt, bei der nur eine konsolidierte Fakturierung vorhanden ist, oder wenn alle Funktionen aktiviert sind.
  - Wenn Sie während des Vorgangs ein Konto einladen, alle Funktionen zu aktivieren, wird in der Einladung angegeben, dass die Organisation, der sie beitreten, alle Funktionen aktiviert hat. Wenn Sie den Vorgang abbrechen, um alle Funktionen zu aktivieren, bevor das Konto die Einladung annimmt, wird diese Einladung abgebrochen. Sie müssen das Konto erneut einladen und einer Organisation nur mit der konsolidierten Fakturierung angehören.
  - Wenn Sie ein Konto einladen und die Einladung noch nicht angenommen wurde, bevor Sie mit dem Aktivieren aller Funktionen beginnen, wird diese Einladung storniert, da in der Einladung angegeben ist, dass die Organisation nur über konsolidierte Fakturierungsfunktionen verfügt. Sie müssen das Konto erneut einladen, Mitglied einer Organisation zu werden, in der alle Funktionen aktiviert sind.
- Sie können auch weiterhin Konten in der Organisation erstellen. Dieser Prozess wird von dieser Änderung nicht beeinflusst.
- AWS Organizations verifizieren außerdem, ob jedes Mitgliedskonto eine servicegebundene Rolle namens `AWSServiceRoleForOrganizations` hat. Diese Rolle ist in allen Konten obligatorisch, um alle Funktionen zu unterstützen. Wenn Sie die Rolle in einem eingeladenen Konto gelöscht haben und dann die Einladung annehmen, wird die Rolle zur Unterstützung aller Funktionen neu erstellt. Wenn Sie die Rolle in einem Konto gelöscht haben, das mit Hilfe von AWS Organizations angelegt wurde, erhält dieses Konto eine Einladung, diese Rolle neu zu erstellen. Alle Einladungen müssen angenommen werden, damit die Organisation den Prozess der Aktivierung aller Funktionen abschließen kann.
- Da die Aktivierung aller Funktionen die Verwendung von Service-Kontrollrichtlinien (SCPs)ermöglicht, stellen Sie sicher, dass Ihre Kontoadministratoren wissen, welche Auswirkungen

die Zuweisung von SCPs zur Organisation, zu Organisationseinheiten oder zu Konten hat. Eine Service-Kontrollrichtlinie kann die Aktionen von Benutzern und sogar Administratoren in betroffenen Konten einschränken. Das Verwaltungskonto kann beispielsweise SCPs anwenden, die verhindern, dass Mitgliedskonten die Organisation verlassen.

- Das Verwaltungskonto bleibt von allen SCPs unberührt. Es ist nicht möglich, mittels SCPs die Aktionen zu beschränken, die Benutzer und Rollen im Verwaltungskonto ausführen können. SCPs wirken sich nur auf Mitgliedskonten aus.
- Die Migration von Funktionen für die konsolidierte Fakturierung in alle Funktionen kann nicht rückgängig gemacht werden. Es ist nicht möglich, eine Organisation, in der alle Funktionen aktiviert sind, auf die Funktionen für die konsolidierte Fakturierung zurückzusetzen.
- (Nicht empfohlen) Wenn in Ihrer Organisation nur die Funktionen der konsolidierten Fakturierung aktiviert sind, können Administratoren von Mitgliedskonten die servicegebundene Rolle mit dem Namen `AWSServiceRoleForOrganizations` löschen. Wenn Sie später alle Funktionen in einer Organisation aktivieren möchten, ist diese Rolle erforderlich und wird in allen Konten neu erstellt, wenn Sie die Einladung zum Aktivieren aller Funktionen annehmen. Weitere Informationen darüber, wie AWS Organizations diese Rolle nutzt, finden Sie unter AWS Organizations und serviceverknüpfte Rollen.

Beginn des Prozesses zur Aktivierung aller Funktionen

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie damit beginnen, alle Funktionen zu aktivieren. Führen Sie dazu die folgenden Schritte aus.

> **Mindestberechtigungen**
>
> Zum Aktivieren aller Funktionen in der Organisation benötigen Sie die folgende Berechtigung:
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So bitten Sie die eingeladenen Mitgliedskonten um Zustimmung für die Aktivierung alle Funktionen in der Organisation

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Einstellungen die Option Vorgang für die Aktivierung aller Features starten.
3. Bestätigen Sie auf der Seite Alle Features aktivieren Ihre Zustimmung, dass Sie nach dem Wechsel nicht nur zu den konsolidierten Fakturierungs-Features zurückkehren können, indem Sie Vorgang für die Aktivierung aller Features starten auswählen.

   AWS Organizations sendet eine Anforderung an jedes eingeladene (nicht jedes erstellte) Konto in der Organisation und bittet um Genehmigung zur Aktivierung aller Funktionen. Wenn Sie Konten haben, die mit AWS Organizations erstellt wurden, und der Administrator des Mitgliedskontos die servicegebundene Rolle mit dem Namen `AWSServiceRoleForOrganizations` gelöscht hat, sendet AWS Organizations diesem Konto eine Aufforderung, die Rolle neu zu erstellen.

   Die Konsole zeigt die Option Status der Genehmigung für die eingeladenen Konten.

   > **Tip**
   >
   > Um später zu dieser Seite zurückzukehren, öffnen Sie die Seite Einstellungen und wählen Sie im Abschnitt Sendedatum anfordern die Option Status anzeigen.

4. Die Seite Alle Funktionen aktivieren zeigt den aktuellen Anforderungsstatus für jedes Konto in der Organisation. Konten, die der Anfrage zugestimmt haben, weisen den Status AKZEPTIERT auf. Konten, die noch nicht zugestimmt haben, weisen den Status OFFEN auf.

AWS CLI & AWS SDKs

So bitten Sie die eingeladenen Mitgliedskonten um Zustimmung für die Aktivierung alle Funktionen in der Organisation

Sie können einen der folgenden Befehle verwenden, um alle Funktionen in einer Organisation zu aktivieren:

- AWS CLI: enable-all-features

  Mit dem folgenden Befehl wird der Vorgang gestartet, um alle Funktionen in der Organisation zu aktivieren.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

  Die Ausgabe zeigt die Details des Handshakes, dem die eingeladenen Mitgliedskonten zustimmen müssen.

- AWS-SDKs: EnableAllFeatures

Hinweise

- Mit dem Zeitpunkt des Anforderungsversands an die Mitgliedskonten beginnt ein Countdown von 90 Tagen. Alle Konten müssen die Anforderung innerhalb dieses Zeitraums genehmigen; ansonsten läuft sie ab. Wenn die Anforderung abläuft, werden alle Anforderungen im Zusammenhang mit diesem Versuch storniert und Sie müssen mit Schritt 2 von vorne beginnen.
- Sobald Sie die Aktivierung aller Features beantragt haben, werden alle bestehenden, nicht angenommenen Kontoeinladungen storniert.
- Während der Migration aller Features können Sie weiterhin neue Kontoeinladungen initiieren und neue Konten erstellen.

Nachdem alle eingeladenen Konten in der Organisation ihre Anforderungen genehmigt haben, können Sie den Vorgang abschließen und alle Funktionen aktivieren. Sie können den Prozess auch sofort abschließen, sofern Ihre Organisation keine eingeladenen Mitgliedskonten aufweist. Um den Prozess abzuschließen, fahren Sie mit Abschließen des Prozesses der Aktivierung aller Funktionen fort.

Genehmigung der Anforderung zum Aktivieren aller Funktionen oder zum Neuanlegen der servicegebundenen Rolle

Wenn Sie sich bei einem der eingeladenen Mitgliedskonten der Organisation anmelden, können Sie eine Anfrage über das Verwaltungskonto genehmigen. Wenn Ihr Konto ursprünglich zum Beitritt zur Organisation eingeladen wurde, dann dient die Einladung dazu, alle Funktionen zu aktivieren und beinhaltet implizit die Genehmigung für die Neuerstellung der Rolle `AWSServiceRoleForOrganizations`, falls erforderlich. Wenn Ihr Konto stattdessen mit AWS Organizations erstellt wurde und Sie die servicegebundene Rolle `AWSServiceRoleForOrganizations` gelöscht haben, dann erhalten Sie nur eine Einladung zur Neuerstellung der Rolle. Führen Sie dazu die folgenden Schritte aus.

Important

Wenn Sie alle Funktionen aktivieren, kann das Verwaltungskonto in der Organisation richtlinienbasierte Kontrollen auf Ihr Mitgliedskonto anwenden. Diese Steuerelemente können

die Aktionen von Benutzern und sogar von Administratoren wie Ihnen im Konto einschränken. Solche Einschränkungen können verhindern, dass Ihr Konto die Organisation verlässt.

Mindestberechtigungen

Zum Genehmigen einer Anforderung für die Aktivierung aller Funktionen für Ihr Mitgliedskonto benötigen Sie die folgende Berechtigung:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:ListHandshakesForAccount` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `iam:CreateServiceLinkedRole` – Nur erforderlich, wenn die `AWSServiceRoleForOrganizations`-Rolle im Mitgliedskonto neu erstellt werden muss.

AWS Management Console

So stimmen Sie der Anforderung für die Aktivierung aller Funktionen in der Organisation zu

1. Melden Sie sich bei der AWS Organizations-Konsole unter AWS Organizations-Konsole an. Sie müssen sich im Mitgliedskonto als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Lesen Sie, welche Konsequenzen die Annahme der Anfrage für alle Funktionen in der Organisation für Ihr Konto hat, und klicken Sie dann auf Accept. Die Seite zeigt den Prozess so lange als unvollständig an, bis alle Konten in der Organisation die Anforderungen annehmen und der Administrator des Verwaltungskontos den Prozess abschließt.

AWS CLI & AWS SDKs

So stimmen Sie der Anforderung für die Aktivierung aller Funktionen in der Organisation zu

Wenn Sie der Anforderung zustimmen möchten, müssen Sie den Handshake mit `"Action": "APPROVE_ALL_FEATURES"` annehmen.

- AWS CLI:

- accept-handshake
- list-handshakes-for-account

Im folgenden Beispiel wird gezeigt, wie Sie die Handshakes für Ihr Konto auflisten. Der Wert von "Id" in der vierten Zeile der Ausgabe ist der Wert, den Sie für den nächsten Befehl benötigen.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
```

```
        }
    ]
}
```

Im folgenden Beispiel wird die ID des Handshakes aus dem vorherigen Befehl verwendet, um diesen Handshake zu akzeptieren.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
```

```
}
```

- AWS-SDKs:
  - list-handshakes-for-account
  - AcceptHandshake

Abschließen des Prozesses der Aktivierung aller Funktionen

Alle eingeladenen Mitgliedskonten müssen die Anforderung genehmigen, um alle Funktionen zu aktivieren. Wenn die Organisation keine eingeladen Mitgliedskonten hat, wird auf der Seite Enable all features progress (Alle Funktionen aktivieren – Fortschritt) mit einem grünen Banner signalisiert, dass Sie den Prozess abschließen können.

Mindestberechtigungen

Zum Abschließen des Prozesses der Aktivierung aller Funktionen in der Organisation benötigen Sie die folgende Berechtigung:

- `organizations:AcceptHandshake`
- `organizations:ListHandshakesForOrganization`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So schließen Sie den Prozess der Aktivierung aller Funktionen ab

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wenn auf der Seite Einstellungen alle eingeladenen Konten die Anfrage zum Aktivieren aller Funktionen akzeptieren, wird oben auf der Seite ein grünes Kästchen angezeigt, um Sie zu informieren. Wählen Sie im grünen Feld Zum Abschluss gehen aus.
3. Wählen Sie auf der Seite Alle Funktionen aktivieren die Option Abschließen aus, und wählen Sie dann im Bestätigungsdialogfeld erneut Abschließen aus.
4. Bei der Organisation wurden jetzt alle Funktionen aktiviert.

AWS CLI & AWS SDKs

So schließen Sie den Prozess der Aktivierung aller Funktionen ab

Wenn Sie Prozess abschließen möchten, müssen Sie den Handshake mit `"Action": "ENABLE_ALL_FEATURES"` annehmen.

- AWS CLI:
  - list-handshakes-for-organization
  - accept-handshake

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

Im folgenden Beispiel wird gezeigt, wie Sie die Handshakes für die Organisation auflisten. Der Wert von `"Id"` in der vierten Zeile der Ausgabe ist der Wert, den Sie für den nächsten Befehl benötigen.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS-SDKs:
  - AcceptHandshake
  - AcceptHandshake

Die nächsten Schritte:

- Aktivieren Sie die zu verwendenden Richtlinientypen. Anschließend können Sie Richtlinien für die Verwaltung der Konten in Ihrer Organisation zuordnen. Weitere Informationen finden Sie unter Verwalten von Richtlinien in AWS Organizations.
- Aktivieren Sie die Integration mit unterstützten Diensten. Weitere Informationen finden Sie unter Verwenden von AWS Organizations mit anderen AWS-Services.

Anzeigen von Details zu Ihrer Organisation

Zum Anzeigen der Details Ihrer Organisation können Sie die folgenden Aufgaben ausführen.

Themen

- Anzeigen von Details zu einer Organisation vom Verwaltungskonto aus
- Anzeigen der Details des Root-Containers
- Anzeigen von Details zu einer OU
- Anzeigen von Details zu einem Konto
- Anzeigen der Details einer Richtlinie

Anzeigen von Details zu einer Organisation vom Verwaltungskonto aus

Wenn Sie sich bei der AWS Organizations-Konsole am Verwaltungskonto der Organisation angemeldet haben, können Sie die Details zu einem Stammbenutzer anzeigen.

> **Mindestberechtigungen**
>
> Zum Anzeigen von Details zu einer Organisation benötigen Sie die folgende Berechtigung:
>
> - `organizations:DescribeOrganization`

AWS Management Console

So zeigen Sie die Details Ihrer Organisation an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zur Seite Einstellungen. Auf dieser Seite werden Details über die Organisation angezeigt, darunter die Organisations-ID sowie der Kontoname und die E-Mail-Adresse, die dem Verwaltungskonto der Organisation zugewiesen sind.

AWS CLI & AWS SDKs

So zeigen Sie die Details Ihrer Organisation an

Sie können einen der folgenden Befehle verwenden, um die Details einer Organisation anzuzeigen:

- AWS CLI: describe-organization

  Das folgende Beispiel zeigt die Informationen, die in der Ausgabe dieses Befehls enthalten sind.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

  Important

  Die `AvailablePolicyTypes` ist veraltet und enthält keine genauen Informationen zu den in Ihrer Organisation aktivierten Richtlinien. Um die genaue und vollständige Liste der Richtlinientypen anzuzeigen, die tatsächlich für die Organisation aktiviert sind, verwenden Sie den `ListRoots`-Befehl, wie im AWS CLI-Abschnitt des folgenden Abschnitts beschrieben.

- AWS-SDKs: DescribeOrganization

Anzeigen der Details des Root-Containers

Wenn Sie sich in der AWS Organizations-Konsole beim Verwaltungskonto der Organisation anmelden, können Sie Details des Root-Containers anzeigen.

Mindestberechtigungen

Zum Anzeigen der Details zum Root benötigen Sie folgende Berechtigungen:

- `organizations:DescribeOrganization` (nur Konsole)
- `organizations:ListRoots`

Der Stamm ist der oberste Container in der Hierarchie der Organisationseinheiten (OUs) und verhält sich im Allgemeinen als Organisationseinheit. Da jedoch der Container ganz oben in der Hierarchie liegt, wirken sich Änderungen am Stamm auf jede andere Organisationseinheit und jede AWS-Konto in der Organisation aus.

AWS Management Console

So zeigen Sie die Details zu einem Stamm an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zur Seite AWS-Konten und wählen Sie die Stamm-OU (der Name, nicht das Optionsfeld).
3. Die Seite Stammdetails wird angezeigt und zeigt die Details des Stammes an.

AWS CLI & AWS SDKs

So zeigen Sie die Details zu einem Stamm an

Sie können einen der folgenden Befehle verwenden, um die Details eines Root-Benutzers anzuzeigen:

- AWS CLI: list-roots

  Das folgende Beispiel zeigt, wie Sie die Details des Stamms aufrufen, einschließlich der Richtlinientypen, die derzeit in der Organisation aktiviert sind:

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
```

```
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
            ]
        }
    ]
}
```

- AWS-SDKs: ListRoots

Anzeigen von Details zu einer OU

Wenn Sie sich bei der AWS Organizations-Konsole am Verwaltungskonto der Organisation angemeldet haben, können Sie die Details der OUs zu einem Stammbenutzer anzeigen.

> **Mindestberechtigungen**
>
> Zum Anzeigen von Details zu einer Organisationseinheit benötigen Sie die folgende Berechtigungen:
>
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:ListOrganizationsUnitsForParent` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:ListRoots` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So zeigen Sie Details zu einer Organisationseinheit an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Klicken Sie auf AWS-Konten und wählen Sie den Namen der Organisationseinheit (nicht das Optionsfeld) aus, die Sie ansehen möchten. Wenn die gewünschte Organisationseinheit einer anderen Organisationseinheit untergeordnet ist, wählen Sie das Dreiecksymbol neben der übergeordneten Organisationseinheit aus, um sie zu erweitern und die Elemente in der nächsten Hierarchieebene anzuzeigen. Wiederholen Sie den Vorgang, bis Sie die gewünschte Organisationseinheit finden.

   In den Details zur Organisationseinheit werden die Informationen zur Organisationseinheit angezeigt.

AWS CLI & AWS SDKs

So zeigen Sie Details zu einer Organisationseinheit an

Sie können einen der folgenden Befehle verwenden, um Details einer Organisationseinheit anzuzeigen:

- AWS CLI-, AWS-SDKs:
  - list-roots
  - list-children
  - describe-organizational-unit

Das folgende Beispiel zeigt, wie Sie die ID von in der Organisationseinheit mithilfe der AWS CLI finden können. Sie finden die OU-ID, indem Sie die Hierarchie beginnend mit dem `list-roots`-Befehl durchlaufen und dann `list-children` für den Stamm und iterativ für jedes ihrer untergeordneten Elemente ausführen, bis Sie die gewünschte gefunden haben.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
```

```
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Nachdem Sie die ID der Organisationseinheit erhalten haben, wird im folgenden Beispiel gezeigt, wie die Details zur Organisationseinheit abgerufen werden.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS-SDKs:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Anzeigen von Details zu einem Konto

Wenn Sie sich bei der AWS Organizations-Konsole am Verwaltungskonto der Organisation angemeldet haben, können Sie die Details zu Ihren Konten anzeigen.

Mindestberechtigungen

Zum Anzeigen der Details zu einem AWS-Konto benötigen Sie folgende Berechtigungen:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

- `organizations:ListAccounts` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So zeigen Sie Details zu einer AWS-Konto an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zu AWS-Konten und wählen Sie den Namen des Kontos (nicht das Optionsfeld) aus, das Sie ansehen möchten. Wenn das gewünschte Konto einer Organisationseinheit untergeordnet ist, müssen Sie möglicherweise das Dreiecksymbol neben einer Organisationseinheit auswählen, um sie zu erweitern und ihre untergeordneten Konten anzuzeigen. Wiederholen Sie dies, bis Sie das Konto gefunden haben.

   In den Kontodetails werden die Informationen zum Konto angezeigt.

AWS CLI & AWS SDKs

So zeigen Sie Details zu einer AWS-Konto an

Sie können einen der folgenden Befehle verwenden, um Details eines Kontos anzuzeigen:

- AWS CLI:
  - list-accounts – listet die Details von allen Konten in der Organisation auf
  - describe-account – listet nur die Details des angegebenen Kontos auf

  Beide Befehle geben die gleichen Details für jedes Konto zurück, das in der Antwort enthalten ist.

  Das folgende Beispiel zeigt, wie die Details eines angegebenen Kontos abgerufen werden.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
```

```
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWS-SDKs:
  - ListAccounts
  - DescribeAccount

Anzeigen der Details einer Richtlinie

Wenn Sie sich bei der AWS Organizations-Konsole am Verwaltungskonto der Organisation angemeldet haben, können Sie die Details zu Ihren Richtlinien anzeigen.

> **Mindestberechtigungen**
>
> Um die Details einer Richtlinie anzuzeigen, benötigen Sie die folgenden Berechtigungen:
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

AWS Management Console

So zeigen Sie die Details einer Richtlinie an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Führen Sie einen der folgenden Schritte aus:
   - Navigieren Sie zu Richtlinien und wählen Sie dann den Richtlinientyp für die Richtlinie aus, die Sie ansehen möchten.

- Navigieren Sie zu AWS-Konten und navigieren Sie dann zu einer Organisationseinheit oder einem Konto, an das die Richtlinie angehängt ist. Wählen Sie abschließend die Option Richtlinien, um die Liste der angehängten Richtlinien anzuzeigen.

3. Wählen Sie den Namen der Richtlinie (nicht das Optionsfeld) aus.

   Auf der Seite Details für die Richtlinie können Sie alle Informationen zur Richtlinie anzeigen, einschließlich des JSON-Richtlinientexts und der Liste der OUs und Konten, denen die Richtlinie zugeordnet ist.

AWS CLI & AWS SDKs

So zeigen Sie die Details einer Richtlinie an

Sie können einen der folgenden Befehle verwenden, um die Details einer Richtlinie anzuzeigen:

- AWS CLI:
  - list-policies
  - describe-policy – listet nur die Details der angegebenen Richtlinie auf

Das folgende Beispiel zeigt, wie Sie die Richtlinien-ID der Richtlinie finden, die Sie ansehen möchten. Sie müssen einen Richtlinientyp angeben und der Befehl gibt alle Richtlinien dieses Typs zurück.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

Die Antwort enthält alle Details mit Ausnahme des JSON-Richtliniendokuments.

Im folgenden Beispiel wird gezeigt, wie nur die Details der angegebenen Richtlinie abgerufen werden, einschließlich des JSON-Richtliniendokuments.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```

- AWS-SDKs:
  - ListPolicies
  - DescribePolicy

Löschen einer Organisation

Wenn Sie Ihre Organisation nicht mehr benötigen, können Sie sie löschen. Wenn eine Organisation gelöscht wird, wird das Verwaltungskonto nicht geschlossen, sondern aus der Organisation entfernt. Zudem wird die Organisation selbst gelöscht. Das ehemalige Verwaltungskonto wird zu einem eigenständigen AWS-Konto-Konto, das nicht mehr von AWS Organizations verwaltet wird. Sie haben dann drei Möglichkeiten: Sie können es weiterhin als eigenständiges Konto verwenden, Sie können es verwenden, um eine andere Organisation zu erstellen, oder Sie können eine Einladung von

einer anderen Organisation annehmen, um das Konto dieser Organisation als ein Mitgliedskonto hinzuzufügen.

> **Important**
>
> - Wenn Sie eine Organisation löschen, können Sie sie nicht wiederherstellen. Wenn Sie Richtlinien innerhalb der Organisation erstellt haben, werden diese ebenfalls gelöscht und können nicht wiederhergestellt werden.
> - Sie können eine Organisation erst löschen, nachdem Sie alle Mitgliedskonten aus der Organisation entfernt haben. Wenn Sie einige Ihrer Mitgliedskonten mithilfe von AWS Organizations erstellt haben, werden Sie diese Konten möglicherweise nicht entfernen können. Sie können ein Mitgliedskonto nur entfernen, wenn es über alle Informationen verfügt, die für den Betrieb als eigenständiges AWS-Konto erforderlich sind. Weitere Informationen darüber, wie Sie diese Informationen bereitstellen und dann das Konto entfernen können, finden Sie unter Verlassen einer Organisation in Ihrem Mitgliedskonto.
> - Wenn Sie ein Mitgliedskonto geschlossen haben, bevor Sie es aus der Organisation entfernen, wird es für einen bestimmten Zeitraum gesperrt und Sie können das Konto nicht aus der Organisation entfernen, bis es endgültig geschlossen ist. Dies kann bis zu 90 Tage dauern und dazu führen, dass Sie die Organisation erst löschen können, wenn alle Mitgliedskonten vollständig geschlossen sind.

Wenn Sie das Verwaltungskonto aus einer Organisation entfernen, indem Sie die Organisation löschen, kann dies folgende Auswirkungen auf das Konto haben:

- Das Konto ist nur für die Zahlung seiner eigenen Gebühren und nicht mehr für die Kosten verantwortlich, die durch ein anderes Konto entstehen.
- Die Integration mit anderen Services wird möglicherweise deaktiviert. Beispielsweise benötigt AWS IAM Identity Center eine aktive Organisation; wenn Sie also ein Konto aus einer Organisation entfernen, die IAM Identity Center unterstützt, können die Benutzer in diesem Konto diesen Service nicht mehr nutzen.

Das Verwaltungskonto einer Organisation ist von Service-Kontrollrichtlinien (Service Control Policies, SCPs) niemals betroffen, sodass es zu keinen Änderungen bei den Berechtigungen kommt, wenn keine SCPs mehr verfügbar sind.

Themen

- Löschen einer Organisation

Löschen einer Organisation

Gehen Sie wie folgt vor, um eine Organisation zu löschen, wodurch das ehemalige Verwaltungskonto in ein eigenständiges AWS-Konto zurückverwandelt wird, das nicht mehr von AWS Organizations verwaltet wird.

> **Mindestberechtigungen**
>
> Um eine Organisation löschen zu können, müssen Sie sich als Benutzer oder Rolle beim Verwaltungskonto anmelden und über folgende Berechtigungen verfügen:
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So löschen Sie eine Organisation

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Bevor Sie die Organisation löschen können, müssen Sie alle Konten aus der Organisation entfernen. Weitere Informationen finden Sie unter Entfernen eines Mitgliedskontos aus Ihrer Organisation.
3. Navigieren Sie zu Einstellungen und wählen Sie dann Organisation löschen aus.
4. Geben Sie im Bestätigungsdialogfeld Organisation löschen die ID der Organisation ein, die in der Zeile über dem Textfeld angezeigt wird. Wählen Sie dann Organisation löschen aus.

> **Important**
>
> Durch diesen Vorgang wird das Verwaltungskonto nicht geschlossen, sondern in ein eigenständiges AWS-Konto zurückverwandelt. Um das Konto zu schließen, führen Sie die Schritte unter So schließen Sie ein Mitliedskonto Ihrer Organisation durch.

AWS CLI & AWS SDKs

So löschen Sie eine Organisation

Verwenden Sie einen der folgenden Befehle, um eine Organisation zu löschen:

- AWS CLI: delete-organization

  Im folgenden Beispiel wird die Organisation gelöscht, für die das AWS-Konto, dessen Anmeldeinformationen verwendet werden, das Verwaltungskonto ist.

  ```
  $ aws organizations delete-organization
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-SDKs: DeleteOrganization

Verwalten von AWS-Konten in Ihrer Organisation

Eine Organisation ist eine Sammlung von AWS-Konten, die Sie zentral verwalten. Sie können die folgenden Aufgaben zum Verwalten der Konten Ihrer Organisation ausführen:

- Anzeigen von Details der Konten in Ihrer Organisation. Sie können die eindeutige ID des Kontos, seinen Amazon-Ressourcennamen (ARN) und die an das Konto angefügten Richtlinien anzeigen.
- Exportieren Sie eine Liste aller AWS-Konten in Ihrer Organisation. Sie können eine .csv-Datei herunterladen, die Kontodetails für jedes Konto in Ihrer Organisation enthält.
- Laden Sie vorhandene AWS-Konten zum Beitritt zu Ihrer Organisation ein. Erstellen Sie Einladungen, verwalten Sie erstellte Einladungen und nehmen Sie Einladungen an oder lehnen diese ab.
- Erstellen eines AWS-Konto als Teil Ihrer Organisation. Erstellen Sie ein AWS-Konto, das automatisch zu Ihrem Unternehmen hinzugefügt wird, und greifen Sie auf das Konto zu.
- Aktualisieren alternativer Kontakte in Ihrer Organisation. Aktualisieren alternativer Kontakte für Ihre AWS-Konto in Ihrer Organisation.
- Entfernen eines AWS-Konto aus Ihrer Organisation. Als Administrator im Verwaltungskonto entfernen Sie Konten, die Sie nicht mehr von Ihrer Organisation aus verwalten möchten. Als Administrator eines Mitgliedskontos entfernen Sie Ihr Konto aus dessen Organisation. Wenn das Verwaltungskonto eine Richtlinie an Ihr Mitgliedskonto angefügt hat, wird das Entfernen Ihres Kontos möglicherweise unterbunden.
- Löschen (oder schließen) Sie AWS-Konto. Wenn Sie ein AWS-Konto nicht mehr benötigen, können Sie das Konto schließen, um zu verhindern, dass es genutzt wird und Kosten entstehen.

Auswirkungen der Mitgliedschaft in einer Organisation

- Welche Auswirkungen hat ein AWS-Konto, das einer Organisation beitritt?
- Welche Auswirkungen hat ein AWS-Konto, das Sie in einer Organisation erstellen?

Auswirkungen auf ein AWS-Konto, das einer Organisation beitritt?

Wenn Sie ein AWS-Konto einladen, einer Organisation beizutreten, und der Kontoinhaber die Einladung annimmt, nimmt AWS Organizations automatisch die folgenden Änderungen an dem neuen Mitgliedskonto vor:

- AWS Organizations erstellt eine serviceverknüpfte Rolle namens `AWSServiceRoleForOrganizations`. Das Konto muss über diese Rolle verfügen, wenn Ihre Organisation alle Funktionen unterstützt. Sie können die Rolle löschen, wenn die Organisation nur den Feature-satz für konsolidierte Fakturierung unterstützt. Wenn Sie die Rolle löschen und später alle Funktionen in Ihrer Organisation aktivieren, erstellt AWS Organizations die Rolle für das Konto neu.
- Möglicherweise verfügen Sie über eine Vielzahl von Richtlinien an den Organisationsstamm oder die Organisationseinheit, die das Konto enthält, angehängt sind. In diesem Fall werden diese Richtlinien unmittelbar für alle Benutzer und Rollen im eingeladenen Konto übernommen.
- Sie können die Vertrauensbeziehung zum Service für einen anderen AWS-Service in Ihrer Organisation aktivieren. Wenn Sie dies tun, kann dieser vertrauenswürdige Service serviceverknüpfte Rollen erstellen oder in einem beliebigen Mitgliedskonto der Organisation, einschließlich einem eingeladenen Konto, Aktionen ausführen.

> **Note**
>
> Bei Konten eingeladener Mitglieder erstellt die IAM-Rolle AWS Organizations nicht automatischOrganizationAccountAccessRole. Diese Rolle gewährt Benutzern im Verwaltungskonto Administratorzugriff auf das Mitgliedskonto. Wenn Sie diese Ebene der administrativen Kontrolle für ein eingeladenes Konto aktivieren möchten, können Sie die Rolle manuell hinzufügen. Weitere Informationen finden Sie unter Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto.

Sie können ein Konto zum Beitritt zu einer Organisation einladen, für die nur die konsolidierte Fakturierung aktiviert ist. Wenn Sie später alle Funktionen für die Organisation aktivieren möchten, müssen eingeladene Konten die Änderung genehmigen.

Auswirkungen auf ein AWS-Konto, das Sie in einer Organisation erstellen?

Wenn Sie ein AWS-Konto in Ihrer Organisation erstellen, nimmt AWS Organizations automatisch die folgenden Änderungen an dem neuen Mitgliedskonto vor:

- AWS Organizations erstellt eine serviceverknüpfte Rolle namens `AWSServiceRoleForOrganizations`. Das Konto muss über diese Rolle verfügen, wenn Ihre Organisation alle Funktionen unterstützt. Sie können die Rolle löschen, wenn die Organisation nur den Feature-satz für konsolidierte Fakturierung unterstützt. Wenn Sie die Rolle löschen und später

alle Funktionen in Ihrer Organisation aktivieren, erstellt AWS Organizations die Rolle für das Konto neu.

- AWS Organizations erstellt die IAM-Rolle OrganizationAccountAccessRole. Diese Rolle gewährt dem Verwaltungskonto Zugriff auf das neue Mitgliedskonto. Obwohl diese Rolle gelöscht werden kann, empfehlen wir, sie nicht zu löschen, damit sie als Wiederherstellungsoption verfügbar ist.
- Wenn dem Stamm der Organisationseinheitsstruktur Richtlinien angefügt sind, gelten diese Richtlinien sofort für alle Benutzer und Rollen im erstellten Konto. Neue Konten werden standardmäßig der Organisationseinheit Root hinzugefügt.
- Wenn Sie für Ihre Organisation Treuhandservice für einen anderen AWS-Service aktiviert haben, kann dieser vertrauenswürdige Service serviceverknüpfte Rollen erstellen oder in einem beliebigen Mitgliedskonto der Organisation, einschließlich Ihrem erstellten Konto, Aktionen ausführen.

Einen einladen AWS-Konto , Ihrer Organisation beizutreten

Nachdem Sie eine Organisation erstellt und sich vergewissert haben, dass Sie Eigentümer der mit dem Verwaltungskonto verknüpften E-Mail-Adresse sind, können Sie bestehende Personen AWS-Konten einladen, Ihrer Organisation beizutreten.

Wenn Sie ein Konto einladen, AWS Organizations sendet eine Einladung an den Kontoinhaber, der entscheidet, ob er die Einladung annimmt oder ablehnt. Sie können die AWS Organizations Konsole verwenden, um Einladungen, die Sie an andere Konten senden, zu initiieren und zu verwalten. Eine Einladung an ein anderes Konto können Sie nur vom Verwaltungskonto Ihrer Organisation aus senden.

> **Note**
>
> Der Abrechnungsverlauf und die Berichte für alle Konten verbleiben beim Zahlerkonto in einer Organisation. Bevor Sie das Konto in eine neue Organisation verschieben, laden Sie alle Abrechnungs- und Berichtsverläufe für alle Mitgliedskonten herunter, die Sie behalten möchten. Dies kann Kosten- und Nutzungsberichte, detaillierte Abrechnungsberichte oder vom Cost-Explorer-Service generierte Berichte umfassen.

Wenn Sie der Administrator einer sind AWS-Konto, können Sie auch eine Einladung einer Organisation annehmen oder ablehnen. Wenn Sie annehmen, wird Ihr Konto Mitglied dieser Organisation. Ihr Konto kann nur einer Organisation beitreten. Wenn Sie also mehrere Einladungen zum Beitritt erhalten, können Sie nur eine annehmen.

In dem Moment, in dem ein Konto die Einladung zum Beitritt einer Organisation annimmt, haftet das Management-Konto der Organisation für alle Gebühren, die durch das neue Mitgliedskonto anfallen. Die dem Mitgliedskonto zugeordnete Zahlungsmethode wird nicht mehr verwendet. Stattdessen bezahlt die Zahlungsart, die dem Verwaltungskonto der Organisation zugeordnet ist, alle Gebühren, die vom Mitgliedskonto anfallen.

Wenn ein Konto mit Einladung Ihrer Organisation beitritt und sich Ihre Organisation im Modus „Alle Funktionen“ befindet, hat das Verwaltungskonto vollen Administratorzugriff auf das Konto und die volle Kontrolle über das Konto des eingeladenen Mitglieds. Im Gegensatz zu erstellten Konten wird die `OrganizationAccountAccessRole` IAM-Rolle jedoch nicht automatisch im Mitgliedskonto erstellt, sodass das Verwaltungskonto die entsprechenden Berechtigungen annehmen kann. Gehen Sie wie folgt vor, um dies zu erstellen und zu konfigurieren, nachdem das eingeladene Konto Mitglied geworden ist. Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto

> **Note**
>
> Wenn Sie ein Konto in Ihrer Organisation erstellen, anstatt ein vorhandenes Konto zum Beitritt einzuladen, AWS Organizations wird automatisch eine IAM-Rolle (`OrganizationAccountAccessRole`standardmäßig benannt) erstellt, mit der Sie Benutzern im Verwaltungskonto Administratorzugriff auf das erstellte Konto gewähren können.

AWS Organizations erstellt automatisch eine dienstbezogene Rolle in den Konten eingeladener Mitglieder, um die Integration zwischen AWS Organizations und anderen AWS Diensten zu unterstützen. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpfte Rollen.

Die Anzahl der Einladungen, die Sie pro Tag versenden können, finden Sie unter Höchst- und Mindestwerte. Akzeptierte Einladungen werden nicht auf dieses Kontingent angerechnet. Sobald eine Einladung akzeptiert wird, können Sie am selben Tag eine weitere Einladung senden. Jede Einladung muss innerhalb von 15 Tagen oder bis zu ihrem Ablauf beantwortet werden.

Eine an ein Konto gesendete Einladung wird auf das Kontokontingent in Ihrer Organisation angerechnet. Die Anrechnung wird wiederhergestellt, wenn das eingeladene Konto ablehnt, das Verwaltungskonto die Einladung ablehnt oder die Einladung abgelaufen ist.

Informationen zum Erstellen eines Kontos, das automatisch Ihrer Organisation angehört, finden Sie unter Erstellen eines Mitliedskontos Ihrer Organisation.

Important

Aus rechtlichen und abrechnungsrechtlichen Gründen können Sie AWS-Konten nur über denselben AWS Verkäufer und dieselbe AWS Partition einladen wie das Verwaltungskonto. In einer AWS EMEA-Organisation können Sie beispielsweise nur Konten des eingetragenen AWS EMEA SARL-Verkäufers einladen.

- Alle Konten in einer Organisation müssen vom selben registrierten Verkäufer wie das Verwaltungskonto stammen, wenn das Verwaltungskonto Ihrer Organisation von Amazon Internet Services Pvt. Ltd (AISPL) erstellt wurde. Als AWS Verkäufer in Indien können Sie beispielsweise nur andere AISPL-Konten in Ihre Organisation einladen. Sie können Konten von AISPL und/oder Konten von anderen Verkäufern AWS nicht kombinieren. AWS
- Alle Konten in einer Organisation müssen aus derselben AWS Partition stammen wie das Verwaltungskonto. Konten in der kommerziellen AWS-Regionen Partition können nicht zu einer Organisation gehören, die Konten aus der Partition China Regions oder Konten aus der Partition AWS GovCloud (US) Regions hat.

Senden von Einladungen an AWS-Konten

Um Konten zu Ihrer Organisation einladen zu können, müssen Sie zuerst überprüfen, ob Sie sich im Besitz der E-Mail-Adresse befinden, die mit dem Verwaltungskonto verknüpft ist. Weitere Informationen finden Sie unter Verifizierung der E-Mail-Adresse. Nachdem Sie Ihre E-Mail-Adresse verifiziert haben, führen Sie die folgenden Schritte aus, um Konten zu Ihrer Organisation einzuladen.

Mindestberechtigungen

AWS-Konto Um einen einzuladen, Ihrer Organisation beizutreten, benötigen Sie die folgenden Berechtigungen:

- `organizations:DescribeOrganization` (nur Konsole)
- `organizations:InviteAccountToOrganization`

AWS Management Console

Einladen eines anderen Kontos zu Ihrer Organisation

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wenn Sie Ihre E-Mail-Adresse bereits mit bestätigt haben AWS, überspringen Sie diesen Schritt.

   Wenn Sie Ihre E-Mail-Adresse noch nicht bestätigt haben, befolgen Sie die Anweisungen in der Verifizierungs-E-Mail innerhalb von 24 Stunden, nachdem Sie die Organisation erstellt haben. Es kann eine Verzögerung eintreten, bevor Sie die Verifizierungs-E-Mail-Nachricht erhalten. Sie können ein Konto erst dann zum Beitritt zu Ihrer Organisation einladen, wenn Sie Ihre E-Mail-Adresse verifiziert haben.
3. Navigieren Sie zu AWS-Konten und wählen Sie Hinzufügen eines AWS -Kontos aus.
4. Klicken Sie auf der Seite Hinzufügen eines AWS-Konto auf Einladen eines vorhandenen AWS -Kontos.
5. Geben Sie auf der AWS Seite „Bestehende Person einladen“ in das Feld E-Mail-Adresse oder Konto-ID der AWS-Konto einzuladenden Person entweder die E-Mail-Adresse des einzuladenden Kontos oder dessen Konto-ID-Nummer ein.
6. (Optional) Geben Sie für Nachricht in der Einladungs-E-Mail-Nachricht einen beliebigen Text ein, den Sie in die E-Mail-Einladung an den eingeladenen Kontoinhaber einfügen möchten.
7. (Optional) Geben Sie im Abschnitt Tags hinzufügen ein oder mehrere Tags an, die automatisch auf das Konto angewendet werden, nachdem der Administrator die Einladung angenommen hat. Wählen Sie dazu Tag hinzufügen und geben Sie dann einen Schlüssel und einen optionalen Wert ein. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können bis zu 50 Tags an ein AWS-Konto anfügen.
8. Wählen Sie Send invitation (Einladung senden) aus.

> **Important**
>
> Wenn Sie eine Meldung erhalten, die darauf hinweist, dass Sie Ihr Kontokontingent für die Organisation überschritten haben oder dass Sie kein Konto hinzufügen

können, weil Ihre Organisation immer noch initialisiert wird, wenden Sie sich an AWS Support.

9. Die Konsole leitet Sie zur Seite Einladungen weiter, auf der Sie alle offenen und angenommenen Einladungen hier anzeigen können. Die Einladung, die Sie gerade erstellt haben, wird oben auf der Liste mit dem Status OPEN angezeigt.

   AWS Organizations sendet eine Einladung an die E-Mail-Adresse des Inhabers des Kontos, das Sie zur Organisation eingeladen haben. Diese E-Mail-Nachricht enthält einen Link zur AWS Organizations Konsole, über die der Kontoinhaber die Details einsehen und entscheiden kann, ob er die Einladung annehmen oder ablehnen möchte. Alternativ kann der Inhaber des eingeladenen Accounts die E-Mail-Nachricht umgehen, direkt zur AWS Organizations Konsole wechseln, die Einladung ansehen und sie annehmen oder ablehnen.

   Die Einladung für dieses Konto wird sofort auf die maximale Anzahl der Konten, die Sie in Ihrer Organisation haben können, angerechnet; AWS Organizations wartet nicht, bis das Konto die Einladung annimmt. Wenn das eingeladene Konto ablehnt, hebt das Verwaltungskonto die Einladung auf. Wenn das eingeladene Konto nicht innerhalb des angegebenen Zeitraums reagiert, läuft die Einladung ab. In beiden Fällen wird die Einladung Ihrem Kontingent nicht mehr angerechnet.

AWS CLI & AWS SDKs

Einladen eines anderen Kontos zu Ihrer Organisation

Sie können einen der folgenden Befehle verwenden, um ein anderes Konto zum Beitritt zu Ihrer Organisation einzuladen:

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
```

```
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```

- AWS SDKs: InviteAccountToOrganization

Verwalten schwebender Einladungen für Ihre Organisation

Wenn Sie an Ihrem Verwaltungskonto angemeldet sind, können Sie alle verknüpften AWS-Konten innerhalb Ihrer Organisation sehen und schwebende (offene) Einladungen abbrechen. Führen Sie dazu die folgenden Schritte aus.

> **Mindestberechtigungen**
>
> Zum Verwalten schwebender Einladungen für Ihre Organisation benötigen Sie folgende Berechtigungen:
>
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:ListHandshakesForOrganization`
> - `organizations:CancelHandshake`

AWS Management Console

Ansehen oder Abbrechen von Einladungen, die von Ihrer Organisation an andere Konten gesendet wurden

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zur Seite Einladungen.

   Auf dieser Seite werden alle Einladungen, die von Ihrer Organisation gesendet werden, und deren aktuellen Status angezeigt.

   > **Note**
   >
   > Akzeptierte, abgebrochene und abgelehnte Einladungen werden 30 Tage lang weiterhin in der Liste angezeigt. Danach werden sie gelöscht und nicht mehr in der Liste angezeigt.

3. Wählen Sie das Optionsfeld
   
   neben

der Einladung aus, die Sie abbrechen möchten und wählen Sie dann Einladung stornieren aus. Wenn das Optionsfeld ausgegraut ist, kann diese Einladung nicht storniert werden.

Der Status der Einladung ändert sich von Offen in Abgebrochen.

AWS sendet eine E-Mail-Nachricht an den Kontoinhaber, dass Sie die Einladung storniert haben. Das Konto kann der Organisation nicht mehr beitreten, es sei denn, Sie senden eine neue Einladung.

AWS CLI & AWS SDKs

Ansehen oder Abbrechen von Einladungen, die von Ihrer Organisation an andere Konten gesendet wurden

Mit den folgenden Befehlen können Sie Einladungen anzeigen oder stornieren:

- AWS CLI: list-handshakes-for-organization, Handshake abbrechen
- Das folgende Beispiel zeigt die Einladungen, die von dieser Organisation an andere Konten gesendet werden.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
```

```
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
```

```
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

Im folgenden Beispiel wird gezeigt, wie Sie eine Einladung zu einem Konto abbrechen.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
```

```
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDKs:, ListHandshakesForOrganizationCancelHandshake

Akzeptieren oder Ablehnen einer Einladung von einer Organisation

AWS-Konto Möglicherweise erhalten Sie eine Einladung, einer Organisation beizutreten. Sie können die Einladung akzeptieren oder ablehnen. Führen Sie dazu die folgenden Schritte aus.

Note

Der Status eines Kontos bei einer Organisation wirkt sich darauf aus, welche Kosten- und Nutzungsdaten angezeigt werden:

- Wenn ein Mitgliedskonto eine Organisation verlässt und ein eigenständiges Konto wird, hat das Konto keinen Zugriff mehr auf Kosten- und Nutzungsdaten aus dem Zeitraum, als das Konto ein Mitglied der Organisation war. Das Konto hat nur Zugriff auf die Daten, die als ein eigenständiges Konto generiert werden.
- Wenn ein Mitgliedskonto Organisation A verlässt, um Organisation B beizutreten, hat das Konto keinen Zugriff mehr auf Kosten- und Nutzungsdaten aus dem Zeitraum, als das Konto Mitglied der Organisation A war. Das Konto hat nur Zugriff auf die Daten, die Mitglied der Organisation B generiert werden.
- Wenn ein Konto erneut einer Organisation beitritt, zu der es vorher gehörte, erhält das Konto wieder Zugriff auf seine früheren Kosten- und Nutzungsdaten.

Note

Einladungen zum Beitritt zu einer Organisation können nur von Mitgliedskonten und eigenständigen Konten angenommen oder abgelehnt werden. Wenn eine Einladung an ein Mitgliedskonto gesendet wird, sollte dieses Konto die aktuelle Organisation verlassen, bevor die Einladung angenommen wird. Wenn eine Einladung an ein Verwaltungskonto gesendet wird, das bereits einer AWS -Organisation angehört, kann die Einladung erst angenommen werden, wenn alle Mitgliedskonten aus der Organisation entfernt wurden und die Organisation gelöscht wurde.

Mindestberechtigungen

Um eine Einladung zum Beitritt zu einer AWS Organisation anzunehmen oder abzulehnen, benötigen Sie die folgenden Berechtigungen:

- `organizations:ListHandshakesForAccount`— Erforderlich, um die Liste der Einladungen in der AWS Organizations Konsole zu sehen.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— Nur erforderlich, wenn für die Annahme der Einladung eine dienstbezogene Rolle im Mitgliedskonto erstellt werden muss, um die Integration mit anderen AWS Diensten zu unterstützen. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpfte Rollen.

AWS Management Console

Akzeptieren oder Ablehnen einer Einladung

1. Eine Einladung zu einer Organisation wird an die E-Mail-Adresse des Kontoinhabers gesendet. Wenn Sie ein Kontoinhaber sind und eine Einladungs-E-Mail-Nachricht erhalten, befolgen Sie die Anweisungen in der E-Mail-Einladung oder gehen Sie in Ihrem Browser zur AWS Organizations -Konsole und wählen Sie dann Einladungen oder gehen Sie direkt zur Einladungsseite des Mitgliedskontos.
2. Wenn Sie dazu aufgefordert werden, melden Sie sich im eingeladen Konto als IAM-Benutzer an, nehmen Sie eine IAM-Rolle an oder melden Sie sich als Stammbenutzer an (nicht empfohlen).
3. Auf der Einladungsseite des Mitgliedskontos werden die offenen Einladungen Ihres Kontos zum Beitritt zu Organisationen angezeigt.

   Wählen Sie entsprechend Einladung annehmen oder Einladung ablehnen.

   - Wenn Sie im vorherigen Schritt Einladung annehmen auswählen, leitet Sie die Konsole zur Seite Organisationsübersicht mit Details zu der Organisation weiter, der Ihr Konto jetzt angehört. Sie können die ID der Organisation und die E-Mail-Adresse des Inhabers sehen.

     > **Note**
     >
     > Akzeptierte Einladungen werden 30 Tage lang weiterhin in der Liste angezeigt. Danach werden sie gelöscht und nicht mehr in der Liste angezeigt.

AWS Organizations erstellt automatisch eine dienstbezogene Rolle im neuen Mitgliedskonto, um die Integration zwischen AWS Organizations und anderen AWS Diensten zu unterstützen. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpfte Rollen.

AWS sendet eine E-Mail-Nachricht an den Inhaber des Verwaltungskontos der Organisation, dass Sie die Einladung angenommen haben. Außerdem wird eine E-Mail-Nachricht an den Inhaber des Mitgliedskontos gesendet, aus der hervorgeht, dass das Konto jetzt Mitglied der Organisation ist.

- Wenn Sie im vorherigen Schritt Ablehnen ausgewählt haben, bleibt Ihr Konto auf der Seite Einladung für Mitgliedskonten, auf der alle anderen schwebenden Einladungen aufgeführt sind.

  AWS sendet eine E-Mail-Nachricht an den Inhaber des Verwaltungskontos der Organisation, dass Sie die Einladung abgelehnt haben.

  > **Note**
  >
  > Abgelehnte Einladungen werden 30 Tage lang weiterhin in der Liste angezeigt. Danach werden sie gelöscht und nicht mehr in der Liste angezeigt.

AWS CLI & AWS SDKs

Akzeptieren oder Ablehnen einer Einladung

Mit den folgenden Befehlen können Sie Einladungen annehmen oder ablehnen:

- AWS CLI: accept-handshake, decline-handshake

  Im folgenden Beispiel wird gezeigt, wie Sie eine Einladung zum Beitritt einer Organisation annehmen.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
```

```
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

Im folgenden Beispiel wird gezeigt, wie Sie eine Einladung zum Beitritt einer Organisation ablehnen.

- AWS SDKs: AcceptHandshake, DeclineHandshake

Erstellen eines Mitliedskontos Ihrer Organisation

Auf dieser Seite wird beschrieben, wie Sie AWS-Konten innerhalb Ihrer Organisation in AWS Organizations erstellen. Weitere Informationen zu den ersten Schritten mit AWS und zum Erstellen eines einzelnen AWS-Konto finden Sie im Ressourcencenter „Erste Schritte“.

Eine Organisation ist eine Sammlung von AWS-Konten, die Sie zentral verwalten. Sie können die folgenden Verfahren zum Verwalten der Konten Ihrer Organisation ausführen:

- Erstellen eines AWS-Konto, das Teil Ihrer Organisation ist
- Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt

Important

- Wenn Sie ein Mitgliedskonto in Ihrer Organisation erstellen, erstellt AWS Organizations automatisch eine IAM-Rolle (AWS Identity and Access Management) vom Typ `OrganizationAccountAccessRole` im Mitgliedskonto, die es den Benutzern und Rollen im Verwaltungskonto ermöglicht, die volle administrative Kontrolle über das Mitgliedskonto auszuüben. Diese Rolle ist von allen für das Mitgliedskonto geltenden Service-Kontrollrichtlinien (Service Control Policies, SCPs) betroffen.

  AWS Organizations fügt dem Mitgliedskonto auch automatisch eine verwaltete Richtlinie mit der `OrganizationAccountAccessRole`-Rolle hinzu. Dies ermöglicht eine zentrale Steuerung, sodass alle zusätzlichen Konten, die mit derselben verwalteten Richtlinie verbunden sind, automatisch aktualisiert werden, wenn die Richtlinie aktualisiert wird. Zuvor wurde für neue Konten, die in einer Organisation erstellt wurden, eine Inline-Richtlinie hinzugefügt, die nur auf dieses einzelne Konto galt. Weitere Informationen zu Inline-Richtlinien finden Sie unter Verwaltete Richtlinien und Inline-Richtlinien im IAM-Benutzerhandbuch.

  AWS Organizations erstellt außerdem automatisch eine servicegebundene Rolle namens `AWSServiceRoleForOrganizations`, die die Integration mit ausgewählten AWS-Services ermöglicht. Um die Integration zu ermöglichen, müssen Sie die anderen Services konfigurieren. Weitere Informationen finden Sie unter AWS Organizations und serviceverknüpfte Rollen.

- Wenn diese Organisation mit AWS Control Tower verwaltet wird, erstellen Sie Ihre Konten mithilfe der AWS Control Tower-Account-Factory in der AWS Control Tower-Konsole oder in den APIs. Wenn Sie ein Konto in Organisationen erstellen, ist dieses Konto nicht bei AWS Control Tower registriert. Weitere Informationen finden Sie unter Verweisen auf Ressourcen außerhalb von AWS Control Tower im AWS Control Tower-Benutzerhandbuch.

> **Note**
>
> AWS-Konten, die Sie als Teil einer Organisation erstellen, abonnieren nicht automatisch AWS-Marketing-E-Mails. Um Ihre Konten für den Erhalt von Marketing-E-Mails anzumelden, siehe https://pages.awscloud.com/communication-preferences.

Erstellen eines AWS-Konto, das Teil Ihrer Organisation ist

Nachdem Sie sich beim Verwaltungskonto der Organisation angemeldet haben, können Sie Mitgliedskonten erstellen, die automatisch Teil Ihrer Organisation sind. Wenn Sie mit dem folgenden Verfahren ein Konto erstellen, kopiert AWS Organizations automatisch die folgenden Informationen des Hauptkontakts aus dem Verwaltungskonto in das neue Mitgliedskonto:

- Phone number (Telefonnummer)
- Unternehmensname
- Website-URL
- Adresse

Außerdem werden die Kommunikationssprache und die Marketplace-Informationen (in einigen AWS-Regionen der Anbieter des Kontos) aus dem Verwaltungskonto kopiert.

> **Note**
>
> AWS erfasst nicht automatisch alle Informationen, die erforderlich sind, damit ein Konto als eigenständiges Konto funktioniert. Wenn Sie jemals ein Mitgliedskonto aus einer Organisation entfernen und es in ein eigenständiges Konto umwandeln müssen, müssen

Sie diese Informationen für das Konto bereitstellen, bevor Sie es entfernen können. Weitere Informationen finden Sie unter Verlassen einer Organisation in Ihrem Mitgliedskonto.

Mindestberechtigungen

Um ein Mitgliedskonto in Ihrer Organisation zu erstellen, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:CreateAccount`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `iam:CreateServiceLinkedRole` (wird dem Prinzipal `organizations.amazonaws.com` gewährt, um die erforderliche serviceverknüpfte Rolle in den Mitgliedskonten zu erstellen).

AWS Management Console

Erstellen eines AWS-Konto, das automatisch Teil Ihrer Organisation ist

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Klicken Sie auf der AWS-Konten-Seite auf Hinzufügen eines AWS-Konto.
3. Klicken Sie auf der Seite Hinzufügen eines AWS-Konto auf Erstellen eines AWS-Konto (wird standardmäßig ausgewählt).
4. Geben Sie auf der Seite Erstellen eines AWS-Konto unter AWS-Konto-Name den Namen ein, den Sie dem Konto zuweisen möchten. Dieser Name hilft Ihnen, das Konto von anderen Konten der Organisation zu unterscheiden. Es handelt sich nicht um den IAM-Alias oder den E-Mail-Namen des Besitzers.
5. Geben Sie für E-Mail-Adresse des Kontoinhabers die E-Mail-Adresse des Kontoinhabers ein. Diese E-Mail-Adresse kann nicht bereits mit einem anderen AWS-Konto verknüpft sein, da sie zum Benutzernamen für den Stammbenutzer des Kontos wird.
6. (Optional) Geben Sie den Namen ein, der der IAM-Rolle zugewiesen wird, die automatisch in dem neuen Konto erstellt wird. Diese Rolle gewährt dem Verwaltungskonto der

Organisation die Kontoberechtigung zum Zugriff auf das neu erstellte Mitgliedskonto. Wenn Sie keinen Namen angeben, gibt AWS Organizations der Rolle den Standardnamen `OrganizationAccountAccessRole`. Wir empfehlen, den Standardnamen für alle Konten zu verwenden, um Konsistenz zu gewährleisten.

> **Important**
>
> Notieren Sie sich diesen Rollennamen. Sie benötigen ihn später, um Benutzern und Rollen im Verwaltungskonto Zugriff auf das neue Konto zu gewähren.

7. (Optional) Fügen Sie im Abschnitt Tags ein oder mehrere Tags zum neuen Konto hinzu, indem Sie Tag hinzufügen auswählen und dann einen Schlüssel und einen optionalen Wert eingeben. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einem Konto bis zu 50 Tags hinzufügen.
8. Wählen Sie Create (Erstellen)AWS-Konto aus.

   - Wenn Sie eine Fehlermeldung erhalten, die darauf hinweist, dass Sie Ihr Kontokontingent für die Organisation überschritten haben, lesen Sie Ich erhalte eine Meldung „Kontingent überschritten“, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen..
   - Wenn Sie eine Fehlermeldung erhalten, die darauf hinweist, dass Sie ein Konto nicht hinzufügen können, weil Ihre Organisation noch initialisiert wird, warten Sie eine Stunde, und versuchen Sie es dann erneut.
   - Sie können auch die AWS CloudTrail-Protokolle auf Informationen darüber prüfen, ob die Kontoerstellung erfolgreich war. Weitere Informationen finden Sie unter Protokollieren und Überwachen in AWS Organizations.
   - Wenn das Problem weiterhin besteht, wenden Sie sich bitte an AWS Support.

   Die AWS-Konten-Seite wird angezeigt und Ihr neues Konto wird der Liste hinzugefügt.
9. Da das Konto nun vorhanden ist und eine IAM-Rolle hat, die einen administrativen Zugriff für Benutzer im Verwaltungskonto zulässt, können Sie dem Konto über die Schritte unter Zugriff auf Mitgliedskonten in Ihrer Organisation Zugriff gewähren.

> **Note**
>
> Wenn Sie ein Konto erstellen, weist AWS Organizations dem Stammbenutzer zunächst ein langes (64 Zeichen), komplexes, zufällig generiertes Passwort zu. Sie können

dieses anfängliche Passwort nicht abrufen. Um als Stammbenutzer erstmals auf das Konto zugreifen zu können, müssen Sie den Prozess für die Passwortwiederherstellung ausführen. Weitere Informationen finden Sie unter Zugreifen auf ein Mitgliedskonto als Root-Benutzer.

AWS CLI & AWS SDKs

Erstellen eines AWS-Konto, das automatisch Teil Ihrer Organisation ist

Sie können einen der folgenden Befehle verwenden, um ein Konto zu erstellen:

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
}
```

Sie können den Status der Kontoerstellung mithilfe des folgenden Befehls überprüfen.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWS-SDKs: CreateAccount

Zugriff auf Mitgliedskonten in Ihrer Organisation

Wenn Sie ein Konto in Ihrer Organisation erstellen, erstellt zusätzlich zum StammbenutzerAWS Organizations automatisch eine IAM-Rolle, die standardmäßig `OrganizationAccountAccessRole` benannt ist. Sie können einen anderen Namen angeben, wenn Sie ihn erstellen. Es wird jedoch empfohlen, ihn konsistent für alle Konten zu benennen. Wir verweisen in diesem Handbuch mit dem Standardnamen auf diese Rolle. AWS Organizations erstellt allerdings keine anderen Benutzer oder Rollen. Um auf die Konten innerhalb Ihrer Organisation zugreifen zu können, müssen Sie eines der folgenden Verfahren durchführen:

- Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch. Weitere Sicherheitsempfehlungen für Root-Benutzer finden Sie unter Bewährte Methoden für Root-Benutzer für Ihren AWS-Konto.
- Wenn Sie ein Konto mithilfe der als Teil von AWS Organizations bereitgestellten Tools erstellen, können Sie über die in allen so erstellten neuen Konten vorhandene vorkonfigurierte Rolle namens `OrganizationAccountAccessRole` auf das Konto zugreifen. Weitere Informationen finden Sie unter Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt.
- Wenn Sie ein vorhandenes Konto zum Beitritt zu Ihrer Organisation einladen und das Konto diese Einladung annimmt, haben Sie die Möglichkeit, eine IAM-Rolle zu erstellen, die dem Verwaltungskonto den Zugriff auf das eingeladene Mitgliedskonto gewährt. Diese Rolle soll mit der Rolle identisch sein, die automatisch einem Konto hinzugefügt wird, das mit AWS Organizations erstellt wird. Informationen zum Erstellen dieser Rolle finden Sie unter Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto. Nach dem Erstellen der Rolle können Sie mit den Schritten in Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt zugreifen.
- Verwenden Sie AWS IAM Identity Center und aktivieren Sie den vertrauenswürdigen Zugriff für IAM Identity Center mit AWS Organizations. Dadurch können sich Benutzer mit ihren Unternehmens-Anmeldeinformationen beim AWS-Zugriffsportal anmelden und auf Ressourcen in den ihnen zugewiesenen Verwaltungs- oder Mitgliedskonten zugreifen.

Weitere Informationen finden Sie unter Berechtigungen für mehrere Konten im Benutzerhandbuch von AWS IAM Identity Center. Weitere Informationen zum Einrichten des vertrauenswürdigen Zugriffs für IAM Identity Center finden Sie unter AWS IAM Identity Center und AWS Organizations.

Mindestberechtigungen

Um von einem anderen Konto in Ihrer Organisation auf ein AWS-Konto zuzugreifen, benötigen Sie die folgende Berechtigung:

- `sts:AssumeRole` – Das `Resource`-Element muss entweder auf ein Sternchen (*) oder auf die Konto-ID-Nummer des Kontos des Benutzers festgelegt sein, der auf das neue Mitgliedskonto zugreifen muss

Zugreifen auf ein Mitgliedskonto als Root-Benutzer

Wenn Sie ein neues Konto erstellen, weist AWS Organizations dem Stammbenutzer zunächst ein Passwort zu, das mindestens 64 Zeichen lang ist. Alle Zeichen werden zufällig generiert, ohne Garantie, dass bestimmte Zeichensätze vorkommen. Sie können dieses anfängliche Passwort nicht abrufen. Um als Stammbenutzer erstmals auf das Konto zugreifen zu können, müssen Sie den Prozess für die Passwortwiederherstellung ausführen. Weitere Informationen finden Sie unter Ich habe mein Root-Benutzerpasswort für mein vergessen AWS-Konto im AWS Benutzerhandbuch für die Anmeldung.

Hinweise

- Als bewährte Methode wird empfohlen, den Root-Benutzer nur für den Zugriff auf Ihr Konto zu nutzen, um andere Benutzer und Rollen mit eingeschränkteren Berechtigungen zu erstellen. Melden Sie sich dann als einer dieser neuen Benutzer oder Rollen an.
- Außerdem empfehlen wir, Multi-Factor-Authentifizierung (MFA) für den Root-Benutzer zu aktivieren. Setzen Sie das Passwort zurück und ordnen Sie dem Stammbenutzer ein MFA-Gerät zu.
- Wenn Sie ein Mitgliedskonto in einer Organisation mit einer falschen E-Mail-Adresse erstellt haben, können Sie sich beim Konto nicht als Root-Benutzer anmelden. Wenden Sie sich an AWS Billing and Support .

Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto

Wenn Sie ein Mitgliedskonto als Teil Ihrer Organisation erstellen, erstellt AWS standardmäßig automatisch eine Rolle im Konto, die IAM-Benutzern im Verwaltungskonto, die die Rolle übernehmen können, Administratorberechtigungen erteilt. Standardmäßig hat diese Rolle den Namen `OrganizationAccountAccessRole`. Weitere Informationen finden Sie unter Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt.

Für Mitgliedskonten allerdings, die Sie zum Beitritt zur Organisation einladen, wird nicht automatisch eine Admin-Rolle erstellt. Sie müssen dies, wie in der folgenden Prozedur gezeigt, manuell erledigen. Die Prozedur dupliziert die automatisch für erstellte Konten eingerichtete Rolle. Wir empfehlen, dass Sie aus Konsistenzgründen und zur leichteren Erkennbarkeit denselben Namen (`OrganizationAccountAccessRole`) für Ihre manuell erstellten Rollen nutzen.

AWS Management Console

Erstellen einer AWS Organizations-Administrator-Rolle in ein Mitgliedskonto

1. Melden Sie sich unter https://console.aws.amazon.com/iam/ bei der IAM-Konsole an. Sie müssen sich im Mitgliedskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Stammbenutzer anmelden (nicht empfohlen). Der Benutzer oder die Rolle muss über die Berechtigung zum Erstellen von IAM-Rollen und Richtlinien verfügen.
2. Navigieren Sie in der IAM-Konsole zu Rollen und wählen Sie dann Rolle erstellen aus.
3. Wählen Sie AWS-Kontound dann Anderes ausAWS-Konto.
4. Geben Sie die 12-stellige Konto-ID-Nummer des Verwaltungskontos ein, für das Sie Administratorzugriff gewähren möchten. Beachten Sie unter Optionen Folgendes:

   - Da die Konten in Ihrem Unternehmen intern sind, sollten Sie für diese Rolle nicht die Option Externe ID erforderlich auswählen. Weitere Informationen zur Option für externe IDs finden Sie unter Wann sollte ich eine externe ID verwenden? im IAM-Benutzerhandbuch.
   - Wenn Sie MFA aktiviert und konfiguriert haben, können Sie optional eine Authentifizierung mithilfe eines Multi-Factor Authentication (MFA)-Geräts festlegen. Weitere Informationen zu MFA finden Sie unter Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.
5. Wählen Sie Weiter aus.

6. Wählen Sie auf der Seite Berechtigungen hinzufügen die AWS verwaltete Richtlinie mit dem Namen `AdministratorAccess` und dann Weiter aus.
7. Geben Sie auf der Seite Name, Überprüfung und Erstellung einen Rollennamen und eine optionale Beschreibung an. Wir empfehlen, dass Sie zur Übereinstimmung mit dem Standardnamen für die Rolle in neuen Konten den Namen „`OrganizationAccountAccessRole`“ verwenden. Wählen Sie Create Role (Rolle erstellen) aus, um Ihre Änderungen zu übernehmen.
8. Die neue Rolle erscheint in der Liste der verfügbaren Rollen. Wählen Sie den Namen der neuen Rolle aus, um die Details anzuzeigen. Beachten Sie dabei besonders die angegebene Link-URL. Geben Sie diese URL an die Benutzer im Mitgliedskonto weiter, die Zugriff auf die Rolle benötigen. Notieren Sie sich außerdem den Role ARN (Rollen-ARN). Sie benötigen ihn in Schritt 15.
9. Melden Sie sich unter https://console.aws.amazon.com/iam/ bei der IAM-Konsole an. Melden Sie sich jetzt als derjenige Benutzer im Verwaltungskonto an, der die Berechtigungen zur Erstellung von Richtlinien hat, und weisen Sie die Richtlinien für die Benutzer oder Gruppen zu.
10. Navigieren Sie zu Richtlinien und wählen Sie dann Richtlinie erstellen aus.
11. Wählen Sie unter Service die Option STS aus.
12. Für Actions geben Sie **`AssumeRole`** in das Feld Filter ein und aktivieren Sie dann das Kontrollkästchen daneben, wenn es angezeigt wird.
13. Stellen Sie unter Ressourcen sicher, dass Spezifisch ausgewählt ist, und wählen Sie dann ARNs hinzufügen aus.
14. Geben Sie Ihre AWS-Mitgliedskonto-ID-Nummer und dann den Namen der Rolle ein, die Sie zuvor in den Schritten 1–8 erstellt haben. Wählen Sie Add ARNs (ARNs hinzufügen) aus.
15. Wenn Sie die Berechtigung zur Übernahme der Rolle in mehreren Mitgliedskonten erteilen, wiederholen Sie die Schritte 14 und 15 für jedes Konto.
16. Wählen Sie Weiter aus.
17. Geben Sie auf der Seite Überprüfen und erstellen einen Namen für die neue Richtlinie ein und wählen Sie dann Richtlinie erstellen aus, um Ihre Änderungen zu speichern.
18. Wählen Sie im Navigationsbereich Benutzergruppen und dann den Namen der Gruppe (nicht das Kontrollkästchen), die Sie zum Delegieren der Verwaltung des Mitgliedskontos verwenden möchten.
19. Wählen Sie die Registerkarte Berechtigungen.

20. Wählen Sie Berechtigungen hinzufügen, wählen Sie Richtlinien anfügen und wählen Sie dann die Richtlinie aus, die Sie in den Schritten 11–18 erstellt haben.

Die Benutzer, die Mitglieder der ausgewählten Gruppe sind, können nun die in Schritt 9 abgerufenen URLs für den Zugriff auf die Rolle der Mitgliedskonten nutzen. Sie können auf diese Mitgliedskonten so zugreifen wie beim Zugriff auf ein in der Organisation erstelltes Konto. Weitere Informationen über die Verwendung der Rolle zur Administration eines Mitgliedskontos finden Sie unter Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt.

Zugreifen auf ein Mitgliedskonto, das über eine Verwaltungskonto-Zugriffsrichtlinie verfügt

Wenn Sie ein Mitgliedskonto mit der AWS Organizations-Konsole erstellen, erstellt AWS Organizations automatisch eine IAM-Rolle namens `OrganizationAccountAccessRole` im Konto. Diese Rolle hat volle administrative Berechtigungen im Mitgliedskonto. Der Zugriffsumfang für diese Rolle umfasst alle Hauptbenutzer im Verwaltungskonto, sodass die Rolle so konfiguriert ist, dass sie diesen Zugriff auf das Verwaltungskonto der Organisation gewährt. Sie können eine identische Rolle für ein eingeladenes Mitgliedskonto erstellen, indem Sie entsprechend der Schritte in Erstellen der OrganizationAccountAccessRole in einem eingeladenen Mitgliedskonto vorgehen. Um diese Rolle für den Zugriff auf das Mitgliedskonto zu verwenden, müssen Sie sich als Benutzer des Verwaltungskonto anmelden, das Berechtigungen zur Annahme der Rolle hat. Führen Sie das folgende Verfahren aus, um diese Berechtigungen zu konfigurieren. Wir empfehlen, dass Sie Berechtigungen zu Gruppen statt zu Benutzern zuweisen. Dies vereinfacht die Wartung.

AWS Management Console

Erteilen von Berechtigungen zum Zugriff auf die Rolle für Mitglieder einer IAM-Gruppe im Verwaltungskonto

1. Melden Sie sich bei der IAM-Konsole unter https://console.aws.amazon.com/iam/ als Benutzer mit Administratorrechten im Verwaltungskonto an. Dies ist erforderlich, um Berechtigungen zu der IAM-Gruppe zuzuweisen, deren Benutzer auf die Rolle im Mitgliedskonto zugreifen.
2. Erstellen Sie zunächst die verwaltete Richtlinie, die Sie später in ??? benötigen.

   Wählen Sie im Navigationsbereich Policies (Richtlinien) und dann Create policy (Richtlinie erstellen) aus.

3. Wählen Sie auf der Registerkarte „Visual Editor (Visueller Editor)“ die Option Choose a service (Service auswählen) aus, geben Sie **`STS`** in das Suchfeld ein, um die Liste zu filtern, und wählen Sie anschließend die Option STS aus.
4. Geben Sie im Abschnitt Aktionen **`assume`** in das Suchfeld ein, um die Liste zu filtern, und wählen Sie dann die AssumeRole Option aus.
5. Wählen Sie im Abschnitt Ressourcen die Option Spezifisch aus, wählen Sie ARNs hinzufügen und geben Sie dann die Mitgliedskontonummer und den Namen der Rolle ein, die Sie im vorherigen Abschnitt erstellt haben (wir empfehlen, sie zu benennen`OrganizationAccountAccessRole`).
6. Wählen Sie ARNs hinzufügen, wenn das Dialogfeld den richtigen ARN anzeigt.
7. (Optional) Wenn Sie eine Multi-Factor Authentication (MFA) anfordern oder den Zugriff auf die Rolle aus einem angegebenen IP-Adressbereich einschränken möchten, erweitern Sie den Abschnitt „Request conditions (Anforderungsbedingungen)“ und wählen die Optionen aus, die Sie durchsetzen möchten.
8. Wählen Sie Weiter aus.
9. Geben Sie auf der Seite Überprüfen und erstellen einen Namen für die neue Richtlinie ein. Beispiel: **`GrantAccessToOrganizationAccountAccessRole`**. Optional können Sie auch eine Beschreibung eingeben.
10. Wählen Sie Create policy (Richtlinie erstellen) aus, um die neue verwaltete Richtlinie zu speichern.
11. Da die Richtlinie jetzt verfügbar ist, können Sie diese einer Gruppe anfügen.

    Wählen Sie im Navigationsbereich Benutzergruppen und dann den Namen der Gruppe (nicht das Kontrollkästchen) aus, deren Mitglieder Sie die Rolle im Mitgliedskonto übernehmen möchten. Falls erforderlich, können Sie eine neue Gruppe erstellen.
12. Wählen Sie die Registerkarte Permissions (Berechtigungen), wählen Sie Add permissions (Berechtigungen hinzufügen) und wählen Sie dann Attach policies (Richtlinien anhängen).
13. (Optional) Sie können im Feld Search (Suchen) mit der Eingabe des Namens Ihrer Richtlinie beginnen, um die Liste zu filtern, bis Ihnen der Name der Richtlinie angezeigt wird, die Sie gerade in Step 2 über Step 10 erstellt haben. Sie können auch alle AWS verwalteten Richtlinien herausfiltern, indem Sie Alle Typen und dann Kundenverwaltet auswählen.
14. Aktivieren Sie das Kontrollkästchen neben Ihrer Richtlinie und wählen Sie dann Richtlinien anfügen aus.

IAM-Benutzer, die Mitglied der Gruppe sind, haben jetzt Berechtigungen zum Wechseln zu der neuen Rolle in der AWS Organizations-Konsole; durch Ausführen der nachfolgenden Schritte.

AWS Management Console

So wechseln Sie zur Rolle für das Mitgliedskonto

Wenn er die Rolle verwendet, hat der Benutzer Administratorberechtigungen im neuen Mitgliedskonto. Weisen Sie Ihre IAM-Benutzer an, die Mitglieder der Gruppe sind, die folgenden Schritte auszuführen, um zur neuen Rolle zu wechseln.

1. Wählen Sie in der rechten oberen Ecke der AWS Organizations-Konsole den Link aus, der Ihren aktuellen Anmeldenamen enthält, und wählen Sie dann Rolle wechseln aus.
2. Geben Sie die von Ihrem Administrator erhaltene Konto-ID und den Rollennamen ein.
3. Geben Sie unter Display Name (Anzeigename) den Text ein, der während der Verwendung der Rolle in der Navigationsleiste in der oberen rechten Ecke statt Ihres Benutzernamens angezeigt werden soll. Optional können Sie eine Farbe auswählen.
4. Wählen Sie Switch Role. Nun werden alle von Ihnen ausgeführten Aktionen mit den für die gewählte Rolle gewährten Berechtigungen ausgeführt. Solange Sie nicht zurück wechseln, müssen die Berechtigungen nicht Ihrem ursprünglichen IAM-Benutzer zugewiesen werden.
5. Nach der Ausführung von Aktionen, für die Sie die Berechtigungen der Rolle benötigen, können Sie zum normalen IAM-Benutzer zurückwechseln. Wählen Sie den Rollennamen in der oberen rechten Ecke (unabhängig davon, was Sie als Anzeigename angegeben haben) und dann Zurück zu aus***UserName***.

Weitere Ressourcen

- Weitere Informationen zum Erteilen von Berechtigungen zum Wechseln von Rollen finden Sie unter Erteilen von Berechtigungen an einen Benutzer zum Wechseln von Rollen im IAM-Benutzerhandbuch.
- Weitere Informationen zur Verwendung einer Rolle, für deren Übernahme Ihnen Berechtigungen erteilt wurden, finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.
- Ein Tutorial zur Verwendung von Rollen für den kontoübergreifenden Zugriff finden Sie unter Tutorial: Delegieren des Zugriffs in mithilfe AWS-Konten von IAM-Rollen im IAM-Benutzerhandbuch.

- Weitere Informationen zum Schließen von AWS-Konten finden Sie unter So schließen Sie ein Mitliedskonto Ihrer Organisation.

Exportieren von AWS-Konto-Details für Ihre Organisation

Mit AWS Organizations können Verwaltungskontobenutzer und delegierte Administratoren für eine Organisation eine .csv-Datei mit allen Kontodetails innerhalb einer Organisation exportieren. Infolgedessen können Organisationsadministratoren Konten einfach anzeigen und nach Status filtern: `ACTIVE`, `SUSPENDED` oder `PENDING`. Wenn Ihre Organisation über viele Konten verfügt, bietet die Download-Option einer .csv-Datei eine einfache Möglichkeit, Kontodetails in einer Tabelle anzuzeigen und zu sortieren.

Zuvor bestand die einzige Möglichkeit, Konten anzuzeigen, darin, sich die Kontohierarchie oder Listenanzeige in der AWS Organizations-Konsole anzeigen zu lassen.

> **Note**
>
> Nur Hauptbenutzer im Verwaltungskonto können die Kontoliste herunterladen.

Exportieren einer Liste aller AWS-Konten in Ihrer Organisation

Wenn Sie sich beim Verwaltungskonto der Organisation anmelden, können Sie eine Liste aller Konten, die zu Ihrer Organisation gehören, als .csv-Datei erhalten. Die Liste enthält einzelne Kontodetails, gibt jedoch nicht an, zu welcher Organisationseinheit (OU) das Konto gehört.

Die CSV-Datei enthält die folgenden Informationen für jedes Konto:

- Konto-ID – Numerische Konto-ID Zum Beispiel: 123456789012.
- ARN – Amazon-Ressourcenname für das Konto. Beispiel: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- E-Mail – Die E-Mail-Adresse des Mitgliedskontos. Zum Beispiel: marymajor@example.com
- Name - Kontoname, der vom Kontoersteller bereitgestellt wird. Zum Beispiel: Stage-Test-Konto
- Status – Kontostatus innerhalb der Organisation. Werte können folgende sein: `PENDING`, `ACTIVE` oder `SUSPENDED`.
- Beitrittsmethode – Gibt an, wie das Konto erstellt wurde. Der Wert kann `INVITED` oder `CREATED` sein.

- Beitrittszeitstempel – Datum und Uhrzeit, zu der das Konto der Organisation beigetreten ist.

> **Mindestberechtigungen**
>
> Um eine .csv-Datei aller Mitgliedskonten in Ihrer Organisation zu exportieren, müssen Sie über die folgenden Berechtigungen verfügen:
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

So exportieren Sie eine .csv-Datei für alle AWS-Konten in Ihrer Organisation

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Klicken Sie auf Aktionen und wählen Sie dann für AWS-Konto die Option Kontoliste exportierenaus. Das blaue Banner oben auf der Seite zeigt an, dass der Exportvorgang läuft.
3. Wenn die Datei fertig ist, wird das Banner grün und zeigt an, dass der Download fertig ist. Wählen Sie CSV herunterladen aus. Die Datei `Organization_accounts_information.csv` wird auf Ihr Gerät heruntergeladen.

AWS CLI & AWS SDKs

Die einzige Möglichkeit, die .csv-Datei mit Kontodetails zu exportieren, besteht darin, die AWS Management Console zu verwenden. Sie können die .csv-Datei der Kontoliste nicht mithilfe der AWS CLI exportieren.

Entfernen eines Mitgliedskontos aus Ihrer Organisation

Bei der Verwaltung von Konten in einer Organisation werden Mitgliedskonten entfernt, die nicht mehr benötigt werden. Wenn ein Mitgliedskonto entfernt wird, wird das Konto nicht geschlossen, sondern aus der Organisation entfernt. Das ehemalige Mitgliedskonto wird zu einem eigenständigen AWS-Konto-Konto, das nicht mehr von AWS Organizations verwaltet wird. Danach unterliegt das

Konto keinen Richtlinien mehr und ist für die Zahlung der eigenen Rechnungen zuständig. Dem Verwaltungskonto der Organisation werden keine Kosten mehr in Rechnung gestellt, die für das Konto angefallen sind, nachdem es aus der Organisation entfernt wurde.

Weitere Informationen zum Entfernen des Verwaltungskontos finden Sie unter Löschen einer Organisation.

Themen

- Überlegungen vor dem Entfernen eines Kontos aus einer Organisation
- Entfernen eines Mitgliedskontos aus Ihrer Organisation
- Verlassen einer Organisation in Ihrem Mitgliedskonto

Überlegungen vor dem Entfernen eines Kontos aus einer Organisation

Bevor Sie ein Konto entfernen, müssen Sie unbedingt Folgendes berücksichtigen:

- Sie können ein Konto nur dann aus Ihrer Organisation entfernen, wenn es über die erforderlichen Informationen verfügt, um als eigenständiges Konto zu funktionieren. Wenn Sie über die AWS Organizations-Konsole, die API oder AWS CLI-Befehle ein Konto in einer Organisation erstellen, werden nicht automatisch alle für eigenständige Konten erforderlichen Informationen erfasst. Sie müssen für jedes Konto, das Sie als eigenständig einrichten möchten die erforderlichen Kontaktinformationen angeben und verifizieren sowie eine aktuelle Zahlungsmethode angeben. AWS verwendet die Zahlungsmethode, um alle gebührenpflichtigen AWS-Aktivitäten (d. h. alle Aktivitäten, die nicht auf dem kostenlosen AWS-Kontingent ausgeführt werden) abzurechnen, die ausgeführt werden, wenn das Konto nicht mit einer Organisation verbunden ist. Um ein Konto zu entfernen, das noch nicht über diese Informationen verfügt, befolgen Sie die Schritte unter Verlassen einer Organisation in Ihrem Mitgliedskonto.
- Um ein Konto zu entfernen, das Sie in der Organisation erstellt haben, müssen Sie bis mindestens sieben Tage nach der Erstellung des Kontos warten. Eingeladene Konten unterliegen dieser Wartezeit nicht.
- In dem Moment, in dem das Konto die Organisation erfolgreich verlässt, haftet der Besitzer des AWS-Konto für alle neu angefallenen AWS-Kosten und die Zahlungsweise des Kontos wird verwendet. Das Verwaltungskonto der Organisation ist nicht mehr verantwortlich.
- Das Konto, das Sie entfernen möchten, darf kein delegiertes Administratorkonto für einen AWS-Dienst sein, der für Ihre Organisation aktiviert ist. Wenn es sich bei dem Konto um einen delegierten Administrator handelt, müssen Sie zuerst das delegierte Administratorkonto in ein

anderes Konto ändern, das in der Organisation verbleibt. Weitere Informationen zum Deaktivieren oder Ändern des Kontos für einen delegierten Administrator für einen AWS-Service finden Sie in der Dokumentation für diesen Service.

- Auch nach dem Entfernen erstellter Konten (Konten, die mit der AWS Organizations-Konsole oder der `CreateAccount`-API erstellt wurden) aus einer Organisation (i) unterliegen erstellte Konten den Bestimmungen der Vereinbarung zwischen Ihnen und uns über die Erstellung eines Verwaltungskontos und (ii) bleibt das erstellende Verwaltungskonto gesamtschuldnerisch für alle Handlungen haftbar, die über die erstellten Konten ausgeführt werden. Kundenverträge mit uns sowie die Rechte und Pflichten aus diesen Verträgen dürfen ohne unsere vorherige Zustimmung weder abgetreten noch übertragen werden. Um unsere Zustimmung einzuholen, wenden Sie sich an AWS.
- Wenn ein Mitgliedskonto eine Organisation verlässt, hat das Konto keinen Zugriff mehr auf Kosten- und Nutzungsdaten aus dem Zeitraum, als das Konto ein Mitglied der Organisation war. Das Verwaltungskonto der Organisation kann jedoch weiterhin auf die Daten zugreifen. Wenn das Konto der Organisation wieder beitritt, kann das Konto wieder auf die Daten zugreifen.
- Wenn ein Mitgliedskonto eine Organisation verlässt, werden alle dem Konto zugeordneten Tags gelöscht.
- Wenn Sie ein Mitgliedskonto aus der Organisation entfernen, werden alle IAM-Rollen, die erstellt wurden, um den Zugriff durch das Verwaltungskonto der Organisation zu ermöglichen, nicht automatisch gelöscht. Wenn Sie diesen Zugriff vom Verwaltungskonto der früheren Organisation beenden möchten, müssen Sie die IAM-Rolle manuell löschen. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

Auswirkungen der Entfernung eines Kontos aus einer Organisation

Wenn Sie ein Konto aus einer Organisation entfernen, werden keine direkten Änderungen am Konto vorgenommen. Es gibt jedoch die folgenden indirekten Auswirkungen:

- Das Konto muss jetzt seine eigenen Gebühren bezahlen und über eine gültige Zahlungsweise verfügen, die dem Konto zugewiesen ist.
- Die Prinzipale im Konto sind nicht mehr von Richtlinien betroffen, die in der Organisation angewendet wurden. Das bedeutet, dass die Einschränkungen durch diese SCPs nicht mehr gültig sind. Außerdem haben die Benutzer und Rollen im Konto ggf. mehr Berechtigungen als zuvor. Andere Organisationsrichtlinientypen können nicht mehr erzwungen oder verarbeitet werden.

- Wenn Sie den Bedingungsschlüssel `aws:PrincipalOrgID` in Richtlinien verwenden, um den Zugriff auf nur Benutzer und Rollen von AWS-Konten in Ihrer Organisation zu beschränken, sollten Sie diese Richtlinien überprüfen und möglicherweise aktualisieren, bevor Sie das Mitgliedskonto entfernen. Wenn Sie die Richtlinien nicht aktualisieren, verlieren Benutzer und Rollen im Konto möglicherweise den Zugriff auf die Ressourcen, wenn das Konto die Organisation verlässt.
- Die Integration mit anderen Services wird möglicherweise deaktiviert. Wenn Sie ein Konto aus einer Organisation entfernen, für die die Integration mit einem AWS-Service aktiviert ist, können die Benutzer in diesem Konto diesen Service nicht mehr verwenden.

Entfernen eines Mitgliedskontos aus Ihrer Organisation

Wenn Sie sich am Verwaltungskonto der Organisation anmelden, können Sie Mitgliedskonten, die Sie nicht mehr benötigen, aus der Organisation entfernen. Um dies zu tun, führen Sie die folgenden Schritte aus. Dieses Verfahren gilt nur für Mitgliedskonten. Um das Verwaltungskonto zu entfernen, müssen Sie die Organisation löschen.

> **Note**
>
> Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, gelten Organisationsvereinbarungen für dieses Konto nicht mehr. Verwaltungskonto-Administratoren sollten Mitgliedskonten hiervon benachrichtigen, bevor sie die Konten aus der Organisation entfernen, so dass die Mitgliedskonten nötigenfalls neue Vereinbarungen einrichten können. Eine Liste der aktiven Organisationsvereinbarungen kann in der AWS Artifact-Konsole auf der Seite AWS Artifact-Organisationsvereinbarungen angezeigt werden.

> **Mindestberechtigungen**
>
> Um einzelne oder mehrere Mitgliedskonten entfernen zu können, müssen Sie als Benutzer oder Rolle beim Verwaltungskonto angemeldet sein und über folgende Berechtigungen verfügen:
>
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:RemoveAccountFromOrganization`

Wenn Sie sich in Schritt 5 als Benutzer oder Rolle bei einem Mitgliedskonto anmelden, muss dieser Benutzer oder diese Rolle über folgende Berechtigungen verfügen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:LeaveOrganization` – Beachten Sie, dass der Administrator der Organisation eine Richtlinie auf Ihr Konto anwenden kann, mit der diese Berechtigung entfernt wird, sodass Sie Ihr Konto nicht aus der Organisation entfernen können.
- Wenn Sie sich als IAM-Benutzer anmelden und dem Konto Zahlungsinformationen fehlen, muss der Benutzer entweder über `aws-portal:ModifyBilling` und `aws-portal:ModifyPaymentMethods` Berechtigungen (wenn das Konto noch nicht zu detaillierten Berechtigungen migriert wurde) ODER über `payments:CreatePaymentInstrument` und `payments:UpdatePaymentPreferences` Berechtigungen (wenn das Konto zu detaillierten Berechtigungen migriert wurde) verfügen. Außerdem muss für das Mitgliedskonto ein IAM-Benutzerzugriff auf die Abrechnung aktiviert sein. Wenn dies nicht bereits aktiviert ist, finden Sie weitere Informationen unter Den Zugriff auf die Fakturierung und Kostenmanagement-Konsole aktivieren im AWS Billing-Benutzerhandbuch.

AWS Management Console

Entfernen eines Mitgliedskontos aus Ihrer Organisation

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite AWS-Konten das Kontrollkästchen☑ neben jedem Mitgliedskonto, das Sie aus Ihrer Organisation entfernen möchten, und aktivieren Sie es. Sie können in der OU-Hierarchie navigieren oder Nur AWS-Konten anzeigen aktivieren, um eine flache Liste von Konten ohne die OU-Struktur anzuzeigen. Wenn Sie viele Konten haben, müssen Sie möglicherweise unten in der Liste Weitere Konten in 'ou-name' laden auswählen, um alle Konten zu finden, die Sie verschieben möchten.

Suchen Sie auf der Seite AWS-Konten den Namen des Mitgliedskontos, das Sie aus Ihrer Organisation entfernen möchten, und wählen Sie ihn aus. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ), um das gewünschte Konto zu finden.

3. Wählen Sie Aktionen und dann unter AWS-Konto die Option Aus Organisation entfernen aus.
4. Wählen Sie unter Konto 'account-name' (#account-id-num) aus der Organisation entfernen? im Dialogfeld Konto entfernen aus.
5. Wenn es AWS Organizations nicht gelingt, eines oder mehrere der Konten zu entfernen, liegt dies in der Regel daran, dass Sie nicht alle erforderlichen Informationen zur Verfügung gestellt haben, damit das Konto als eigenständiges Konto betrieben werden kann. Führen Sie die folgenden Schritte aus:

   a. Melden Sie sich den fehlgeschlagenen Konten an. Wir empfehlen Ihnen, sich beim Mitgliedskonto anzumelden, indem Sie Copy link auswählen und ihn dann in die Adressleiste eines neuen Inkognito-Browserfensters einfügen. Wenn Sie kein Inkognito-Fenster verwenden, sind Sie vom Verwaltungskonto abgemeldet und können nicht mehr zu diesem Dialogfeld zurücknavigieren.

   b. Der Browser führt Sie direkt zum Anmeldevorgang, um die für dieses Konto fehlenden Schritte abzuschließen. Führen Sie alle aufgeführten Schritte aus. Dazu kann Folgendes gehören:

      - Kontaktinformationen bereitstellen
      - Gültige Zahlungsmethode angeben
      - Telefonnummer bestätigen
      - Support-Plan auswählen

   c. Nachdem Sie den letzten Anmeldeschritt abgeschlossen haben, leitet AWS Ihren Browser automatisch auf die AWS Organizations-Konsole für das Mitgliedskonto um. Wählen Sie Leave organization aus und bestätigen Sie Ihre Wahl im Bestätigungsdialog. Sie werden zur Seite Getting Started der AWS Organizations-Konsole weitergeleitet. Hier können Sie alle ausstehenden Einladungen für Ihr Konto zum Beitritt zu anderen Organisationen sehen.

   d. Entfernen Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation.

> **Important**
>
> Wenn Ihr Konto in der Organisation erstellt wurde, hat Organizations automatisch eine IAM-Rolle in dem Konto erstellt, mit dem der Zugriff durch das Verwaltungskonto der Organisation aktiviert wurde. Wenn das Konto zum Beitritt eingeladen wurde, hat Organizations eine solche Rolle nicht automatisch erstellt, allerdings haben möglicherweise Sie oder ein anderer Administrator eine entsprechende Rolle erstellt, um dieselben Vorteile zu erhalten. In beiden Fällen wird beim Entfernen des Kontos aus der Organisation eine solche Rolle nicht automatisch gelöscht. Wenn Sie diesen Zugriff aus dem Verwaltungskonto der früheren Organisation beenden möchten, müssen Sie diese IAM-Rolle manuell löschen. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

AWS CLI & AWS SDKs

Entfernen eines Mitgliedskontos aus Ihrer Organisation

Sie können einen der folgenden Befehle verwenden, um ein Mitgliedskonto zu entfernen:

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-SDKs: RemoveAccountFromOrganization

Nachdem das Mitgliedskonto aus der Organisation entfernt wurde, stellen Sie sicher, dass Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation.

> **Important**
>
> Wenn Ihr Konto in der Organisation erstellt wurde, hat Organizations automatisch eine IAM-Rolle in dem Konto erstellt, mit dem der Zugriff durch das Verwaltungskonto der Organisation aktiviert wurde. Wenn das Konto zum Beitritt eingeladen wurde,

hat Organizations eine solche Rolle nicht automatisch erstellt, allerdings haben möglicherweise Sie oder ein anderer Administrator eine entsprechende Rolle erstellt, um dieselben Vorteile zu erhalten. In beiden Fällen wird beim Entfernen des Kontos aus der Organisation eine solche Rolle nicht automatisch gelöscht. Wenn Sie diesen Zugriff aus dem Verwaltungskonto der früheren Organisation beenden möchten, müssen Sie diese IAM-Rolle manuell löschen. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

Mitgliedskonten können sich stattdessen mit leave-organization selbst entfernen. Weitere Informationen finden Sie unter Verlassen einer Organisation in Ihrem Mitgliedskonto.

Verlassen einer Organisation in Ihrem Mitgliedskonto

Wenn Sie an einem Konto angemeldet sind, können Sie dieses Konto aus der entsprechenden Organisation entfernen. Um dies zu tun, führen Sie die folgenden Schritte aus. Dieses Verfahren gilt nur für Mitgliedskonten. Das Verwaltungskonto darf die Organisation nicht mittels dieser Methode verlassen. Um das Verwaltungskonto zu entfernen, müssen Sie die Organisation löschen.

Note

Der Status eines Kontos bei einer Organisation wirkt sich darauf aus, welche Kosten- und Nutzungsdaten angezeigt werden:

- Wenn ein Mitgliedskonto eine Organisation verlässt und ein eigenständiges Konto wird, hat das Konto keinen Zugriff mehr auf Kosten- und Nutzungsdaten aus dem Zeitraum, als das Konto ein Mitglied der Organisation war. Das Konto hat nur Zugriff auf die Daten, die als ein eigenständiges Konto generiert werden.
- Wenn ein Mitgliedskonto Organisation A verlässt, um Organisation B beizutreten, hat das Konto keinen Zugriff mehr auf Kosten- und Nutzungsdaten aus dem Zeitraum, als das Konto Mitglied der Organisation A war. Das Konto hat nur Zugriff auf die Daten, die Mitglied der Organisation B generiert werden.
- Wenn ein Konto erneut einer Organisation beitritt, zu der es vorher gehörte, erhält das Konto wieder Zugriff auf seine früheren Kosten- und Nutzungsdaten.

Important

Wenn Sie eine Organisation verlassen, gelten Organisationsvereinbarungen für Sie nicht mehr, die in Ihrem Namen vom Verwaltungskonto der Organisation akzeptiert wurden. Sie können eine Liste dieser Organisationsvereinbarungen in der AWS Artifact-Konsole auf der Seite AWS Artifact-Organisationsvereinbarungen anzeigen. Bevor Sie die Organisation verlassen, sollten Sie ermitteln (bei Bedarf mit Unterstützung der für rechtliche Angelegenheiten, Datenschutz oder Compliance zuständigen Teams), ob es für Sie notwendig ist, (eine) neue Vereinbarung(en) abzuschließen.

Mindestberechtigungen

Zum Verlassen einer AWS-Organisation benötigen Sie folgende Berechtigungen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:LeaveOrganization` – Beachten Sie, dass der Administrator der Organisation eine Richtlinie auf Ihr Konto anwenden kann, mit der diese Berechtigung entfernt wird, sodass Sie Ihr Konto nicht aus der Organisation entfernen können.
- Wenn Sie sich als IAM-Benutzer anmelden und dem Konto Zahlungsinformationen fehlen, muss der Benutzer entweder über `aws-portal:ModifyBilling` und `aws-portal:ModifyPaymentMethods` Berechtigungen (wenn das Konto noch nicht zu detaillierten Berechtigungen migriert wurde) ODER über `payments:CreatePaymentInstrument` und `payments:UpdatePaymentPreferences` Berechtigungen (wenn das Konto zu detaillierten Berechtigungen migriert wurde) verfügen. Außerdem muss für das Mitgliedskonto ein IAM-Benutzerzugriff auf die Abrechnung aktiviert sein. Wenn dies nicht bereits aktiviert ist, finden Sie weitere Informationen unter Den Zugriff auf die Fakturierung und Kostenmanagement-Konsole aktivieren im AWS Billing-Benutzerhandbuch.

AWS Management Console

So verlassen Sie eine Organisation in Ihrem Mitgliedskonto

1. Melden Sie sich bei der AWS Organizations-Konsole unter AWS Organizations-Konsole an. Sie müssen sich im Mitgliedskonto als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

   Standardmäßig haben Sie keinen Zugriff auf das Passwort des Stammbenutzers in einem Mitgliedskonto, das mit AWS Organizations erstellt wurde. Falls erforderlich, stellen Sie das Passwort des Stammbenutzers wieder her, indem Sie die Schritte unter Zugreifen auf ein Mitgliedskonto als Root-Benutzer befolgen.
2. Wählen Sie auf der Seite Organisations-Dashboard die Option Diese Organisation verlassen aus.
3. Wählen Sie im Dialogfeld Verlassen der Organisation bestätigen? Organisation verlassen. Wenn Sie dazu aufgefordert werden, bestätigen Sie Ihre Wahl, um das Konto zu löschen. Sobald bestätigt, werden Sie zur Seite Erste Schritte der AWS Organizations-Konsole weitergeleitet. Hier können Sie alle ausstehenden Einladungen für Ihr Konto zum Beitritt zu anderen Organisationen sehen.

   Wenn Sie die Meldung Sie können die Organisation noch nicht verlassen sehen, verfügt Ihr Konto nicht über alle erforderlichen Informationen, um als eigenständiges Konto betrieben zu werden. In diesem Fall fahren Sie mit dem nächsten Schritt fort.
4. Wenn der Verlassen der Organisation bestätigen? Im Dialogfeld wird die Meldung Sie können die Organisation noch nicht verlassen, klicken Sie auf den Link Schritte zur Kontoregistrierung abschließen.
5. Geben Sie auf der AWS-Anmeldeseite alle erforderlichen Informationen ein, um ein eigenständiges Konto zu erstellen. Dies kann die folgenden Arten von Informationen umfassen:

   - Name und Adresse der Kontaktperson
   - Gültige Zahlungsmethode
   - Verifizierung der Telefonnummer
   - Optionen für den Supportplan
6. Wenn Sie das Dialogfenster zum Abschluss des Anmeldevorgangs sehen, wählen Sie Leave organization aus.

Ein Bestätigungsdialogfeld wird angezeigt. Bestätigen Sie Ihre Wahl, um das Konto zu löschen. Sie werden zur Seite Getting Started der AWS Organizations-Konsole weitergeleitet. Hier können Sie alle ausstehenden Einladungen für Ihr Konto zum Beitritt zu anderen Organisationen sehen.

7. Entfernen Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation.

> **Important**
>
> Wenn Ihr Konto in der Organisation erstellt wurde, hat Organizations automatisch eine IAM-Rolle in dem Konto erstellt, mit dem der Zugriff durch das Verwaltungskonto der Organisation aktiviert wurde. Wenn das Konto zum Beitritt eingeladen wurde, hat Organizations eine solche Rolle nicht automatisch erstellt, allerdings haben möglicherweise Sie oder ein anderer Administrator eine entsprechende Rolle erstellt, um dieselben Vorteile zu erhalten. In beiden Fällen wird beim Entfernen des Kontos aus der Organisation eine solche Rolle nicht automatisch gelöscht. Wenn Sie diesen Zugriff aus dem Verwaltungskonto der früheren Organisation beenden möchten, müssen Sie diese IAM-Rolle manuell löschen. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

AWS CLI & AWS SDKs

Verlassen einer Organisation als Mitgliedskonto

Sie können einen der folgenden Befehle verwenden, um eine Organisation zu verlassen:

- AWS CLI: leave-organization

  Das folgende Beispiel bewirkt, dass das Konto, dessen Anmeldeinformationen zum Ausführen des Befehls verwendet werden, die Organisation verlässt.

  ```
  $ aws organizations leave-organization
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: LeaveOrganization

Nachdem das Mitgliedskonto die Organisation verlassen hat, stellen Sie sicher, dass Sie die IAM-Rollen, die Zugriff auf Ihr Konto gewähren, aus der Organisation.

> **Important**
>
> Wenn Ihr Konto in der Organisation erstellt wurde, hat Organizations automatisch eine IAM-Rolle in dem Konto erstellt, mit dem der Zugriff durch das Verwaltungskonto der Organisation aktiviert wurde. Wenn das Konto zum Beitritt eingeladen wurde, hat Organizations eine solche Rolle nicht automatisch erstellt, allerdings haben möglicherweise Sie oder ein anderer Administrator eine entsprechende Rolle erstellt, um dieselben Vorteile zu erhalten. In beiden Fällen wird beim Entfernen des Kontos aus der Organisation eine solche Rolle nicht automatisch gelöscht. Wenn Sie diesen Zugriff aus dem Verwaltungskonto der früheren Organisation beenden möchten, müssen Sie diese IAM-Rolle manuell löschen. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

Mitgliedskonten können von einem Benutzer im Verwaltungskonto stattdessen auch mit remove-account-from-organization entfernt werden. Weitere Informationen finden Sie unter Entfernen eines Mitgliedskontos aus Ihrer Organisation.

So schließen Sie ein Mitliedskonto Ihrer Organisation

Wenn Sie ein Mitgliedskonto in Ihrer Organisation nicht mehr benötigen, können Sie es über die AWS Organizations Konsole schließen, indem Sie den Anweisungen in diesem Abschnitt folgen. Sie können ein Mitgliedskonto nur mit der AWS Organizations Konsole schließen, wenn sich Ihre Organisation im Modus Alle Funktionen befindet.

Sie können ein auch AWS-Konto direkt auf der Seite Konto in der schließen, AWS Management Console nachdem Sie sich als Root-Benutzer angemeldet haben. step-by-step Anweisungen finden Sie unter Schließen eines AWS-Konto im AWS Kontoverwaltungshandbuch.

Informationen zum Schließen eines Verwaltungskontos finden Sie unter Schließen eines Verwaltungskontos in Ihrer Organisation.

So schließen Sie ein Mitgliedskonto

Wenn Sie sich im Verwaltungskonto der Organisation anmelden, können Sie Mitgliedskonten schließen, die Teil Ihrer Organisation sind. Führen Sie dazu die folgenden Schritte aus.

> **Important**
>
> Bevor Sie Ihr Mitgliedskonto schließen, empfehlen wir Ihnen dringend, Überlegungen zu lesen und die Auswirkungen auf die Schließung eines Kontos zu verstehen. Weitere Informationen finden Sie unter Was Sie wissen müssen, bevor Sie Ihr Konto schließen, und Was Sie erwarten, nachdem Sie Ihr Konto geschlossen haben im AWS Kontoverwaltungshandbuch.

AWS Management Console

So schließen Sie ein Mitgliedskonto über die AWS Organizations Konsole

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. Organisationen im konsolidierten Fakturierungsmodus können die Schaltfläche Schließen in der Konsole nicht sehen. Um ein Konto im konsolidierten Fakturierungsmodus zu schließen, führen Sie die Schritte auf der Registerkarte Eigenständiges Konto unter So schließen Sie Ihr Konto im AWS Kontoverwaltungshandbuch aus.
4. Aktivieren Sie jedes Kontrollkästchen, um alle erforderlichen Kontoschließungs-Anweisungen zu bestätigen.
5. Geben Sie die Mitgliedskonto-ID ein und wählen Sie dann Konto schließen aus.

> **Note**
>
> Jedes Mitgliedskonto, das Sie schließen, zeigt in der AWS Organizations Konsole eine `SUSPENDED` Bezeichnung neben seinem Kontonamen an.

So schließen Sie ein Mitgliedskonto auf der Seite Konten

Optional können Sie ein - AWS Mitgliedskonto direkt auf der Seite Konten in der schließen AWS Management Console. Befolgen step-by-step Sie die Anweisungen unter Schließen eines AWS-Konto im AWS Kontoverwaltungshandbuch.

AWS CLI & AWS SDKs

So schließen Sie eine AWS-Konto

Sie können einen der folgenden Befehle verwenden, um ein Konto zu schließen:

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- -AWS SDKs CloseAccount:

Schützen von Mitgliedskonten vor der Schließung

Wenn Sie ein Mitgliedskonto vor versehentlicher Schließung schützen möchten, können Sie eine IAM-Richtlinie erstellen, um anzugeben, welche Konten von der Schließung ausgenommen sind. Jedes mit diesen Richtlinien geschützte Mitgliedskonto kann nicht geschlossen werden. Dies kann mit einem SCP nicht erreicht werden, da sie die Prinzipale im Verwaltungskonto nicht beeinflussen.

Sie können eine IAM-Richtlinie erstellen, die das Schließen von Konten auf zwei Arten verweigert:

- Führen Sie jedes Konto, das Sie schützen möchten, explizit in der Richtlinie auf, indem Sie den `arn` in das `Resource`-Element einfügen. Beispiele finden Sie unter Verhindern, dass Mitgliederkonten, die in dieser Richtlinie aufgeführt sind, geschlossen werden.
- Markieren Sie einzelne Konten, um zu verhindern, dass sie geschlossen werden. Verwenden Sie den globalen Bedingungsschlüssel des `aws:ResourceTag`-Tags in Ihrer Richtlinie, um zu verhindern, dass Konten mit dem Tag geschlossen werden. Informationen zum Markieren eines Kontos finden Sie unter Markieren von Organisationsressourcen. Beispiele finden Sie unter Verhindern Sie, dass Mitgliedskonten mit den Tags geschlossen werden .

Beispiele für IAM-Richtlinien, die Schließungen von Mitgliedskonten verhindern

Die folgenden Codebeispiele zeigen zwei verschiedene Methoden, mit denen Sie Mitgliedskonten daran hindern können, ihr Konto zu schließen.

Verhindern Sie, dass Mitgliedskonten mit den Tags geschlossen werden

Sie können die folgende Richtlinie an eine Identität in Ihrem Verwaltungskonto anfügen. Diese Richtlinie hindert Prinzipale im Verwaltungskonto daran, Mitgliedskonten zu schließen, die mit dem globalen Bedingungsschlüssel des `aws:ResourceTag`-Tags, dem `AccountType`-Schlüssel und dem `Critical`-Tag-Wert gekennzeichnet sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Verhindern, dass Mitgliederkonten, die in dieser Richtlinie aufgeführt sind, geschlossen werden

Sie können die folgende Richtlinie an eine Identität in Ihrem Verwaltungskonto anfügen. Diese Richtlinie verhindert, dass Prinzipale im Verwaltungskonto Mitgliederkonten schließen, die explizit im `Resource`-Element angegeben wurden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
```

```
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

Schließen eines Verwaltungskontos in Ihrer Organisation

Um das Verwaltungskonto in Ihrer Organisation zu schließen, müssen Sie zunächst entweder alle Mitgliedskonten in der Organisation schließen oder entfernen. Durch das Schließen des Verwaltungskontos werden auch die Instance von AWS Organizations und alle Richtlinien gelöscht, die Sie innerhalb dieser Organisation nach Ablauf der Phase nach Kontoschließung erstellt haben.

So schließen Sie ein Verwaltungskonto

Gehen Sie wie folgt vor, um ein Verwaltungskonto zu schließen.

> **Important**
>
> Bevor Sie Ihr Verwaltungskonto schließen, empfehlen wir Ihnen dringend, Überlegungen zu überprüfen und die Auswirkungen auf die Schließung eines Kontos zu verstehen. Weitere Informationen finden Sie unter Was Sie wissen müssen, bevor Sie Ihr Konto schließen, und Was Sie erwarten, nachdem Sie Ihr Konto geschlossen haben im AWS Kontoverwaltungshandbuch.

AWS Management Console

So schließen Sie ein Verwaltungskonto auf der Seite Konten

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

1. Melden Sie sich bei der 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 -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 über ein Mitgliedskonto verfügen, das noch aktiv ist, müssen Sie die Anleitungen unter befolgen, So schließen Sie ein Mitliedskonto Ihrer Organisation bevor Sie mit dem nächsten Schritt fortfahren können.
3. Wählen Sie auf der Navigationsleiste in der oberen rechten Ecke Ihren Kontonamen oder Ihre Kontonummer und dann Konto aus.
4. Scrollen Sie auf der Seite Konto nach unten zum Abschnitt Konto schließen. Lesen Sie sich den Prozess der Kontoschließung durch und stellen Sie sicher, dass Sie ihn verstehen.
5. Wählen Sie die Schaltfläche Konto schließen, um den Kontoschließungsprozess zu starten.
6. Innerhalb weniger Minuten sollten Sie eine E-Mail-Bestätigung erhalten, dass Ihr Konto geschlossen wurde.

AWS CLI & AWS SDKs

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

Aktualisieren alternativer Kontakte in Ihrer Organisation

Sie können alternative Kontakte für Konten in Ihrer Organisation aktualisieren, indem Sie die AWS-Organisationskonsole verwenden oder programmgesteuert mit dem AWS-CLI oder AWS-SDKs. Weitere Informationen zum Aktualisieren von alternativen Kontakten finden Sie unter Zugreifen auf oder Aktualisieren der alternativen Kontakte in der AWS-Kontoverwaltungs-Referenz.

Aktualisierung der primären Kontaktinformationen in Ihrer Organisation

Sie können primäre Kontaktinformationen für Konten in Ihrer Organisation aktualisieren, indem Sie die AWS-Organisationskonsole verwenden oder programmgesteuert mit der AWS-CLI oder den AWS-SDKs. Informationen zum Aktualisieren der primären Kontaktinformationen finden Sie unter

Accessing or updating the primary account contact (Zugriff auf den primären Kontokontakt oder Aktualisieren des primären Kontokontakts) in der AWS-Kontoverwaltungsreferenz.

Aktualisieren aktivierter AWS-Regionen in Ihrer Organisation

Sie können aktivierte AWS-Regionen für Konten innerhalb Ihrer Organisation über die AWS Organizations-Konsole aktualisieren. Wie Sie aktivierten AWS-Regionen aktualisieren können, erfahren Sie in der AWS-Referenz zur Kontoverwaltung unter Festlegen, welche AWS-Regionen Ihr Konto verwenden kann.

Verwalten von Richtlinien in AWS Organizations

Dank der Richtlinien in AWS Organizations haben Sie zusätzliche Möglichkeiten, die AWS-Konten innerhalb Ihrer Organisation zu verwalten. Sie können Richtlinien verwenden, wenn alle Features in Ihrer Organisation aktiviert sind.

Die AWS Organizations-Konsole zeigt den aktivierten oder deaktivierten Status für jedes Richtlinientyps an. Wählen Sie im linken Navigationsbereich auf der Registerkarte Organize accounts (Konten organisieren) `Root` aus. Im Detailbereich auf der rechten Seite des Bildschirms werden alle verfügbaren Richtlinientypen angezeigt. Die Liste gibt an, welche aktiviert sind und welche in diesem Organisationsstamm deaktiviert sind. Wenn die Option Enable zum Aktivieren eines Typs vorhanden ist, dann ist der betreffende Typ aktuell deaktiviert. Wenn die Option Disable vorhanden ist, dann ist der betreffende Typ aktuell aktiviert.

Richtlinientypen

Organizations bietet Richtlinientypen in den folgenden zwei großen Kategorien an:

Autorisierungsrichtlinien

Autorisierungsrichtlinien helfen Ihnen, die Sicherheit der AWS-Konten in Ihrer Organisation zentral zu verwalten.

- Service-Kontrollrichtlinien (Service Control Policies, SCPs) ermöglichen die zentrale Kontrolle der maximal verfügbaren Berechtigungen für alle Konten Ihrer Organisation.

Management-Richtlinien

Mit Verwaltungsrichtlinien können Sie AWS Services und deren Features zentral konfigurieren und verwalten.

- Opt-out-Richtlinien für künstliche Intelligenz (KI)ermöglichen es Ihnen, die Datensammlung für AWS-KI-Services für alle Konten Ihrer Organisation zu kontrollieren.
- Backup-Richtlinien helfen Ihnen, Backup-Pläne zentral zu verwalten und auf die AWS-Ressourcen über die Konten Ihrer Organisation hinweg anzuwenden.
- MitTag-Richtlinien können Sie die Tags standardisieren, die den AWS-Ressourcen in den Konten Ihrer Organisation angefügt sind.

In der folgenden Tabelle sind einige der Merkmale der einzelnen Richtlinientypen zusammengefasst. Weitere Merkmale zu diesen Richtlinientypen finden Sie unter Kontingente für AWS Organizations.

Richtlinientyp	Beeinträchtigt das Verwaltungskonto	Maximale Anzahl, die Sie einem Stamm, einer OU oder einem Konto anfügen können	Maximale Größe	Unterstützt die Anzeige effektiver Richtlinien für OU oder Konto
SCP	 Nein	5	5120 Zeichen	 Nein
Richtlinie zur Abmeldung von KI-Services	 Ja	5	2500 Zeichen	 Ja
Backup-Richtlinie	 Ja	10	10,000 Zeichen	 Ja
Tag-Richtlinie	 Ja	10	10,000 Zeichen	 Ja

Verwenden von Richtlinien in Ihrer Organisation

- Aktivieren und Deaktivieren von Richtlinientypen
- Abrufen von Informationen zu den Richtlinien Ihrer Organisation
- Delegierter Administrator für AWS Organizations

- Management-Richtlinien
- Service-Kontrollrichtlinien (SCPs)

Aktivieren und Deaktivieren von Richtlinientypen

Aktivieren eines Richtlinientyps

Bevor Sie eine Richtlinie erstellen und Ihrer Organisation zuweisen können, müssen Sie diesen Richtlinientyp für die Verwendung aktivieren. Das Aktivieren eines Richtlinientyps ist eine einmalige Aufgabe im Organisationsstamm. Sie können einen Richtlinientyp nur über das Verwaltungskonto der Organisation aktivieren.

Mindestberechtigungen

Um einen Richtlinientyp zu aktivieren, benötigen Sie die Berechtigung zum Ausführen der folgenden Aktionen:

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:ListRoots` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So aktivieren Sie einen Richtlinientyp

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Klicken Sie auf Richtlinien und wählen Sie den Namen des Richtlinientyp aus, den Sie aktivieren möchten.
3. Wählen Sie auf der Seite Richtlinientyp Aktivieren des ***Richtlinientyps*** aus.

   Die Seite wird durch eine Liste der verfügbaren Richtlinien des angegebenen Typs ersetzt.

AWS CLI & AWS SDKs

So aktivieren Sie einen Richtlinientyp

Sie können einen Richtlinientyp mit einer der folgenden Befehlen aktivieren:

- AWS CLI: enable-policy-type

  Im folgenden Beispiel wird veranschaulicht, wie Backup-Richtlinien für Ihre Organisation aktiviert werden können. Beachten Sie, dass Sie die ID des Stammes Ihrer Organisation angeben müssen.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  Die Liste von `PolicyTypes` in der Ausgabe enthält jetzt den angegebenen Richtlinientyp mit dem `Status` von `ENABLED`.

- AWS-SDKs: EnablePolicyType

Deaktivieren eines Richtlinientyps

Wenn Sie einen bestimmten Richtlinientyp in Ihrer Organisation nicht mehr verwenden möchten, können Sie diesen Typ deaktivieren, um die versehentliche Verwendung zu verhindern. Sie können einen Richtlinientyp nur über das Verwaltungskonto der Organisation deaktivieren.

Important

- Wenn Sie einen Richtlinientyp deaktivieren, werden alle Richtlinien des angegebenen Typs automatisch von allen Entitäten im Organisationsstamm getrennt. Die Richtlinien werden nicht gelöscht.
- (Nur Service-Kontrollrichtlinien-Richtlinientyp) Wenn Sie den SCP-Richtlinientyp später erneut aktivieren, werden alle Entitäten im Organisationsstammverzeichnis zunächst nur dem `FullAWSAccess`-Standard-SCP zugewiesen. Anhänge von SCPs an Entitäten gehen verloren, wenn die SCPs in der Organisation deaktiviert sind. Wenn Sie SCPs später wieder aktivieren möchten, müssen Sie sie gegebenenfalls erneut an den Stammordner, die Organisationseinheiten und die Konten der Organisation anhängen.

Mindestberechtigungen

Für die Deaktivierung von SCPs benötigen Sie die Berechtigung zum Ausführen der folgenden Aktionen:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:ListRoots` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So deaktivieren Sie einen Richtlinientyp

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Klicken Sie auf Richtlinien und wählen Sie den Namen des Richtlinientyp aus, den Sie deaktivieren möchten.
3. Wählen Sie auf der Seite Richtlinientyp Deaktivieren des ***Richtlinientyps*** aus.

4. Geben Sie im Bestätigungsdialogfeld das Wort **`disable`** ein und wählen Sie dann Deaktivieren.

   Die Liste der verfügbaren Richtlinien des angegebenen Typs wird ausgeblendet.

AWS CLI & AWS SDKs

So deaktivieren Sie einen Richtlinientyp

Sie können zum Deaktivieren eines Richtlinientyps einen der folgenden Befehle verwenden:

- AWS CLI: disable-policy-type

  Im folgenden Beispiel wird veranschaulicht, wie Backup-Richtlinien für Ihre Organisation deaktiviert werden können. Beachten Sie, dass Sie die ID des Stammes Ihrer Organisation angeben müssen.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

  Die Liste von `PolicyTypes` in der Ausgabe enthält nicht mehr den angegebenen Richtlinientyp.

- AWS-SDKs: DisablePolicyType

Abrufen von Informationen zu den Richtlinien Ihrer Organisation

In diesem Abschnitt werden verschiedene Möglichkeiten beschrieben, um detaillierte Informationen zu Richtlinien in Ihrer Organisation zu erhalten. Diese Verfahren gelten für alle Richtlinientypen. Im Organisationsstamm müssen Sie einen Richtlinientyp aktivieren, bevor Sie Richtlinien dieses Typs an Entitäten in diesem Organisationsstamm anhängen können.

Auflisten aller Richtlinien

Mindestberechtigungen

Wenn Sie die Richtlinien innerhalb Ihrer Organisation auflisten möchten, benötigen Sie folgende Berechtigung:

- `organizations:ListPolicies`

Sie können die Richtlinien in Ihrer Organisation im AWS Management Console oder mithilfe eines AWS Command Line Interface-(AWS CLI)-Befehls oder eines AWS-SDK-Vorgangs anzeigen.

AWS Management Console

So listen Sie alle Richtlinien in der Organisation auf

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Richtlinien die Richtlinie aus, die Sie auflisten möchten.

   Wenn der angegebene Richtlinientyp aktiviert ist, zeigt die Konsole eine Liste aller Richtlinien dieses Typs an, die derzeit in der Organisation verfügbar sind.
3. Kehren Sie zur Seite Richtlinien zurück und wiederholen Sie den Vorgang für jeden Richtlinientyp.

AWS CLI & AWS SDKs

So listen Sie alle Richtlinien in der Organisation auf

Sie können einen der folgenden Befehle verwenden, um Richtlinien in einer Organisation aufzulisten:

- AWS CLI: list-policies

  Das folgende Beispiel zeigt, wie Sie eine Liste aller Service-Kontrollrichtlinien in Ihrer Organisation abrufen. Sie müssen den Richtlinientyp angeben, den Sie sehen möchten. Wiederholen Sie den Befehl für jeden Richtlinientyp, den Sie einschließen möchten.

```
$ aws organizations list-policies \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS-SDKs: ListPolicies

Auflisten der Richtlinien, die einem Root, einer Organisationseinheit oder einem zugewiesen sind

> **Mindestberechtigungen**
>
> Um die Richtlinien, die an einen Root, eine Organisationseinheit (Organizational Unit, OU) oder ein Konto innerhalb Ihrer Organisation angehängt sind, aufzulisten, benötigen Sie folgende Berechtigung:
>
> - `organizations:ListPoliciesForTarget` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den Amazon-Ressourcennamen (ARN) für das angegebene Ziel enthält (oder „*“)

AWS Management Console

Auflisten aller Richtlinien, die direkt an einen angegebenen Root, eine Organisationseinheit oder ein Konto angehängt sind

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der AWS-Konten-Seite den Namen des Stamms, der OU oder des Kontos aus, dessen Richtlinien Sie anzeigen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit zu finden.
3. Wählen Sie auf der Seite Stamm, Organisationseinheit oder Konto die Registerkarte Richtlinien aus.

   Auf der Registerkarte Richtlinien werden alle Richtlinien angezeigt, die diesem Stamm, dieser Organisationseinheit oder diesem Konto zugeordnet sind, gruppiert nach Richtlinientyp.

AWS CLI & AWS SDKs

Auflisten aller Richtlinien, die direkt an einen angegebenen Root, eine Organisationseinheit oder ein Konto angehängt sind

Sie können einen der folgenden Befehle verwenden, um Richtlinien aufzulisten, die einer Entität angefügt sind:

- AWS CLI: list-policies-for-target

  Im folgenden Beispiel werden alle Service-Kontrollrichtlinien aufgelistet, die der angegebenen Organisationseinheit zugeordnet sind. Sie müssen sowohl die ID des Stammes, der Organisationseinheit oder des Kontos als auch den Richtlinientyp angeben, den Sie auflisten möchten.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
```

```
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWS-SDKs: ListPoliciesForTarget

Auflisten aller Roots, Organisationseinheiten und Konten, denen eine Richtlinie zugewiesen ist

Mindestberechtigungen

Zum Auflisten der Elemente, an die eine Richtlinie angehängt ist, benötigen Sie folgende Berechtigung:

- `organizations:ListTargetsForPolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")

AWS Management Console

Auflisten aller Roots, Organisationseinheiten und Konten, an denen eine bestimmte Richtlinie angehängt ist

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Richtlinien den Richtlinientyp und dann den Namen der Richtlinie aus, deren Anhänge Sie überprüfen möchten.
3. Wählen Sie die Registerkarte Ziele aus, um eine Tabelle aller Stämme, OUs und Konten anzuzeigen, denen die ausgewählte Richtlinie zugeordnet ist.

AWS CLI & AWS SDKs

Auflisten aller Roots, Organisationseinheiten und Konten, an denen eine bestimmte Richtlinie angehängt ist

Sie können einen der folgenden Befehle verwenden, um Entitäten aufzulisten, die über eine Richtlinie verfügen:

- AWS CLI: list-targets-for-policy

  Das folgende Beispiel zeigt alle Anhänge an Stämme, Organisationseinheiten und Konten für die angegebene Richtlinie.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
```

```
        }
    ]
}
```

- AWS-SDKs: ListTargetsForPolicy

Abrufen von Details zu einer Richtlinie

Mindestberechtigungen

Zum Abrufen der Details einer Richtlinie benötigen Sie folgende Berechtigung:

- `organizations:DescribePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")

AWS Management Console

Abrufen von Details über eine Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Richtlinien den Richtlinientyp der Richtlinie aus, die Sie überprüfen möchten, und wählen Sie dann den Namen der Richtlinie aus.

   Auf der Richtlinienseite werden die verfügbaren Informationen zur Richtlinie angezeigt, einschließlich ARN, Beschreibung und angehängter Ziele.

   - Die Registerkarte Inhalt zeigt den aktuellen Inhalt der Richtlinie im JSON-Format an.
   - Die Registerkarte Ziele zeigt eine Liste der Stämme, OUs und Konten an, mit denen die Richtlinie verknüpft ist.
   - Die Registerkarte Tags zeigt die an die Richtlinie angehängten Tags an. Hinweis: Die Registerkarte Tags ist für AWS-verwaltete Richtlinien nicht verfügbar.

   Um die Richtlinie zu bearbeiten, wählen Sie Richtlinie bearbeiten. Da für jeden Richtlinientyp unterschiedliche Bearbeitungsanforderungen gelten, lesen Sie die Anweisungen zum Erstellen und Aktualisieren von Richtlinien des angegebenen Richtlinientyps.

AWS CLI & AWS SDKs

Abrufen von Details über eine Richtlinie

Sie können einen der folgenden Befehle verwenden, um Details zu einer Richtlinie zu erhalten:

- AWS CLI: describe-policy

  Im folgenden Beispiel werden die Details für die angegebene Richtlinie angezeigt.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
    }
}
```

- AWS-SDKs: DescribePolicy

Delegierter Administrator für AWS Organizations

Wir empfehlen, das Verwaltungskonto von AWS Organizations und die zugehörigen Benutzer und Rollen nur für Aufgaben zu verwenden, die über dieses Konto ausgeführt werden müssen. Außerdem sollten Sie die AWS-Ressourcen in anderen Mitgliedskonten in der Organisation speichern und sie aus dem Verwaltungskonto heraushalten. Der Grund dafür ist, dass Sicherheitsfeatures wie die Service-Kontrollrichtlinien (SCPs) von Organizations die Benutzer oder Rollen im Verwaltungskonto nicht einschränken.

Über das Verwaltungskonto der Organisation können Sie die Richtlinienverwaltung für Organizations an bestimmte Mitgliedskonten delegieren, um Richtlinienaktionen auszuführen, die standardmäßig nur für das Verwaltungskonto verfügbar sind.

Erstellen oder Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie

Erstellen oder aktualisieren Sie vom Verwaltungskonto aus eine ressourcenbasierte Delegierungsrichtlinie für Ihre Organisation und fügen Sie eine Erklärung hinzu, die angibt, welche Mitgliedskonten Aktionen im Rahmen von Richtlinien ausführen können. Sie können der Richtlinie mehrere Anweisungen hinzufügen, um unterschiedliche Berechtigungen für Mitgliedskonten anzugeben.

Mindestberechtigungen

Um die ressourcenbasierte Delegierungsrichtlinie zu erstellen oder zu aktualisieren, benötigen Sie die Berechtigung, die folgenden Aktionen auszuführen:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Darüber hinaus müssen Sie Rollen und Benutzern im delegierten Administratorkonto die entsprechenden IAM-Berechtigungen für die erforderlichen Aktionen gewähren. Ohne IAM-Berechtigungen wird davon ausgegangen, dass der aufrufende Prinzipal nicht über die erforderlichen Berechtigungen zur Verwaltung von AWS Organizations-Richtlinien verfügt.

AWS Management Console

Verwenden Sie eine der folgenden Methoden, um der ressourcenbasierten Delegierungsrichtlinie in der AWS Management Console Anweisungen hinzuzufügen:

- JSON-Richtlinie – Fügen Sie ein Beispiel für eine ressourcenbasierte Delegierungsrichtlinie ein und passen Sie es an, um es in Ihrem Konto zu verwenden, oder geben Sie Ihr eigenes JSON-Richtliniendokument in den JSON-Editor ein.
- Visueller Editor – Erstellen Sie im visuellen Editor eine neue Delegierungsrichtlinie, die Sie beim Erstellen einer Delegierungsrichtlinie unterstützt, ohne JSON-Syntax schreiben zu müssen.

Verwenden des JSON-Richtlinieneditors zum Erstellen oder Aktualisieren einer Delegierungsrichtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie im Abschnitt Delegierter Administrator für AWS Organizations die Option Delegate (Delegieren) aus, um die Delegierungsrichtlinie für Organizations zu erstellen. Um eine bestehende Delegierungsrichtlinie zu aktualisieren, wählen Sie Edit (Bearbeiten).
4. Geben oder fügen Sie ein JSON-Richtliniendokument ein. Weitere Informationen zur IAM-Richtliniensprache finden Sie in der IAM-JSON-Richtlinienreferenz.
5. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung erzeugt wurden, und wählen Sie dann Create policy (Richtlinie erstellen).

Verwenden des visuellen Editors zum Erstellen oder Aktualisieren einer Delegierungsrichtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie im Abschnitt Delegierter Administrator für AWS Organizations die Option Delegate (Delegieren) aus, um die Delegierungsrichtlinie für Organizations zu erstellen. Um eine bestehende Delegierungsrichtlinie zu aktualisieren, wählen Sie Edit (Bearbeiten).
4. Wählen Sie auf der Seite Create Delegation policy (Delegierungsrichtlinie erstellen) die Option Add new statement (Neue Anweisung hinzufügen) aus.
5. Stellen Sie Effect (Effekt) auf `Allow`.
6. Fügen Sie den `Principal` hinzu, um die Mitgliedskonten zu definieren, an die Sie delegieren möchten. Weitere Informationen zur Syntax finden Sie unter Beispiel für ressourcenbasierte Delegierungsrichtlinien.
7. Wählen Sie aus der Liste Actions (Aktionen) die Aktionen aus, die Sie delegieren möchten. Sie können die Auswahl mithilfe der Option Filter actions (Aktionen filtern) eingrenzen.
8. Um anzugeben, ob das delegierte Mitgliedskonto Richtlinien an die Stammorganisation oder die Organisationseinheiten (OUs) anhängen kann, legen Sie `Resources` fest. Sie müssen

auch `policy` als Ressourcentyp auswählen. Weitere Details finden Sie unter Beispiel für ressourcenbasierte Delegierungsrichtlinien. Sie können Ressourcen auf folgende Weise angeben:

- Wählen Sie Add a resource (Ressource hinzufügen) und erstellen Sie den Amazon-Ressourcennamen (ARN), indem Sie den Anweisungen im Dialogfeld folgen.
- Listen Sie die Ressourcen-ARNs manuell im Editor auf. Weitere Informationen zur ARN-Syntax finden Sie unter Amazon-Ressourcenname (ARN) im Allgemeinen Referenzhandbuch von AWS. Hinweise zur Verwendung von ARNs im Ressourcenelement einer Richtlinie finden Sie unter IAM-JSON-Richtlinienelemente: Ressource.

9. Wählen Sie Add a condition (Bedingung hinzufügen), um weitere Bedingungen anzugeben, einschließlich des Richtlinientyps, den Sie delegieren möchten. Wählen Sie den Condition Key (Bedingungsschlüssel), den Tag key (Tag-Schlüssel), den Qualifier (Qualifizierer) und den Operator (Operator) der Bedingung aus und geben Sie dann einen **`Value`** (Wert) ein. Weitere Details finden Sie unter Beispiel für ressourcenbasierte Delegierungsrichtlinien. Wählen Sie danach Add condition (Bedingung hinzufügen) aus. Weitere Informationen zum Element Condition (Bedingung) finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung in der IAM-JSON-Richtlinienreferenz.
10. Um mehr Berechtigungsblöcke hinzuzufügen, wählen Sie Add new statement (Neue Anweisung hinzufügen). Wiederholen Sie die Schritte 5 bis 9 für jeden Block.
11. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung erzeugt wurden, und wählen Sie dann Create policy (Richtlinie erstellen), um Ihre Arbeit zu speichern.

AWS CLI & AWS SDKs

Erstellen oder Aktualisieren einer Delegierungsrichtlinie

Sie können zum Erstellen oder Aktualisieren einer Richtlinie die folgenden Befehle verwenden:

- AWS CLI: put-resource-policy

  Im folgenden Beispiel wird die Delegierungsrichtlinie erstellt oder aktualisiert.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

Unterstützte Richtlinienaktionen zur Delegierung

Folgende Aktionen werden in der Delegierungsrichtlinie unterstützt:

- `AttachPolicy`

- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource
- ListTargetsForPolicy

- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Anzeigen einer ressourcenbasierte Delegierungsrichtlinie

Sehen Sie sich vom Verwaltungskonto aus die ressourcenbasierte Delegierungsrichtlinie Ihrer Organisation an, um zu erfahren, welche delegierten Administratoren Zugriff auf die Verwaltung welcher Richtlinientypen haben.

> **Mindestberechtigungen**
>
> Um die ressourcenbasierte Delegierungsrichtlinie anzuzeigen, benötigen Sie die Berechtigung, die folgende Aktion auszuführen: `organizations:DescribeResourcePolicy`.

AWS Management Console

So zeigen Sie eine Delegierungsrichtlinie an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie Settings (Einstellungen) aus.
3. Scrollen Sie im Abschnitt Delegierter Administrator für AWS Organizations, um die vollständige Delegierungsrichtlinie anzuzeigen.

AWS CLI & AWS SDKs

Anzeigen einer Delegierungsrichtlinie

Sie können zum Anzeigen einer Delegierungsrichtlinie den folgenden Befehl verwenden:

- AWS CLI: describe-resource-policy

  Das folgende Beispiel ruft die Richtlinie ab.

```
$ aws organizations describe-resource-policy
```

- AWS SDK: DescribeResourcePolicy

Löschen einer ressourcenbasierte Delegierungsrichtlinie

Wenn Sie die Verwaltung von Richtlinien in Ihrer Organisation nicht mehr delegieren müssen, können Sie die ressourcenbasierte Delegierungsrichtlinie aus dem Verwaltungskonto der Organisation löschen.

> **Important**
>
> Wenn Sie Ihre ressourcenbasierte Delegierungsrichtlinie löschen, können Sie sie nicht wiederherstellen.

> **Mindestberechtigungen**
>
> Um die ressourcenbasierte Delegierungsrichtlinie zu löschen, benötigen Sie die Berechtigung, die folgende Aktion auszuführen: `organizations:DeleteResourcePolicy`.

AWS Management Console

So löschen Sie eine Delegierungsrichtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie im Bereich Delegierter Administrator für AWS Organizations die Option Löschen aus.
4. Geben Sie im Bestätigungsdialogfeld Delet policy (Richtlinie löschen) **`delete`** ein. Wählen Sie dann Delete policy (Richtlinie löschen).

AWS CLI & AWS SDKs

Löschen einer Delegierungsrichtlinie

Sie können zum Löschen einer Delegierungsrichtlinie den folgenden Befehl verwenden:

- AWS CLI: delete-resource-policy

  Im folgenden Beispiel wird die Richtlinie gelöscht.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

Beispiel für ressourcenbasierte Delegierungsrichtlinien

Die folgenden Codebeispiele veranschaulichen, wie Sie ressourcenbasierte Delegierungsrichtlinien verwenden.

Beispiele

- Beispiel: Anzeigen der Organisation, Organisationseinheiten, Konten und Richtlinien
- Beispiel: Konsolidierte Berechtigungen zur Verwaltung der Backup-Richtlinien einer Organisation

Beispiel: Anzeigen der Organisation, Organisationseinheiten, Konten und Richtlinien

Bevor Sie die Verwaltung von Richtlinien delegieren, müssen Sie die Berechtigungen delegieren, um in der Struktur einer Organisation zu navigieren und die Organisationseinheiten (OUs), Konten und die damit verbundenen Richtlinien einzusehen.

Dieses Beispiel zeigt, wie Sie diese Berechtigungen in Ihre ressourcenbasierte Delegierungsrichtlinie für das Mitgliedskonto *AccountId* aufnehmen können.

> **Important**
>
> Es ist ratsam, dass Sie nur Berechtigungen für die im Beispiel gezeigten Mindestaktionen gewähren. Es ist jedoch möglich, mithilfe dieser Richtlinie alle schreibgeschützten Aktionen von Organizations zu delegieren.

Diese Beispieldelegierungsrichtlinie gewährt die Berechtigungen, die erforderlich sind, um Aktionen programmgesteuert über die AWS-API oder AWS CLI durchzuführen. Um diese Delegierungsrichtlinie zu verwenden, ersetzen Sie den AWS Platzhaltertext für *AccountId* durch Ihre eigenen Informationen. Folgen Sie dann den Anweisungen in Delegierter Administrator für AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Beispiel: Konsolidierte Berechtigungen zur Verwaltung der Backup-Richtlinien einer Organisation

Dieses Beispiel zeigt, wie Sie eine ressourcenbasierte Delegierungsrichtlinie erstellen können, die es dem Verwaltungskonto ermöglicht, alle Berechtigungen zu delegieren, die für die Verwaltung von

Backup-Richtlinien innerhalb der Organisation erforderlich sind, einschließlich der Aktionen `create`, `read`, `update`und `delete` sowie der Richtlinienaktionen `attach` und `detach`. Informationen zur Bedeutung der einzelnen Aktionen, Ressourcen und Bedingungen finden Sie unter Beispiel für ressourcenbasierte Delegierungsrichtlinien.

> **Important**
>
> Diese Richtlinie ermöglicht es delegierten Administratoren, die angegebenen Aktionen für Richtlinien auszuführen, die von einem beliebigen Konto in der Organisation erstellt wurden, einschließlich des Verwaltungskontos.

Diese Beispielrichtlinie gewährt die Berechtigungen, die erforderlich sind, um Aktionen programmgesteuert über die AWS-API oder AWS CLI durchzuführen. Um diese Delegierungsrichtlinie zu verwenden, ersetzen Sie denAWS Platzhaltertext für *`MemberAccountId`*, *`ManagementAccountId`*, *`OrganizationID`* und *`rootId`* durch Ihre eigenen Informationen. Folgen Sie dann den Anweisungen in Delegierter Administrator für AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
```

```
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Management-Richtlinien

Mit Verwaltungsrichtlinien können Sie AWS Services und deren Features zentral konfigurieren und verwalten. Wie sich Richtlinien auf die OUs und Konten auswirken, die sie erben, hängt vom Typ der Verwaltungsrichtlinie ab, die Sie in AWS Organizations anwenden. Lesen Sie sich die Themen

in diesem Abschnitt durch, um die relevanten Begriffe und Konzepte zu Verwaltungsrichtlinien zu verstehen.

Themen

- Vererbung von Verwaltungsrichtlinien verstehen
- Richtlinien zur Abmeldung von KI-Services
- Backup-Richtlinien
- Tag-Richtlinien

Vererbung von Verwaltungsrichtlinien verstehen

> **Note**
>
> Die Informationen in diesem Abschnitt gelten nicht für SCPs, da SCPs sowohl das Zulassen als auch das Ablehnen von IAM-Aktionen verwalten. SCPs sind zwar Root-, OUs- und Accounts zugeordnet, für die Zulassung von Aktionen ist jedoch eine ausdrückliche `allow` Angabe der SCPs auf jeder Ebene erforderlich, vom Stammverzeichnis bis hin zu jeder Organisationseinheit im direkten Pfad zum Konto (einschließlich des Zielkontos selbst). Weitere Informationen zur Funktionsweise von SCPs in einer AWS Organizations-Hierarchie finden Sie unter SCP-Bewertung.

Sie können Verwaltungsrichtlinien an Organisationsentitäten (Organisationsstamm, Organisationseinheit (OU) oder Konto) in Ihrer Organisation anfügen:

- Wenn Sie dem Organisationsstamm eine Verwaltungsrichtlinie hinzufügen, erben alle Konten in der Organisation diese Richtlinie.
- Wenn Sie einer bestimmten OU eine Verwaltungsrichtlinie hinzufügen, erben Konten, die direkt unter dieser OU oder einer untergeordneten OU stehen, diese Richtlinie.
- Wenn Sie eine Verwaltungsrichtlinie an ein bestimmtes Konto anfügen, wirkt sich dies nur auf dieses Konto aus.

Da Sie Verwaltungsrichtlinien mehreren Ebenen in der Organisation hinzufügen können, können Konten mehrere Richtlinien erben.

In diesem Abschnitt wird erläutert, wie übergeordnete Richtlinien und untergeordnete Richtlinien zur effektiven Richtlinie für ein Konto verarbeitet werden.

Themen

- Vererbungsterminologie
- Richtliniensyntax und Vererbung für Verwaltungsrichtlinientypen
- Vererbungsoperatoren
- Beispiele für Vererbungen

Vererbungsterminologie

In diesem Thema werden die folgenden Begriffe verwendet, um die Vererbung von Verwaltungsrichtlinien zu diskutieren.

Richtlinienvererbung

Die Interaktion von Richtlinien auf unterschiedlichen Ebenen einer Organisation, die sich vom Stamm der obersten Ebene der Organisation über die Hierarchie der Organisationseinheiten (OUs) nach unten zu einzelnen Konten erstreckt.

Sie können Richtlinien an den Organisationsstamm, Organisationseinheiten, einzelne Konten und eine beliebige Kombination dieser Organisationseinheiten anfügen. Die Richtlinienvererbung bezieht sich auf Verwaltungsrichtlinien, die dem Organisationsstamm oder einer OU zugeordnet sind. Alle Konten, die Mitglieder des Organisationsstammes oder der OU sind, denen eine Verwaltungsrichtlinie hinzugefügt wird, erben diese Richtlinie.

Wenn beispielsweise Verwaltungsrichtlinien an den Organisationsstamm angehängt sind, erben alle Konten in der Organisation diese Richtlinie. Das liegt daran, weil alle Konten einer Organisation immer dem Organisationsstamm untergeordnet sind. Wenn Sie einer bestimmten OU eine Richtlinie hinzufügen, erben Konten, die direkt unter dieser OU oder einer untergeordneten OU stehen, diese Richtlinie. Da Sie Richtlinien mehreren Organisationsebenen hinzufügen können, können Konten mehrere Richtliniendokumente eines einzelnen Richtlinientyps erben.

Übergeordnete Richtlinien

Richtlinien, die innerhalb der Organisationsstruktur auf höherer Ebene hinzugefügt sind als Richtlinien, die mit Entitäten auf niedrigerer Ebene innerhalb der Struktur verknüpft sind.

Wenn Sie beispielsweise die Richtlinie A an den OU anhängen, handelt es sich lediglich um eine Richtlinie. Wenn Sie auch Richtlinie B an eine Organisationseinheit unter diesem Stamm anfügen, ist Richtlinie A die übergeordnete Richtlinie von Richtlinie B. Richtlinie B ist die untergeordnete Richtlinie von Richtlinie A. Zusammengeführt ergeben Richtlinie A und Richtlinie B die effektive Tag-Richtlinie für Konten in der OU.

Untergeordnete Richtlinien

Richtlinien, die auf einer niedrigeren Ebene innerhalb der Organisationsstruktur hinzugefügt sind als die übergeordnete Richtlinie.

Effektive Richtlinien

Das letzte, einzelne Richtliniendokument, das die Regeln angibt, die für ein Konto gelten. Die effektive Richtlinie ist die Aggregation aller Richtlinien, die das Konto erbt, sowie jeder Richtlinie, die direkt mit dem Konto verknüpft ist. Mit Tag-Richtlinien können Sie beispielsweise die effektive Tag-Richtlinie anzeigen, die für jedes Ihrer Konten gilt. Weitere Informationen finden Sie unter Anzeigen effektiver Tag-Richtlinien.

Vererbungsoperatoren

Operatoren, die steuern, wie geerbte Richtlinien zu einer einzigen effektiven Richtlinie zusammengeführt werden. Diese Operatoren gelten als erweitertes Feature. Erfahrene Richtlinienautoren verwenden sie zur Einschränkung der Änderungen, die eine untergeordnete Richtlinie vornehmen darf, und wie Einstellungen in Richtlinien zusammengeführt werden. Weitere Informationen finden Sie unter Vererbungsoperatoren.

Richtliniensyntax und Vererbung für Verwaltungsrichtlinientypen

Wie sich Richtlinien auf die OUs und Konten auswirken, die sie erben, hängt vom Typ der gewählten Verwaltungsrichtlinie ab: Zu den Verwaltungsrichtlinientypen gehören:

- Opt-out-Richtlinien für künstliche Intelligenz-(KI)-Services
- Sicherungsrichtlinien
- Tag-Richtlinien

Die Syntax für Verwaltungsrichtlinientypen enthält Vererbungsoperatoren, mit denen Sie mit feiner Granularität angeben können, welche Elemente aus den übergeordneten Richtlinien angewendet werden und welche Elemente bei der Vererbung durch untergeordnete OUs und Konten überschrieben oder geändert werden können.

Die effektive Richtlinie ist der Satz von Regeln, die vom Organisationsstamm und Organisationsverwalter zusammen mit den direkt an das Konto angefügten Regeln geerbt werden. Die gültige Richtlinie legt die endgültigen Regeln fest, die für das Konto gelten. Sie können die effektive Richtlinie für ein Konto anzeigen, das die Auswirkungen aller Vererbungsoperatoren in den angewendeten Richtlinien enthält. Weitere Informationen finden Sie unter Anzeigen effektiver Tag-Richtlinien.

Vererbungsoperatoren

Vererbungsoperatoren steuern, wie geerbte Richtlinien und Richtlinien von Konten in die effektive Richtlinie des Kontos zusammengeführt werden. Zu diesen Operatoren gehören wertbestimmende Operatoren und untergeordnete Steuerungsoperatoren.

Wenn Sie den visuellen Editor in der AWS Organizations-Konsole verwenden, können Sie nur den `@@assign`-Operator verwenden. Andere Operatoren gelten als erweitertes Feature. Um die anderen Operatoren zu verwenden, müssen Sie die JSON-Richtlinie manuell erstellen. Erfahrene Richtlinienautoren können Vererbungsoperatoren zur Steuerung der Werte verwenden, die auf die effektive Richtlinie angewendet werden sollen, und zur Einschränkung der Änderungen, die untergeordnete Richtlinien vornehmen dürfen.

Wertbestimmende Operatoren

Mithilfe der folgenden wertbestimmenden Operatoren können Sie steuern, wie Ihre Richtlinie mit den übergeordneten Richtlinien interagiert:

- `@@assign` – Überschreibt alle geerbten Richtlinieneinstellungen mit den angegebenen Einstellungen. Wenn die angegebene Einstellung nicht vererbt wird, fügt dieser Operator sie der effektiven Richtlinie hinzu. Dieser Operator kann auf jede beliebige Richtlinieneinstellung jedes Typs angewendet werden.
  - Bei Einstellungen mit nur einem Wert ersetzt dieser Operator den geerbten Wert durch den angegebenen Wert.
  - Bei Einstellungen mit mehreren Werten (JSON-Arrays) entfernt dieser Operator alle geerbten Werte und ersetzt sie durch die in dieser Richtlinie angegebenen Werte.
- `@@append` – Fügt den geerbten Einstellungen die angegebenen Einstellungen hinzu (ohne irgendwelche zu entfernen). Wenn die angegebene Einstellung nicht vererbt wird, fügt dieser Operator sie der effektiven Richtlinie hinzu. Sie können diesen Operator nur mit Einstellungen mit mehreren Werten verwenden.
  - Dieser Operator fügt die angegebenen Werte zu allen Werten in dem geerbten Array hinzu.

- `@@remove` – Entfernt die angegebenen geerbten Einstellungen aus der effektiven Richtlinie, sofern sie vorhanden sind. Sie können diesen Operator nur mit Einstellungen mit mehreren Werten verwenden.
  - Dieser Operator entfernt nur die angegebenen Werte aus dem Array von Werten, die von den übergeordneten Richtlinien geerbt wurden. Andere Werte können weiterhin im Array vorhanden sein und von untergeordneten Richtlinien geerbt werden.

Untergeordnete Steuerungsoperatoren

Die Verwendung von untergeordneten Steuerungsoperatoren ist optional. Mit dem `@@operators_allowed_for_child_policies`-Operator können Sie steuern, welche wertbestimmenden Operatoren untergeordnete Richtlinien verwenden dürfen. Sie können alle Operatoren, bestimmte Operatoren oder keine Operatoren zulassen. Standardmäßig sind alle Operatoren (`@@all`) zulässig.

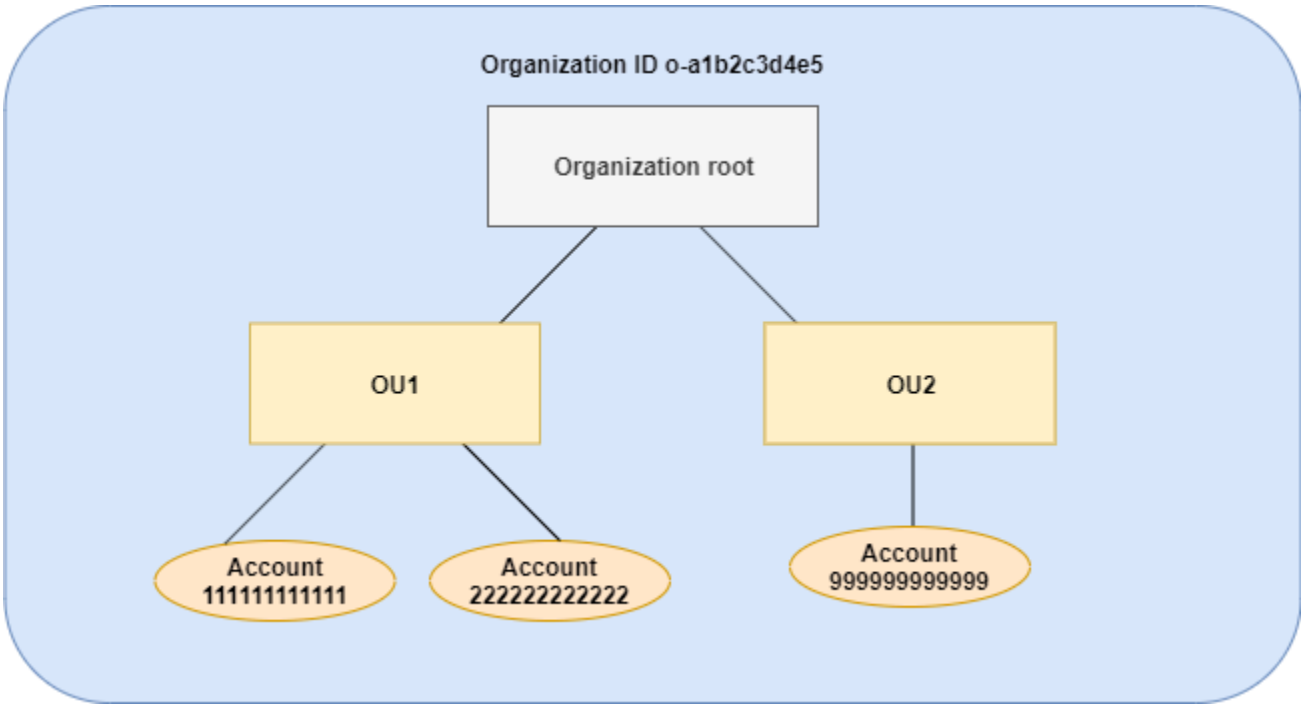
- `"@@operators_allowed_for_child_policies":["@@all"]` – Untergeordnete OUs und Konten können in Richtlinien jeden beliebigen Operator verwenden. Standardmäßig sind alle Operatoren in untergeordneten Richtlinien zulässig.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` – Untergeordnete OUs und Konten können in untergeordneten Richtlinien nur die angegebenen Operatoren verwenden. In diesem untergeordneten Steuerungsoperator können Sie einen oder mehrere wertbestimmende Operatoren angeben.
- `"@@operators_allowed_for_child_policies":["@@none"]` – Untergeordnete OUs und Konten können keine Operatoren in Richtlinien verwenden. Sie können diesen Operator verwenden, um die Werte, die in einer übergeordneten Richtlinie definiert sind, effektiv zu sperren, damit untergeordnete Richtlinien diese Werte nicht hinzufügen, anhängen oder entfernen können.

> **Note**
>
> Wenn ein geerbter untergeordneter Steuerungsoperator die Verwendung eines Operators beschränkt, können Sie diese Regel nicht in einer untergeordneten Richtlinie rückgängig machen. Wenn Sie untergeordnete Steuerungsoperatoren in eine übergeordnete Richtlinie aufnehmen, beschränken diese die wertbestimmenden Operatoren in allen untergeordneten Richtlinien.

Beispiele für Vererbungen

In diesen Beispielen wird gezeigt, wie die Richtlinienvererbung funktioniert, indem übergeordnete und untergeordnete Tag-Richtlinien zu einer effektiven Tag-Richtlinie für ein Konto zusammengeführt werden.

Die Beispiele gehen davon aus, dass Sie die im folgenden Diagramm dargestellte Organisationsstruktur besitzen.



Beispiele

- Beispiel 1: Zulassen, dass untergeordnete Richtlinien nur Tag-Werte überschreiben
- Beispiel 2: Geerbten Tags neue Werte hinzufügen
- Beispiel 3: Entfernen von Werten aus geerbten Tags
- Beispiel 4: Änderungen an untergeordneten Richtlinien einschränken
- Beispiel 5: Konflikte mit untergeordneten Steuerungsoperatoren
- Beispiel 6: Konflikte mit dem Anhängen von Werten auf derselben Hierarchieebene

Beispiel 1: Zulassen, dass untergeordnete Richtlinien nur Tag-Werte überschreiben

Die folgende Tag-Richtlinie definiert den Tag-Schlüssel `CostCenter` und die zulässigen Werte `Development` und `Support`. Wenn Sie diese dem Organisationsstamm anhängen, gilt die Tag-Richtlinie für alle Konten in der Organisation.

Richtlinie A – Tag-Richtlinie des Organisationsstamms

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Angenommen Sie möchten, dass Benutzer in OU1 einen anderen Tag-Wert für einen Schlüssel verwenden, und Sie möchten die Tag-Richtlinie für bestimmte Ressourcentypen durchsetzen. Da Richtlinie A nicht angibt, welche untergeordneten Steuerungsoperatoren zulässig sind, sind alle Operatoren zulässig. Sie können den `@@assign`-Operator verwenden und eine Tag-Richtlinie wie die folgende erstellen, die OU1 hinzugefügt werden soll.

Richtlinie B – OU1-Tag-Richtlinie

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
```

```
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Wenn Sie den `@@assign`-Operator für das Tag angeben, wird bei Zusammenführung von Richtlinie A und Richtlinie B Folgendes ausgeführt, um die effektive Tag-Richtlinie für ein Konto zu bilden:

- Richtlinie B überschreibt die beiden Tag-Werte, die in der übergeordneten Richtlinie (Richtlinie A) angegeben wurden. Dies hat zur Folge, dass `Sandbox` der einzige konforme Wert für den Tag-Schlüssel `CostCenter` ist.
- Das Hinzufügen von `enforced_for` gibt an, dass das `CostCenter`-Tag als angegebener Tag-Wert für alle Amazon-Redshift-Ressourcen und Amazon-DynamoDB-Tabellen verwendet werden muss.

Wie im Diagramm gezeigt, enthält OU1 zwei Konten: 111111111111 und 222222222222.

Resultierende effektive Tag-Richtlinie für die Konten 111111111111 und 222222222222

> **Note**
>
> Sie können den Inhalt einer angezeigten effektiven Richtlinie nicht direkt als Inhalt einer neuen Richtlinie verwenden. Die Syntax enthält nicht die Operatoren, die zum Steuern der Zusammenführung mit anderen untergeordneten und übergeordneten Richtlinien erforderlich sind. Die Anzeige einer effektiven Richtlinie dient nur dazu, die Ergebnisse der Fusion zu verstehen.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
```

```
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Beispiel 2: Geerbten Tags neue Werte hinzufügen

Es kann vorkommen, dass alle Konten in Ihrer Organisation einen Tag-Schlüssel mit einer kurzen Liste zulässiger Werte angeben sollen. Für Konten in einer OU möchten Sie möglicherweise einen zusätzlichen Wert zulassen, den nur diese Konten beim Erstellen von Ressourcen angeben können. In diesem Beispiel wird dargestellt, wie dies mithilfe des `@@append`-Operators durchgeführt wird. Der `@@append`-Operator ist ein erweitertes Feature.

Wie Beispiel 1 beginnt dieses Beispiel mit der Richtlinie A der Tag-Richtlinie des Organisationsstamms.

Richtlinie A – Tag-Richtlinie des Organisationsstamms

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Fügen Sie in diesem Beispiel OU2 die Richtlinie C hinzu. Der Unterschied in diesem Beispiel besteht darin, dass die Verwendung des `@@append`-Operators in Richtlinie C die Liste der zulässigen Werte und die `enforced_for`-Regel erweitert und nicht überschreibt.

Richtlinie C – OU2-Tag-Richtlinie zum Hinzufügen von Werten

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Das Anhängen von Richtlinie C an OU2 hat bei der Zusammenführung von Richtlinie A und Richtlinie C folgende Auswirkungen, um die effektive Tag-Richtlinie für ein Konto zu bilden:

- Da Richtlinie C den `@@append`-Operator enthält, ermöglicht sie das Hinzufügen – nicht aber das Überschreiben – zur Liste der zulässigen Tagwerte, die in Richtlinie A angegeben sind.
- Wie in Richtlinie B gibt das Hinzufügen von `enforced_for` an, dass das `CostCenter`-Tag als der angegebene Tag-Wert für alle Amazon-Redshift-Ressourcen und Amazon-DynamoDB-Tabellen verwendet werden muss. Überschreiben (`@@assign`) und Hinzufügen (`@@append`) haben dieselbe Wirkung, wenn die übergeordnete Richtlinie keinen untergeordneten Steuerungsoperator enthält, der einschränkt, was eine untergeordnete Richtlinie angeben kann.

Wie im Diagramm gezeigt, enthält OU2 ein Konto: 999999999999. Richtlinie A und Richtlinie C werden zusammengeführt, um die effektive Tag-Richtlinie für das Konto 999999999999 zu bilden.

Effektive Tag-Richtlinie für Konto 999999999999

> **Note**
>
> Sie können den Inhalt einer angezeigten effektiven Richtlinie nicht direkt als Inhalt einer neuen Richtlinie verwenden. Die Syntax enthält nicht die Operatoren, die zum Steuern der Zusammenführung mit anderen untergeordneten und übergeordneten Richtlinien erforderlich sind. Die Anzeige einer effektiven Richtlinie dient nur dazu, die Ergebnisse der Fusion zu verstehen.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Beispiel 3: Entfernen von Werten aus geerbten Tags

Es kann Fälle geben, in denen die Tag-Richtlinie, die der Organisation hinzugefügt ist, mehr Tag-Werte definiert, als ein Konto verwenden soll. In diesem Beispiel wird erläutert, wie eine Tag-Richtlinie mit dem Operator `@@remove` überarbeitet wird. `@@remove` ist ein erweitertes Feature.

Wie in den anderen Beispielen beginnt dieses Beispiel mit Richtlinie A der Tag-Richtlinie des Organisationsstamms.

Richtlinie A – Tag-Richtlinie des Organisationsstamms

```
{
    "tags": {
        "costcenter": {
```

```
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

In diesem Beispiel fügen Sie dem Konto 999999999999 Richtlinie D hinzu.

Richtlinie D – Tag-Richtlinie für Konto 999999999999 zum Entfernen von Werten

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

Das Anfügen von Richtlinie D an Konto 999999999999 hat folgende Auswirkungen, wenn Richtlinie A, Richtlinie C und Richtlinie D zusammengeführt werden, um die effektive Tag-Richtlinie zu bilden:

- Unter der Annahme, dass Sie alle vorherigen Beispiele ausgeführt haben, sind Richtlinien B, C und C untergeordnete Richtlinien von A. Richtlinie B ist nur an OU1 angehängt und hat deshalb keine Auswirkung auf Konto 9999999999999.
- Für Konto 999999999999 ist der einzige akzeptable Wert für den `CostCenter`-Tag-Schlüssel `Support`.
- Die Compliance für den `CostCenter`-Tag-Schlüssel wird nicht erzwungen.

Neue effektive Tag-Richtlinie für Konto 999999999999

> **Note**
>
> Sie können den Inhalt einer angezeigten effektiven Richtlinie nicht direkt als Inhalt einer neuen Richtlinie verwenden. Die Syntax enthält nicht die Operatoren, die zum Steuern der Zusammenführung mit anderen untergeordneten und übergeordneten Richtlinien erforderlich sind. Die Anzeige einer effektiven Richtlinie dient nur dazu, die Ergebnisse der Fusion zu verstehen.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Wenn Sie OU2 später weitere Konten hinzufügen, unterscheiden sich ihre effektiven Tag-Richtlinien von denen des Kontos 999999999999. Das liegt daran, weil die restriktivere Richtlinie D nur auf Kontoebene und nicht der OU hinzugefügt ist.

Beispiel 4: Änderungen an untergeordneten Richtlinien einschränken

Es kann vorkommen, dass Sie Änderungen in untergeordneten Richtlinien einschränken möchten. In diesem Beispiel wird erläutert, wie dies mit untergeordneten Steuerungsoperatoren durchgeführt wird.

Dieses Beispiel beginnt mit einer neuen Tag-Richtlinie des Organisationsstamms und setzt voraus, dass Organisations-Entitäten noch keine Tag-Richtlinien hinzugefügt wurden.

Richtlinie E – Tag-Richtlinie des Organisationsstamms zum Einschränken von Änderungen in untergeordneten Richtlinien

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Wenn Sie Richtlinie E an den Organisationsstamm anfügen, verhindert die Richtlinie, dass untergeordnete Richtlinien den `Project`-Tag-Schlüssel ändern. Untergeordnete Richtlinien können jedoch Tag-Werte überschreiben oder hinzufügen.

Angenommen, Sie fügen eine OU der folgende Richtlinie F hinzu.

Richtlinie F – OU-Tag-Richtlinie

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
```

```
            }
        }
    }
}
```

Die Zusammenführung der Richtlinien E und F hat folgende Auswirkungen auf die Konten der OU:

- Richtlinie F ist eine untergeordnete Richtlinie von Richtlinie E.
- Richtlinie F versucht, die Fallbehandlung zu ändern, kann dies aber nicht. Das liegt daran, weil Richtlinie E den `"@@operators_allowed_for_child_policies": ["@@none"]`-Operator für den Tag-Schlüssel enthält.
- Richtlinie F kann jedoch dem Schlüssel Tag-Werte hinzufügen. Das liegt daran, dass Richtlinie E als Tag-Wert `"@@operators_allowed_for_child_policies": ["@@append"]` enthält.

Effektive Richtlinie für Konten in der OU

> **Note**
>
> Sie können den Inhalt einer angezeigten effektiven Richtlinie nicht direkt als Inhalt einer neuen Richtlinie verwenden. Die Syntax enthält nicht die Operatoren, die zum Steuern der Zusammenführung mit anderen untergeordneten und übergeordneten Richtlinien erforderlich sind. Die Anzeige einer effektiven Richtlinie dient nur dazu, die Ergebnisse der Fusion zu verstehen.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Beispiel 5: Konflikte mit untergeordneten Steuerungsoperatoren

Untergeordnete Steuerungsoperatoren können in Tag-Richtlinien vorhanden sein, die auf derselben Ebene in der Organisationshierarchie hinzugefügt sind. In diesem Fall wird bei Zusammenführung der Richtlinien der Schnittmenge der zulässigen Operatoren verwendet, um die effektive Richtlinie für Konten zu bilden.

Angenommen, Richtlinien G und H sind dem Organisationsstamm hinzugefügt.

Richtlinie G – Tag-Richtlinie 1 des Organisationsstamms

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Richtlinie H – Tag-Richtlinie 2 des Organisationsstamms

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

In diesem Beispiel definiert eine Richtlinie am Organisationsstamm, dass die Werte für den Tag-Schlüssel nur angehängt werden können. Mithilfe der anderen, dem Organisationsstamm angehängten Richtlinie können untergeordnete Richtlinien Werte anhängen und entfernen. Die Schnittmenge dieser beiden Berechtigungen wird für untergeordnete Richtlinien verwendet. Im Ergebnis können untergeordnete Richtlinien Werte hinzufügen, jedoch keine Werte entfernen.

Daher kann die untergeordnete Richtlinie der Liste der Tag-Werte einen Wert hinzufügen, den `Maintenance`-Wert jedoch nicht entfernen.

Beispiel 6: Konflikte mit dem Anhängen von Werten auf derselben Hierarchieebene

Sie können jeder Organisations-Entität mehrere Tag-Richtlinien hinzufügen. Wenn Sie dies tun, können die Tag-Richtlinien, die derselben Organisations-Entität angefügt wurden, widersprüchliche Informationen enthalten. Richtlinien werden basierend auf der Reihenfolge, in der sie der Organisations-Entität hinzugefügt wurden, ausgewertet. Um zu ändern, welche Richtlinie zuerst ausgewertet wird, können Sie eine Richtlinie trennen und dann erneut hinzufügen.

Angenommen, Richtlinie J wurde als erste dem Organisationsstamm hinzugefügt, und anschließend Richtlinie K.

Richtlinie J – Erste dem Organisationsstamm hinzugefügte Tag-Richtlinie

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Richtlinie K – Zweite dem Organisationsstamm hinzugefügte Tag-Richtlinie

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

In diesem Beispiel wird der Tag-Schlüssel `PROJECT` in der effektiven Tag-Richtlinie verwendet, da die sie definierende Richtlinie zuerst dem Organisationsstamm hinzugefügt wurde.

Richtlinie JK – Effektive Tag-Richtlinie des Kontos

Die effektive Richtlinie des Kontos lautet wie folgt.

> **Note**
>
> Sie können den Inhalt einer angezeigten effektiven Richtlinie nicht direkt als Inhalt einer neuen Richtlinie verwenden. Die Syntax enthält nicht die Operatoren, die zum Steuern der Zusammenführung mit anderen untergeordneten und übergeordneten Richtlinien erforderlich sind. Die Anzeige einer effektiven Richtlinie dient nur dazu, die Ergebnisse der Fusion zu verstehen.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

Richtlinien zur Abmeldung von KI-Services

AWS-Services für künstliche Intelligenz (KI) wie Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe und Contact Lens für Amazon Connect können ggf. von diesen Services verarbeitete Kundeninhalte speichern und für die Weiterentwicklung und kontinuierliche Verbesserung anderer AWS-Services nutzen. Als AWS-Kunden können Sie sich entscheiden, dass Ihre Inhalte gespeichert oder für Serviceverbesserungen verwendet werden.

> **Note**
>
> AWS-Services für künstliche Intelligenz (KI) müssen Ihre Inhalte möglicherweise speichern, um die Services bereitzustellen. Das gilt auch dann, wenn Sie die Nutzung Ihrer Daten für

Serviceverbesserungen durch AWS deaktivieren. Weitere Informationen finden Sie in der Dokumentation zu dem von Ihnen verwendeten KI-Service.

Anstatt diese Einstellung einzeln für jedes AWS-Konto zu konfigurieren, das Ihre Organisation verwendet, können Sie eine Organisationsrichtlinie konfigurieren, die Ihre Einstellungsauswahl für alle Konten erzwingt, die Mitglieder der Organisation sind. Sie können wählen, ob Sie die Speicherung von Inhalten deaktivieren und für einen einzelnen KI-Service oder für alle abgedeckten Services gleichzeitig verwenden möchten. Sie können die effektive Richtlinie für jedes Konto abfragen, um die Auswirkungen Ihrer Einstellungsoptionen zu sehen.

⚠ Important

- Wenn Sie eine Opt-In- oder Opt-Out-Voreinstellung für einen Service angeben, ist diese Einstellung global und wird auf alle AWS-Regionen angewendet. Festlegen des Werts innerhalb eines AWS-Region repliziert auf alle anderen Regionen.
- Wenn Sie die Nutzung von Inhalten durch einen AWS-KI-Service deaktivieren, löscht dieser Service alle zugehörigen historischen Inhalte, die mit AWS geteilt wurden, bevor Sie die Option festlegen. Diese Löschung sollte auf gespeicherte Daten beschränkt sein, die zur Bereitstellung von Servicefunktionen nicht erforderlich sind.

Erste Schritte mit KI-Services-Opt-Out-Richtlinien

Führen Sie die folgenden Schritte aus, um mit den Opt-Out-Richtlinien für Services für künstliche Intelligenz (KI) zu beginnen.

1. Aktivieren der Abmelderichtlinien für KI-Services für Ihre Organisation.
2. Erstellen einer Richtlinie zur Abmeldung von KI-Services.
3. Fügen Sie die KI-Services-Opt-Out-Richtlinie an den Organisationsstamm, die Organisationseinheit oder das Konto an.
4. Zeigen Sie die kombinierte effektive KI-Services-Opt-Out-Richtlinie an, die für ein Konto gilt.

Für alle diese Schritte melden Sie sich als AWS Identity and Access Management-(IAM)-Benutzer an, übernehmen eine IAM-Rolle oder melden sich als Stammbenutzer (nicht empfohlen) im Verwaltungskonto der Organisation an.

Weitere Informationen

- Erfahren Sie mehr über die Richtliniensyntax für KI-Services und finden Sie Richtlinienbeispiele

So erstellen, aktualisieren und löschen Sie Abmelderichtlinien für KI-Services

In diesem Thema:

- Nach der Aktivierung von KI-Services-Opt-Out-Richtlinien für Ihre Organisation, können Sie eine Tag-Richtlinie erstellen.
- Wenn sich Ihre KI-Services-Opt-Out-Anforderungen ändern, können Sie eine vorhandene Richtlinie aktualisieren.
- Wenn Sie eine Richtlinie nicht mehr benötigen, können Sie sie löschen, nachdem Sie sie von allen Organisationseinheiten (Organizational Units OUs) und Konten getrennt haben.

Erstellen einer Richtlinie zur Abmeldung von KI-Services

> **Mindestberechtigungen**
>
> Zum Erstellen einer KI-Services-Opt-Out-Richtlinie benötigen Sie die Berechtigung zur Ausführung folgender Aktion:
>
> - `organizations:CreatePolicy`

AWS Management Console

Erstellen einer Richtlinie zur Abmeldung von KI-Services

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Services-Opt-Out-Richtlinien die Option Richtlinie erstellen aus.
3. Geben Sie auf der Seite Neue KI-Service-Opt-Out-Richtlinie erstellen einen Richtliniennamen und eine optionale Richtlinienbeschreibung ein.
4. (Optional) Sie können der Richtlinie ein oder mehrere Tags hinzufügen, indem Sie Tag hinzufügen auswählen und dann einen Schlüssel und einen optionalen Wert eingeben. Wenn

Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einer Richtlinie bis zu 50 Tags hinzufügen. Weitere Informationen finden Sie unter Markieren von AWS Organizations-Ressourcen.

5. Geben Sie Richtlinientext auf der Registerkarte JSON oder fügen Sie ihn ein. Weitere Informationen zur Syntax der Opt-out-Richtlinie für KI-Services finden Sie unter Syntax und Beispiele für KI-Services-Opt-Out-Richtlinien. So finden Sie beispielsweise Richtlinien, die Sie als Ausgangspunkt verwenden können, unter Beispiele für Richtlinien zur Deaktivierung von KI-Services.
6. Wenn Sie mit der Bearbeitung Ihrer Richtlinie fertig sind, wählen Sie in der unteren rechten Ecke der Seite Richtlinie erstellen aus.

AWS CLI & AWS SDKs

Erstellen einer Richtlinie zur Abmeldung von KI-Services

Sie können eine der folgenden Optionen verwenden, um eine Tag-Richtlinie zu erstellen:

- AWS CLI: create-policy

1. Erstellen Sie eine KI-Services-Opt-Out-Richtlinie wie die folgende und speichern Sie sie in einer Textdatei. Beachten Sie, dass bei „`optOut`“ und „`optIn`“ die Groß-/Kleinschreibung beachtet wird.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Diese Opt-Out-Richtlinie für KI-Services legt fest, dass alle von der Richtlinie betroffenen Konten von allen KI-Services mit Ausnahme von Amazon Rekognition abgemeldet werden.

2. Importieren Sie die JSON-Richtliniendatei, um eine neue Richtlinie in der Organisation zu erstellen. In diesem Beispiel wurde die vorherige JSON-Datei `policy.json` benannt.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWS-SDKs: CreatePolicy

Weitere Vorgehensweisen

Nachdem Sie eine Richtlinie für KI-Services erstellt haben, können Sie Ihre Opt-out-Optionen in Kraft setzen. Dies ist möglich durch Anfügen der Richtlinie an den Organisationsstamm, die Organisationseinheiten (OUs), die AWS-Konten innerhalb Ihrer Organisation oder einer Kombination hiervon.

Aktualisieren einer Richtlinie zur Abmeldung von KI-Services

> **Mindestberechtigungen**
>
> Um eine KI-Services-Opt-Out-Richtlinie zu aktualisieren, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:

- `organizations:UpdatePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")
- `organizations:DescribePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den Amazon-Ressourcennamen (ARN) für die angegebene Richtlinie enthält (oder „*“)

AWS Management Console

Aktualisieren einer Richtlinie zur Abmeldung von KI-Services

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Services-Opt-Out-Richtlinien den Namen der Richtlinie aus, die Sie aktualisieren möchten.
3. Wählen Sie auf der Detailseite der Richtlinie Richtlinie bearbeiten aus.
4. Sie können einen neuen Richtliniennamen oder eine Richtlinienbeschreibung eingeben oder den JSON-Richtlinientext bearbeiten. Weitere Informationen zur Syntax der Opt-out-Richtlinie für KI-Services finden Sie unter Syntax und Beispiele für KI-Services-Opt-Out-Richtlinien. So finden Sie beispielsweise Richtlinien, die Sie als Ausgangspunkt verwenden können, unter Beispiele für Richtlinien zur Deaktivierung von KI-Services.
5. Wenn Sie mit der Aktualisierung der Richtlinie fertig sind, wählen Sie Save changes (Änderungen speichern) aus.

AWS CLI & AWS SDKs

So aktualisieren Sie eine Richtlinie

Zum Aktualisieren einer Richtlinie können Sie einen der folgenden Befehle verwenden:

- AWS CLI: update-policy

  Im folgenden Beispiel wird eine Richtlinie zum Abmelden von KI-Services umbenannt.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
```

```
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

Im folgenden Beispiel wird die Beschreibung einer KI-Services-Opt-Out-Richtlinie hinzugefügt oder geändert.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

Im folgenden Beispiel wird das JSON-Richtliniendokument geändert, das einer KI-Service-Opt-Out-Richtlinie zugeordnet ist. In diesem Beispiel wird der Inhalt einer Datei namens `policy.json` mit folgendem Text entnommen:

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n}\n"}
}
```

- AWS-SDKs: UpdatePolicy

Bearbeiten von Tags, die an eine AI-Service-Opt-Out-Richtlinie angehängt sind

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie die Tags hinzufügen oder entfernen, die einer KI-Services-Opt-Out-Richtlinie zugeordnet sind. Weitere Informationen über das Markieren mit Tags finden Sie unter Markieren von AWS Organizations-Ressourcen.

> **Mindestberechtigungen**
>
> Um die an eine KI-Services-Opt-Out-Richtlinie in Ihrer AWS-Organisation angefügten Tags zu bearbeiten, müssen Sie über die folgenden Berechtigungen verfügen:
>
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:DescribePolicy` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

So bearbeiten Sie die Tags, die an eine AI-Service-Opt-Out-Richtlinie angehängt sind

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Services-Opt-Out-Richtlinien den Namen der Richtlinie mit den Tags aus, die Sie bearbeiten möchten.
3. Wählen Sie auf der Detailseite der ausgewählten Richtlinie die Registerkarte Tags und dann Tags verwalten aus.
4. Sie können auf dieser Seite eine der folgenden Aktionen ausführen:
   - Bearbeiten Sie den Wert für ein beliebiges Tag, indem Sie einen neuen Wert über dem alten eingeben. Sie können den Schlüssel nicht ändern. Um einen Schlüssel zu ändern, müssen Sie das Tag mit dem alten Schlüssel löschen und ein Tag mit dem neuen Schlüssel hinzufügen.
   - Entfernen Sie ein vorhandenes Tag, indem Sie Entfernen wählen.

- Fügen Sie ein neues Tag-Schlüssel-Wert-Paar hinzu. Wählen Sie Tag hinzufügen aus und geben Sie dann den neuen Schlüsselnamen und den optionalen Wert in die bereitgestellten Felder ein. Wenn Sie das Feld Wert leer lassen, ist der Wert eine leere Zeichenfolge; er ist nicht `null`.

5. Wählen Sie Änderungen speichern, nachdem Sie alle gewünschten Ergänzungen, Entfernungen und Änderungen vorgenommen haben.

AWS CLI & AWS SDKs

So bearbeiten Sie die Tags, die an eine KI-Service-Opt-Out-Richtlinie angehängt sind

Sie können einen der folgenden Befehle verwenden, um die einer KI-Services-Opt-Out-Richtlinie zugeordneten Tags zu bearbeiten:

- AWS CLI: tag-resource und untag-resource
- AWS-SDKs: TagResource und UntagResource

Löschen einer Richtlinie zur Abmeldung von KI-Services

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Richtlinie löschen, die Sie in Ihrer Organisation nicht mehr benötigen.

Bevor Sie eine Richtlinie löschen können, müssen Sie sie zuerst von allen angehängten Elementen trennen.

Mindestberechtigungen

Um eine Richtlinie zu löschen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:

- `organizations:DescribePolicy` (Nur Konsole – um zur Richtlinie zu navigieren)
- `organizations:DeletePolicy`

AWS Management Console

Löschen einer Richtlinie zur Abmeldung von KI-Services

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Services-Opt-Out-Richtlinien den Namen der Richtlinie aus, die Sie löschen möchten.
3. Sie müssen zuerst die Richtlinie, die Sie löschen möchten, von allen Stammverzeichnissen, Organisationseinheiten und Konten trennen. Wählen Sie die Registerkarte Ziele aus, wählen Sie das Optionsfeld neben jedem Stamm, jeder OU oder jedem Konto aus, die in der Liste Ziele angezeigt werden und wählen Sie dann Trennen. Wählen Sie im Bestätigungsdialogfeld Trennen aus. Wiederholen Sie dies, bis Sie alle Ziele entfernt haben.
4. Wählen Sie oben auf der Seite Löschen.
5. Geben Sie im Bestätigungsdialogfeld den Namen der Richtlinie ein und wählen Sie dann Löschen aus.

AWS CLI & AWS SDKs

Löschen einer Richtlinie zur Abmeldung von KI-Services

Zum Löschen einer Tag-Richtlinie können Sie eine der folgenden Optionen verwenden:

- AWS CLI: delete-policy

  Im folgenden Beispiel wird die angegebene Richtlinie gelöscht. Sie funktioniert nur, wenn die Richtlinie keinem Stamm, keiner Organisationseinheit oder keinem Konto angefügt ist.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: DeletePolicy

Zuordnen und Trennen von KI-Service-Opt-Out-Richtlinien

Sie können Opt-Out-Richtlinien für künstliche Intelligenz (KI) sowohl für eine ganze Organisation als auch für Organisationseinheiten (OUs) und einzelne Konten verwenden. Worauf die KI-Services-Opt-Out-Richtlinie angewendet wird, hängt davon ab, an welches Organisationselement Sie es anfügen:

- Wenn Sie eine KI-Services-Opt-Out-Richtlinie an den Organisationsstamm anfügen, gilt die Richtlinie für alle Organisationseinheiten und Konten der Stammmitglieder.
- Wenn Sie eine KI-Services-Opt-Out-Richtlinie an eine Organisationseinheit (OU) anfügen, gilt diese Richtlinie für die Konten, die zu der OU oder einer ihrer untergeordneten Organisationseinheiten gehören. Diese Konten unterliegen auch jeder Richtlinie, die an den Organisationsstamm angefügt ist.
- Wenn Sie eine KI-Services-Opt-Out-Richtlinie an ein Konto, anfügen, gilt diese Richtlinie nur für dieses Konto. Das Konto unterliegt auch jeder Richtlinie, die an den Organisationsstamm und alle Organisationseinheiten angefügt ist, zu denen das Konto gehört.

Die Aggregation aller KI-Services-Opt-Out-Richtlinien, die das Konto vom Stamm und den übergeordneten Organisationseinheiten erbt, sowie aller Richtlinien, die direkt an das Konto angefügt sind, ist die effektive Richtlinie. Weitere Informationen zur Zusammenführung von Richtlinien zu einer effektiven Richtlinie finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

> **Mindestberechtigungen**
>
> Um KI-Services-Opt-Out-Richtlinien anzuhängen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:
>
> - `organizations:AttachPolicy`

AWS Management Console

Sie können eine Richtlinie für eine KI-Services anfügen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, an das Sie die Richtlinie anfügen möchten, navigieren.

So fügen Sie eine Richtlinie für die Abmeldung von KI-Services an, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, dem Sie eine Richtlinie anfügen möchten, und wählen Sie dann den Namen aus. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Eintrag für KI-Services-Opt-Out-Richtlinien die Option Anfügen.
4. Suchen Sie die gewünschte Richtlinie und wählen Sie Richtlinie anfügen aus.

   Die Liste der angehängten KI-Services-Opt-Out-Richtlinien auf der Registerkarte Richtlinien wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

So fügen Sie eine Deaktivierungsrichtlinie für KI-Services an, indem Sie zur Richtlinie navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Services-Opt-Out-Richtlinien den Namen der Richtlinie aus, die Sie anfügen möchten.
3. Klicken Sie in der Registerkarte Ziele auf Anfügen.
4. Aktivieren Sie das Optionsfeld neben dem Stammverzeichnis, der Organisationseinheit oder dem Konto, an das bzw. die Sie die Richtlinie anfügen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
5. Wählen Sie Attach policy (Richtlinie anfügen) aus.

Die Liste der angehängten KI-Services-Opt-Out-Richtlinien auf der Registerkarte Ziele wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So fügen Sie eine Deaktivierungsrichtlinie für KI-Services an das Stammverzeichnis, die OU oder das Konto der Organisation an

Sie können eine der folgenden Optionen verwenden, um eine Richtlinie für eine KI-Services hinzuzufügen, um eine Opt-out-Richtlinie hinzuzufügen:

- AWS CLI: attach-policy

  Im folgenden Beispiel wird eine Richtlinie einer Organisationseinheit angefügt.

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: AttachPolicy

Die Richtlinienänderung wird sofort wirksam.

Trennen einer Richtlinie zur Abmeldung von KI-Services

Wenn Sie im Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine KI-Services-Opt-Out-Richtlinie vom Organisationsstamm, der OU oder vom Konto, dem sie hinzugefügt ist, trennen. Nach dem Trennen der KI-Services-Opt-Out-Richtlinie von einem Element, gilt diese Richtlinie nicht mehr für Konten, auf die sich das jetzt getrennte Element zuvor ausgewirkt hat. Führen Sie zum Trennen einer Richtlinie die folgenden Schritte aus.

> **Mindestberechtigungen**
>
> Um eine KI-Services-Opt-Out-Richtlinie vom Organisationsstamm, der OU oder dem Konto zu trennen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:

- `organizations:DetachPolicy`

AWS Management Console

Sie können eine Richtlinie für eine KI-Services trennen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, von denen Sie die Richtlinie trennen möchten, navigieren.

So trennen Sie eine Richtlinie für die Abmeldung von KI-Services, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren, an die sie angefügt ist

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, von dem Sie eine Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. Wählen Sie den Namen des Stamms, der Organisationseinheit oder des Kontos aus.
3. Wählen Sie auf der Registerkarte Richtlinien das Optionsfeld neben der KI-Services-Opt-Out-Richtlinie aus, die Sie trennen möchten und wählen Sie dann Trennen aus.
4. Wählen Sie im Bestätigungsdialogfeld Richtlinie trennen aus.

   Die Liste der angehängten Abmelderichtlinien für KI-Services wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

So trennen Sie eine Deaktivierungsrichtlinie für KI-Services, indem Sie zur Richtlinie navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite KI-Service-Opt-Out-Richtlinien den Namen der Richtlinie aus, die Sie von einem Stamm, einer OU oder einem Konto trennen möchten.

3. Wählen Sie auf der Registerkarte Ziele das Optionsfeld neben dem Stamm, der OU oder dem Konto aus, von dem Sie die Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
4. Wählen Sie Detach (Trennen) aus.
5. Wählen Sie im Bestätigungsdialogfeld Trennen aus.

   Die Liste der angehängten Abmelderichtlinien für KI-Services wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So trennen Sie eine Deaktivierungsrichtlinie für KI-Services an das Stammverzeichnis, die OU oder das Konto der Organisation

Sie können eine der folgenden Optionen verwenden, um eine Richtlinie für eine KI-Services-Opt-out-Richtlinie zu trennen:

- AWS CLI: detach-policy

  Im folgenden Beispiel wird eine Richtlinie von einer Organisationseinheit entfernt.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-SDKs: DetachPolicy

Die Richtlinienänderung wird sofort wirksam.

Effektive Abmelderichtlinien für KI-Services anzeigen

Bestimmen Sie die effektive Richtlinie für Services für künstliche Intelligenz (KI) für ein Konto in Ihrer Organisation.

Was ist die effektive KI-Services Opt-Out-Richtlinie?

Die Effektive KI-Services-Opt-Out-Richtlinie gibt die endgültigen Regeln an, die für eine AWS-Konto gültig sind. Es handelt sich um die Aggregation aller Opt-out-Richtlinien für KI-Services, die das Konto übernimmt, sowie alle Opt-out-Richtlinien für KI-Services, die direkt mit dem Konto verbunden sind. Wenn Sie eine KI-Services-Opt-Out-Richtlinie an den Organisationsstamm anfügen, gilt diese für alle Konten in Ihrer Organisation. Wenn Sie eine KI-Services-Opt-Out-Richtlinie an eine OU anfügen, gilt diese für alle Konten und OUs, die zu der OU gehören. Wenn Sie eine Richtlinie direkt an ein Konto anfügen, gilt diese nur für das betreffende AWS-Konto.

Beispielsweise kann die Deaktivierungsrichtlinie für KI-Services, die dem Stamm der Organisation zugeordnet ist, festlegen, dass alle Konten in der Organisation die Nutzung von Inhalten durch alle AWS-Services für Machine Learning deaktivieren. Eine separate KI-Services-Opt-out-Richtlinie, die direkt einem Mitgliedskonto zugeordnet ist, gibt an, dass es sich für die Inhaltsverwendung nur für Amazon Rekognition. Die Kombination dieser KI-Services-Opt-Out-Richtlinien umfasst die effektive KI-Services-Opt-Out-Richtlinie. Das Ergebnis ist, dass alle Konten in der Organisation von allenAWS-Services, mit Ausnahme eines Kontos, das sich für Amazon Rekognition.

Weitere Informationen dazu, wie Richtlinien zu der endgültigen effektiven Richtlinie kombiniert werden, finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

So zeigen Sie die wirksame Deaktivierungsrichtlinie für KI-Services an

Sie können die effektive KI-Services-Opt-Out-Richtlinie für ein Konto über die AWS Management Console, AWS API oder AWS Command Line Interface anzeigen.

> **Mindestberechtigungen**
>
> Um die effektive KI-Services-Opt-Out-Richtlinie für ein Konto anzuzeigen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:
>
> - `organizations:DescribeEffectivePolicy`
> - `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So zeigen Sie die effektive Richtlinie für KI-Services an, die für ein Konto an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite AWS-Konten den Namen des Kontos aus, für das Sie die effektive KI-Services-Opt-Out-Richtlinie anzeigen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Abschnitt KI-Services-Opt-Out-Richtlinien die Option Effektive Tag-Richtlinie für dieses AWS-Konto anzeigen aus.

   Die Konsole zeigt die effektive Richtlinie an, die auf das angegebene Konto angewendet wird.

   > **Note**
   >
   > Es ist nicht möglich, eine effektive Richtlinie zu kopieren und einzufügen und ohne wesentliche Änderungen als JSON für eine andere KI-Services-Opt-Out-Richtlinie zu verwenden. KI-Services-Opt-Out-Richtliniendokumente müssen die Vererbungsoperatoren enthalten, die angeben, wie die einzelnen Einstellungen zu der endgültigen effektiven Richtlinie zusammengeführt werden.

AWS CLI & AWS SDKs

So zeigen Sie die effektive Richtlinie für KI-Services an, die für ein Konto an

Sie können eine der folgenden Optionen zum Anzeigen der effektiven KI-Services-Opt-Out-Richtlinie verwenden:

- AWS CLI: describe-effective-policy

  Das folgende Beispiel zeigt die effektive KI-Services-Opt-Out-Richtlinie für ein Konto.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
```

```
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWS-SDKs: DescribeEffectivePolicy

Syntax und Beispiele für KI-Services-Opt-Out-Richtlinien

In diesem Thema wird die Syntax der Deaktivierungsrichtlinie für Services der künstlichen Intelligenz (KI) beschrieben und Beispiele bereitgestellt.

Richtliniensyntax zur Abmeldung von KI-Services

Eine KI-Services-Deaktivierungs-Richtlinie ist eine Textdatei, die den Regeln der JSON-Struktur folgt. Die Syntax für KI-Services-Deaktivierungs-Richtlinien folgt der Syntax für Verwaltungsrichtlinientypen. Eine umfassende Erläuterung dieser Syntax finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen. Dieses Thema konzentriert sich auf die Anwendung dieser allgemeinen Syntax auf die spezifischen Anforderungen des KI-Services-Opt-Out-Richtlinientyps.

> **Important**
>
> Wichtig ist die Großschreibung der in diesem Abschnitt beschriebenen Werte. Geben Sie die Werte mit Groß- und Kleinbuchstaben ein, wie in diesem Thema gezeigt. Die Richtlinien funktionieren nicht, wenn Sie unerwartete Großschreibung verwenden.

Die folgende Richtlinie zeigt die grundlegende Richtliniensyntax für KI-Services-Opt-Out Wenn dieses Beispiel direkt an ein Konto angefügt wäre, würde dieses Konto explizit von einem Service abmelden und sich für einen anderen anmelden. Andere Services können durch Richtlinien, die von höheren Ebenen geerbt werden (OU oder Stammrichtlinien), abgeschaltet werden.

```
{
    "services": {
        "rekognition": {
```

```
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Stellen Sie sich die folgende Beispielrichtlinie vor, die an den Organisationsstamm angefügt ist. Es legt die Standardeinstellung für die Organisation fest, dass alle KI-Services deaktiviert werden. Dies schließt automatisch alle KI-Services ein, die nicht anderweitig ausdrücklich ausgenommen sind, einschließlich aller KI-Services, die AWS in Zukunft bereitstellen könnte. Sie können untergeordnete Richtlinien an Organisationseinheiten oder direkt an Konten anfügen, um diese Einstellung für alle KI-Services außer Amazon Comprehend zu überschreiben. Der zweite Eintrag im folgenden Beispiel verwendet `@@operators_allowed_for_child_policies` auf `none` gesetzt, um zu verhindern, dass er überschrieben wird. Der dritte Eintrag im Beispiel stellt eine organisationsweite Befreiung für Amazon Rekognition. Es wird in der gesamten Organisation für diesen Service entschieden, aber die Richtlinie erlaubt, untergeordnete Richtlinien gegebenenfalls außer Kraft zu setzen.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
```

```
}
```

Die Syntax der Deaktivierungsrichtlinie für KI-Services umfasst die folgenden Elemente:

- Das `services`-Element. Eine KI-Service-Opt-Out-Richtlinie wird durch diesen festen Namen als das äußerste JSON-Element identifiziert, das enthält.

  Eine KI-Services-Opt-Out-Richtlinie kann eine oder mehrere Anweisungen unter dem `services`-Element haben. Jede Anweisung enthält die folgenden Elemente:

  - Ein Servicenamenschlüssel, der einen AWS-KI-Service identifiziert. Die folgenden Schlüsselnamen sind gültige Werte für dieses Feld:
    - **`default`**— stellt alle derzeit verfügbaren KI-Services dar und schließt implizit und automatisch alle KI-Services ein, die in Zukunft hinzugefügt werden könnten.
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`
    - `connectamd`
    - `connectoptimization`
    - `contactlens`
    - `datazone`
    - `frauddetector`
    - `guardduty`
    - `lex`
    - `polly`
    - `q`
    - `quicksightq`
    - `rekognition`
    - `securitylake`
    - `textract`
    - `transcribe`

- `translate`

Jede Richtlinienanweisung, die durch einen Servicenamenschlüssel identifiziert wird, kann die folgenden Elemente enthalten:

- Der `opt_out_policy`-Schlüssel Dieser Schlüssel muss vorhanden sein. Dies ist der einzige Schlüssel, den Sie unter einem Service-Name-Schlüssel platzieren können.

  Der `opt_out_policy`-Schlüssel kann nur den `@@assign`-Operator mit einem der folgenden Werte enthalten:

  - `optOut` – Sie entscheiden sich für die Verwendung von Inhalten für den angegebenen KI-Service.
  - `optIn` – Sie entscheiden sich für die Inhaltsverwendung für den angegebenen KI-Service.

  > **Hinweise**
  >
  > - Sie können die Vererbungsoperatoren `@@append` und `@@remove` nicht in Deaktivierungsrichtlinien für KI-Services verwenden.
  > - Sie können den `@@enforced_for`-Operator nicht in den Deaktivierungsrichtlinien für KI-Services verwenden.

- Auf jeder Ebene können Sie den `@@operators_allowed_for_child_policies`-Operator angeben, der steuert, was untergeordnete Richtlinien tun können, um die von übergeordneten Richtlinien auferlegten Einstellungen zu überschreiben. Sie können einen der folgenden Werte angeben:

  - `@@assign` – Untergeordnete Richtlinien dieser Richtlinie können den `@@assign`-Operator verwenden, um den geerbten Wert mit einem anderen Wert zu überschreiben.
  - `@@none` – Die untergeordneten Richtlinien dieser Richtlinie können den Wert nicht ändern.

  Das Verhalten der `@@operators_allowed_for_child_policies` hängt davon ab, wo Sie sie platzieren. Sie können die folgenden Speicherorte verwenden:

  - Unter dem `services`-Schlüssel – steuert, ob eine untergeordnete Richtlinie die Liste der Services in der wirksamen Richtlinie hinzufügen oder ändern kann.
  - Unter dem Schlüssel für einen bestimmten KI-Service oder dem `default`-Schlüssel – steuert, ob eine untergeordnete Richtlinie die Liste der Schlüssel unter diesem bestimmten Eintrag hinzufügen oder ändern kann.

- Unter dem `opt_out_policies`-Schlüssel für einen bestimmten Service – steuert, ob eine untergeordnete Richtlinie nur die Einstellung für diesen bestimmten Service ändern kann.

Beispiele für Richtlinien zur Deaktivierung von KI-Services

Die folgenden Richtlinienbeispiele dienen nur zu Informationszwecken.

Beispiel 1: Abmelden aller AI-Services für alle Konten in der Organisation

Das folgende Beispiel zeigt eine Richtlinie, die Sie dem Stammverzeichnis Ihrer Organisation hinzufügen können, um KI-Services für Konten in Ihrer Organisation zu deaktivieren.

> **Tip**
>
> Wenn Sie das folgende Beispiel mit der Schaltfläche Kopieren in der oberen rechten Ecke des Beispiels kopieren, enthält die Kopie die Zeilennummern nicht. Es ist fertig zum Einfügen.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – Die `"@@operators_allowed_for_child_policies": ["@@none"]` unter `services` verhindert, dass eine untergeordnete Richtlinie neue Abschnitte für einzelne Services außer dem bereits vorhandenen Abschnitt `default` hinzufügt. `Default` ist der Platzhalter, der „alle KI-Services“ darstellt.
- [2] – Die `"@@operators_allowed_for_child_policies": ["@@none"]` unter `default` verhindert, dass eine untergeordnete Richtlinie neue Abschnitte außer dem bereits vorhandenen `opt_out_policy`-Abschnitt hinzufügt.

- [3] — Die `"@@operators_allowed_for_child_policies": ["@@none"]` unter `opt_out_policy` verhindert, dass untergeordnete Richtlinien den Wert der `optOut`-Einstellung ändern oder zusätzliche Einstellungen hinzufügen.

Beispiel 2: Festlegen einer Organisationsstandardeinstellung für alle Services, aber untergeordnete Richtlinien dürfen die Einstellung für einzelne Services außer Kraft setzen

Die folgende Beispielrichtlinie legt einen organisationsweiten Standard für alle AI-Services fest. Der Wert für `default` verhindert, dass eine untergeordnete Richtlinie den `optOut`-Wert für Service `default`, den Platzhalter für alle KI-Services, ändert. Wenn diese Richtlinie als übergeordnete Richtlinie angewendet wird, indem sie an den Stamm oder eine Organisationseinheit angehängt wird, können untergeordnete Richtlinien weiterhin die Deaktivierungs-Einstellung für einzelne Services ändern, wie in der zweiten Richtlinie dargestellt.

- Da unter dem Schlüssel `"@@operators_allowed_for_child_policies": ["@@none"]` kein `services` steht, können untergeordnete Richtlinien neue Abschnitte für einzelne Services hinzufügen.
- Die `"@@operators_allowed_for_child_policies": ["@@none"]` unter `default` verhindert, dass eine untergeordnete Richtlinie neue Abschnitte außer dem bereits vorhandenen `opt_out_policy`-Abschnitt hinzufügt.
- Die `"@@operators_allowed_for_child_policies": ["@@none"]` unter `opt_out_policy` verhindert, dass untergeordnete Richtlinien den Wert der `optOut`-Einstellung ändern oder zusätzliche Einstellungen hinzufügen.

Übergeordnete Richtlinie zur Abmeldung von KI-Services im Organisationsstamm

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

In der folgenden Beispielrichtlinie wird davon ausgegangen, dass die vorherige Beispielrichtlinie entweder dem Organisationsstamm oder einer übergeordneten Organisationseinheit zugeordnet ist und dass Sie dieses Beispiel einem Konto zuordnen, das von der übergeordneten Richtlinie betroffen ist. Es überschreibt die standardmäßige Abmeldungs-Einstellung und meldet sich explizit nur für den Amazon-Lex-Service an.

Untergeordnete Richtlinie zur Abmeldung von KI-Services

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Die daraus resultierende effektive Richtlinie für AWS-Konto besteht darin, dass sich das Konto nur für Amazon Lex anmeldet und alle anderen AWS-KI-Services aufgrund der von der übergeordneten Richtlinie übernommenen `default`-Deaktivierungseinstellung ablehnt.

Beispiel 3: Definieren einer organisationsweiten KI-Services-Opt-Out-Richtlinie für einen einzelnen Service

Das folgende Beispiel zeigt eine Deaktivierungsrichtlinie für KI-Services, die eine `optOut`-Einstellung für einen einzelnen KI-Service definiert. Wenn diese Richtlinie an das Stammverzeichnis der Organisation angefügt ist, verhindert sie, dass eine untergeordnete Richtlinie die `optOut`-Einstellung für diesen einen Service überschreibt. Andere Services werden von dieser Richtlinie nicht behandelt, können jedoch von untergeordneten Richtlinien in anderen Organisationseinheiten oder Konten betroffen sein.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
```

```
    }
}
```

Backup-Richtlinien

Mithilfe von AWS Backup können Sie Backup-Pläne erstellen, die festlegen, wie Ihre AWS-Ressourcen gesichert werden sollen. Die Regeln in dem Plan umfassen eine Vielzahl von Einstellungen, z. B. die Backup-Häufigkeit, das Zeitfenster, in dem der Backup erfolgt, die AWS-Region mit den zu sichernden Ressourcen und den Tresor, in dem der Backup gespeichert werden soll. Sie können dann einen Backup-Plan auf Gruppen von AWS-Ressourcen anwenden, die mithilfe von Tags identifiziert wurden. Sie müssen auch eine AWS Identity and Access Management-(IAM)-Rolle identifizieren, die AWS Backup die Berechtigung zum Ausführen der Backup-Operation in Ihrem Namen erteilt.

Die Backup-Richtlinien in AWS Organizations kombinieren alle diese Teile in JSON-Textdokumenten. Sie können eine Backup-Richtlinie an jedes Element in der Struktur Ihrer Organisation anfügen, beispielsweise an das Stammverzeichnis, Organisationseinheiten (OUs) und einzelne Konten. Organizations wenden Vererbungsregeln an, um die Richtlinien im Organisationsstamm, die Richtlinien in allen übergeordneten Organisationseinheiten oder die dem Konto angefügten Richtlinien zu kombinieren. Das Ergebnis ist eine effektive Backup-Richtlinie für jedes Konto. Diese effektive Richtlinie weist AWS Backup an, wie Ihre AWS-Ressourcen automatisch gesichert werden sollen.

Backup-Richtlinien ermöglichen Ihnen eine präzise Kontrolle über den Backup Ihrer Ressourcen auf der Ebene, die Ihre Organisation benötigt. Sie können beispielsweise in einer dem Organisationsstamm angefügten Richtlinie angeben, dass alle Amazon-DynamoDB-Tabellen gesichert werden müssen. In dieser Richtlinie kann eine Standard-Backup-Häufigkeit angegeben sein. Sie können dann eine Backup-Richtlinie an Organisationseinheiten anfügen, die die Backup-Häufigkeit entsprechend den Anforderungen jeder Organisationseinheit überschreiben. So könnte die Organisationseinheit `Developers` beispielsweise eine Backup-Häufigkeit von einmal pro Woche angeben, während die Organisationseinheit `Production` einmal täglich angibt.

Sie können partielle Backup-Richtlinien erstellen, die jeweils nur einen Teil der erforderlichen Informationen für den erfolgreichen Backup Ihrer Ressourcen enthalten. Sie können diese Richtlinien an verschiedene Teile der Organisationsstruktur anfügen, beispielsweise an das Stammverzeichnis oder eine übergeordnete Organisationseinheit, mit der Absicht, dass diese partiellen Richtlinien von untergeordneten Organisationseinheiten und Konten geerbt werden. Wenn Organizations alle Richtlinien für ein Konto mithilfe von Vererbungsregeln kombiniert, muss die daraus resultierende

effektive Richtlinie über alle erforderlichen Elemente verfügen. Andernfalls betrachtet AWS Backup die Richtlinie als ungültig und sichert die betroffenen Ressourcen nicht.

> **Important**
>
> AWS Backup kann nur ein erfolgreiches Backup durchführen, wenn diese von einer vollständigen effektiven Richtlinie, die alle erforderlichen Elemente enthält, aufgerufen wird. Obwohl eine partielle Richtlinienstrategie wie oben beschrieben funktionieren kann, führt dies zu Fehlern oder Ressourcen, die nicht erfolgreich gesichert werden, wenn eine effektive Richtlinie für ein Konto unvollständig ist. Als alternative Strategie sollten Sie erwägen, zu verlangen, dass alle Backup-Richtlinien für sich genommen vollständig und gültig sind. Verwenden Sie Standardwerte, die von Richtlinien bereitgestellt werden, die an höherer Stelle in der Hierarchie angefügt sind, und überschreiben Sie diese bei Bedarf in untergeordneten Richtlinien, indem Sie untergeordnete Steuerungsoperatoren für die Vererbung einschließen.

Der effektive Backup-Plan für jedes AWS-Konto in der Organisation wird in der AWS Backup-Konsole als unveränderlicher Plan für das betreffende Konto angezeigt. Sie können ihn sehen, aber nicht ändern.

Wenn AWS Backup ein Backup auf der Grundlage eines von Richtlinien erstellten Backup-Plans beginnt, können Sie den Status der Backup-Aufgabe in der AWS Backup-Konsole anzeigen. Ein Benutzer in einem Mitgliedskonto kann den Status und alle Fehler für die Backup-Aufgaben in diesem Mitgliedskonto anzeigen. Wenn Sie auch den vertrauenswürdigen Servicezugriff mit AWS Backup aktivieren, kann ein Benutzer im Verwaltungskonto der Organisation den Status und Fehler für alle Backup-Aufgaben in der Organisation anzeigen. Weitere Informationen finden Sie unter Aktivieren der kontoübergreifenden Verwaltung im AWS Backup-Entwicklerhandbuch.

Erste Schritte mit Backup-Richtlinien

Führen Sie die folgenden Schritte für den Einstieg in die Verwendung von Backup-Richtlinien aus.

1. Erfahren Sie mehr über die Berechtigungen, die Sie zum Ausführen von Backup-Richtlinienaufgaben benötigen.
2. Informieren Sie sich über einige bewährte Methoden, die wir bei der Verwendung von Backup-Richtlinien empfehlen.
3. Aktivieren Sie Backup-Richtlinien für Ihre Organisation.
4. Erstellen Sie eine Backup-Richtlinie.

5. Fügen Sie die Backup-Richtlinie an den Organisationsstamm, die Organisationseinheit oder das Konto an.
6. Zeigen Sie die kombinierte effektive Backup-Richtlinie an, die für ein Konto gilt.

Für alle diese Schritte melden Sie sich als IAM-Benutzer an, übernehmen eine IAM-Rolle oder melden sich als Stammbenutzer (nicht empfohlen) im Verwaltungskonto der Organisation an.

Weitere Informationen

- Informationen zur Syntax von Sicherungsrichtlinien und Beispielrichtlinien

Voraussetzungen und Berechtigungen zum Verwalten von Backup-Richtlinien

Auf dieser Seite werden die Voraussetzungen und erforderlichen Berechtigungen zur Verwaltung von Backup-Richtlinien in beschrieben AWS Organizations.

Themen

- Voraussetzungen für die Verwaltung von Backup-Richtlinien
- Berechtigungen zur Verwaltung von Backup-Richtlinien

Voraussetzungen für die Verwaltung von Backup-Richtlinien

Für die Verwaltung von Backup-Richtlinien in einer Organisation müssen folgende Voraussetzungen erfüllt sein:

- Für Ihre Organisation müssen alle Funktionen aktiviert sein.
- Sie müssen im Verwaltungskonto Ihrer Organisation angemeldet sein.
- Ihr AWS Identity and Access Management-(IAM)-Benutzer oder Ihre Rolle benötigt die im folgenden Abschnitt aufgeführten Berechtigungen.

Berechtigungen zur Verwaltung von Backup-Richtlinien

Die folgende IAM-Beispielrichtlinie bietet Berechtigungen zum Verwalten aller Aspekte von Backup-Richtlinien in einer Organisation.

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

```
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zu IAM-Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch.

Bewährte Methoden für die Verwendung von Backup-Richtlinien

AWS empfiehlt die folgenden bewährten Methoden für die Verwendung von Backup-Richtlinien:

Entscheidung bezüglich einer Backup-Richtlinienstrategie

Sie können Backup-Richtlinien in unvollständigen Teilen erstellen, die vererbt und zusammengeführt werden, um eine vollständige Richtlinie für jedes Mitgliedskonto zu erstellen. Wenn Sie dies tun, besteht die Gefahr, dass Ihre effektive Richtlinie unvollständig ist, wenn Sie eine Änderung auf einer Ebene vornehmen, ohne sorgfältig die Auswirkungen der Änderung auf alle Konten unterhalb dieser Ebene zu berücksichtigen. Um dies zu verhindern, sollten Sie sicherstellen, dass die Backup-Richtlinien, die Sie auf allen Ebenen implementieren, für sich selbst genommen „vollständig“ sind. Behandeln Sie die übergeordneten Richtlinien als Standardrichtlinien, die durch die in untergeordneten Richtlinien festgelegten Einstellungen überschrieben werden können. Auf diese Weise ist die geerbte Richtlinie auch dann vollständig, wenn keine untergeordnete Richtlinie vorhanden ist, und verwendet die Standardwerte. Mithilfe der Vererbungsoperatoren für untergeordnete Steuerelemente können Sie steuern, welche Einstellungen von untergeordneten Richtlinien hinzugefügt, geändert oder entfernt werden können.

Validieren von Änderungen an Ihren Backup-Richtlinien mithilfe von **`GetEffectivePolicy`**

Nachdem Sie eine Änderung an einer Backup-Richtlinie vorgenommen haben, überprüfen Sie die effektiven Richtlinien für repräsentative Konten unterhalb der Ebene, auf der Sie die Änderung vorgenommen haben. Sie können die effektive Richtlinie über die AWS Management Console oder unter Verwendung der API-Operation GetEffectivePolicy oder einer Ihrer AWS CLI- oder AWS-SDK-Varianten anzeigen. Stellen Sie sicher, dass die vorgenommene Änderung die beabsichtigten Auswirkungen auf die effektive Richtlinie hatte.

Einfach starten und kleine Änderungen vornehmen

Um das Debuggen zu vereinfachen, beginnen Sie mit einfachen Richtlinien und nehmen Sie jeweils Änderungen an einem Element vor. Überprüfen Sie das Verhalten und die Auswirkungen jeder Änderung, bevor Sie die nächste Änderung vornehmen. Dieser Ansatz reduziert die Anzahl der Variablen, die Sie berücksichtigen müssen, wenn ein Fehler oder ein unerwartetes Ergebnis auftritt.

Speichern Sie Kopien Ihrer Backups in anderen AWS-Regionen und Konten in Ihrer Organisation

Um Ihre Notfallwiederherstellung-Position zu verbessern, können Sie Kopien Ihrer Backups speichern.

- Eine andere Region – Wenn Sie Kopien des Backups in zusätzlichen AWS-Regionen speichern, tragen Sie dazu bei, das Backup in der ursprünglichen Region vor versehentlicher Beschädigung oder Löschung zu schützen. Verwenden Sie den Abschnitt `copy_actions` der Richtlinie, um

einen Tresor in einer oder mehreren Regionen desselben Kontos anzugeben, in dem der Backup-Plan ausgeführt wird. Identifizieren Sie dazu das Konto mithilfe der `$account`-Variablen, wenn Sie den ARN des Backup-Tresors angeben, in dem die Kopie des Backups gespeichert werden soll. Die `$account` Variable wird zur Laufzeit automatisch durch die Konto-ID ersetzt, in der die Backup-Richtlinie ausgeführt wird.

- Ein anderes Konto – Wenn Sie Kopien des Backups in zusätzlichen AWS-Konten speichern, fügen Sie eine Sicherheitsbarriere hinzu, die zum Schutz vor einem böswilligen Akteur beiträgt, der eines Ihrer Konten kompromittiert. Verwenden Sie den `copy_actions`-Abschnitt der Richtlinie, um einen Tresor in einem oder mehreren Konten in Ihrer Organisation anzugeben, getrennt von dem Konto, in dem der Backup-Plan ausgeführt wird. Identifizieren Sie dazu das Konto anhand der tatsächlichen Konto-ID-Nummer, wenn Sie den ARN des Backup-Tresors angeben, in dem die Kopie des Backups gespeichert werden soll.

Begrenzen der Anzahl der Pläne pro Richtlinie

Die Fehlerbehebung von Richtlinien, die mehrere Pläne enthalten, ist aufgrund der größeren Anzahl von Ausgaben, die alle geprüft werden müssen, komplizierter. Um das Debuggen und die Fehlerbehebung zu vereinfachen, sollte jede Richtlinie daher nur einen einzigen Backup-Plan enthalten. Sie können dann zusätzliche Richtlinien mit anderen Plänen hinzufügen, um andere Anforderungen zu erfüllen. Durch diesen Ansatz bleiben Probleme mit einem Plan auf eine Richtlinie beschränkt und erschweren nicht die Fehlerbehebung von Problemen mit anderen Richtlinien und deren Plänen.

Verwenden von Stack-Sets, um die erforderlichen Backup-Tresore und IAM-Rollen zu erstellen

Verwenden Sie die AWS CloudFormation-StackSets-Integration mit Organizations, um die erforderlichen Backup-Tresore und AWS Identity and Access Management-(IAM)-Rollen automatisch in allen Mitgliedskonten in Ihrer Organisation zu erstellen. Sie können ein Stack-Set erstellen, das die Ressourcen enthält, die automatisch in jedem AWS-Konto in Ihrer Organisation verfügbar sein sollen. Durch diesen Ansatz haben Sie bei der Ausführung Ihrer Backup-Pläne die Gewissheit, dass die Abhängigkeiten bereits erfüllt sind. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen im AWS CloudFormation-Benutzerhandbuch.

Überprüfen Sie Ihre Ergebnisse durch Prüfung des ersten Backups, die in jedem Konto erstellt wurde.

Wenn Sie eine Änderung an einer Richtlinie vornehmen, überprüfen Sie den nächsten Backup, der nach dieser Änderung erstellt wurde, um sicherzustellen, dass die Änderung die gewünschten Auswirkungen hatte. Dieser Schritt beinhaltet mehr als die Prüfung der effektiven Richtlinie. Es

wird sichergestellt, dass AWS Backup Ihre Richtlinien so interpretiert und die Backuppläne so implementiert, wie Sie dies beabsichtigt haben.

Erstellen, Aktualisieren und Löschen von Backup-Richtlinien

In diesem Thema:

- Nach der Aktivierung von Backup-Richtlinien für Ihre Organisation können Sie eine Richtlinie erstellen.
- Wenn sich Ihre Backup-Anforderungen ändern, können Sie eine vorhandene Richtlinie aktualisieren.
- Wenn Sie eine Richtlinie nicht mehr benötigen, können Sie sie löschen, nachdem Sie sie von allen Organisationseinheiten (Organizational Units OUs) und Konten getrennt haben.

Erstellen einer Backup-Richtlinie

> **Mindestberechtigungen**
>
> Zum Erstellen einer Backup-Richtlinie benötigen Sie die Berechtigung zur Ausführung folgender Aktion:
>
> - `organizations:CreatePolicy`

AWS Management Console

Sie können eine Backup-Richtlinie in der AWS Management Console auf zwei Arten erstellen:

- Mit einem visuellen Editor, bei dem Sie Optionen auswählen können und der JSON-Richtlinientext für Sie generiert wird.
- Mit einem Texteditor, bei dem Sie den JSON-Richtlinientext direkt selbst erstellen können.

Der visuelle Editor macht den Prozess einfach, schränkt aber Ihre Flexibilität ein. Er ist sehr gut geeignet, um Ihre ersten Richtlinien zu erstellen und sich mit deren Verwendung vertraut zu machen. Wenn Sie die Funktionsweise der Richtlinien verstanden haben und allmählich durch die Möglichkeiten des visuellen Editors eingeschränkt sind, können Sie Ihren Richtlinien erweiterte Funktionen hinzufügen, indem Sie den JSON-Richtlinientext selbst bearbeiten. Der

visuelle Editor verwendet nur den @@assign-Werteinstellungsoperator und bietet keinen Zugriff auf die untergeordneten Steuerungsoperatoren. Sie können die Operatoren des untergeordneten Steuerelements nur hinzufügen, wenn Sie den JSON-Richtlinientext manuell bearbeiten.

Erstellen Sie wie folgt eine Backup-Richtlinie:

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Backup policies (Backup-Richtlinien) die Option Create policy (Richtlinie erstellen) aus.
3. Geben Sie auf der Seite Richtlinie erstellen unter Richtlinienname einen Namen und unter Richtlinienbeschreibung eine optionale Beschreibung für die Richtlinie ein.
4. (Optional) Sie können der Richtlinie ein oder mehrere Tags hinzufügen, indem Sie Tag hinzufügen auswählen und dann einen Schlüssel und einen optionalen Wert eingeben. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einer Richtlinie bis zu 50 Tags hinzufügen. Weitere Informationen über das Markieren mit Tags finden Sie unter Markieren von AWS Organizations-Ressourcen.
5. Sie können die Richtlinie mit dem Visual Editor (Visuellen Editor) erstellen, wie in diesem Verfahren beschrieben. Sie können auch Richtlinientext auf der Registerkarte JSON eingeben oder einfügen. Weitere Informationen zur Syntax von Backup-Richtlinien finden Sie unter Syntax und Beispiele für Backup-Richtlinien.

   Wenn Sie Visual Editor (Visueller Editor) verwenden möchten, wählen Sie die für Ihr Szenario geeigneten Backup-Optionen aus. Ein Backup-Plan besteht aus drei Teilen. Weitere Informationen zu diesen Backup-Plan-Elementen finden Sie unter Erstellen eines Backup-Plans und Zuweisen von Ressourcen im AWS Backup-Entwicklerhandbuch.

   a. Details zum Backup-Plan

      - Der Backup plan name (Name des Backup-Plans) darf nur aus alphanumerischen Zeichen, Bindestrichen und Unterstrichen bestehen.
      - Sie müssen mindestens eine Backup plan region (Region für Backup-Plan) aus der Liste auswählen. Der Plan kann Ressourcen nur in den ausgewählten AWS-Regionen sichern.

   b. Eine oder mehrere Backup-Regeln, die angeben, wie und wann AWS Backup ausgeführt werden soll. Jede Backup-Regel definiert die folgenden Elemente:

- Einen Zeitplan, der die Häufigkeit des Backups und das mögliche Zeitfenster für den Backup enthält.
- Den Namen des zu verwendenden Backup-Tresors. Der Backup vault name (Name des Backup-Tresors) darf nur aus alphanumerischen Zeichen, Bindestrichen und Unterstrichen bestehen. Der Backup-Tresor muss vorhanden sein, bevor der Plan erfolgreich ausgeführt werden kann. Erstellen Sie den Tresor über die AWS Backup-Konsole oder mithilfe von AWS CLI-Befehlen.
- (Optional) Eine oder mehrere Regeln „Copy to region (In Region kopieren), um den Backup auch in Tresore in anderen AWS-Regionen zu kopieren.
- Ein oder mehrere Tag-Schlüssel- und Wertepaare, die an die Backup-Wiederherstellungspunkte angefügt werden, die bei jeder Ausführung dieses Backup-Plans erstellt werden.
- Lebenszyklusoptionen, die angeben, wann der Backup zum Cold Storage übergeht und wann die Sicherung abläuft.

Wählen Sie Regel hinzufügen, um dem Plan jede benötigte Regel hinzuzufügen.

Weitere Informationen zu Backup-Regeln finden Sie unter Backup-Regeln im AWS Backup-Entwicklerhandbuch.

c. Eine Ressourcenzuordnung, die die Ressourcen angibt, die AWS Backup mit diesem Plan sichern soll. Die Zuweisung erfolgt durch Angabe von Tag-Paaren, die AWS Backup verwendet, um Ressourcen zu finden und abzugleichen

- Der Ressource assignment name (Name der Ressourcenzuordnung) darf nur aus alphanumerischen Zeichen, Bindestrichen und Unterstrichen bestehen.
- Geben Sie die IAM-Rolle an, die AWS Backup zur Ausführung des Backups anhand ihres Namens verwenden soll.

  In der Konsole geben Sie nicht den gesamten Amazon-Ressourcennamen (ARN) an. Sie müssen sowohl den Rollennamen als auch das Präfix angeben, das den Rollentyp angibt. Die Präfixe sind normalerweise `role` oder `service-role` und werden durch einen Schrägstrich ('/') vom Rollennamen getrennt. So könnten Sie beispielsweise `role/MyRoleName` oder `service-role/MyManagedRoleName` eingeben. Dies wird beim Speichern in der zugrunde liegenden JSON in einen vollständigen ARN konvertiert.

> **Important**
>
> Die angegebene IAM-Rolle muss bereits in dem Konto vorhanden sein, auf das die Richtlinie angewendet wird. Wenn dies nicht der Fall ist, kann der Backup-Plan Backup-Aufgaben zwar möglicherweise erfolgreich starten, diese Backup-Aufträge schlagen jedoch fehl.

- Geben Sie ein oder mehrere Ressourcen-Tag-Schlüssel- und Tag-Wert-Paare an, um Ressourcen zu identifizieren, die Sie sichern möchten. Wenn mehr als ein Tag-Wert vorhanden ist, trennen Sie die Werte durch Kommas.

Wählen Sie Zuweisung hinzufügen, um jede konfigurierte Ressourcenzuweisung zum Backup-Plan hinzuzufügen.

Weitere Informationen finden Sie unter Zuweisen von Ressourcen zu einem Backup-Plan im AWS Backup-Entwicklerhandbuch.

6. Wenn Sie mit dem Erstellen der Richtlinie fertig sind, wählen Sie Richtlinie erstellen aus. Die Richtlinie wird in der Liste der verfügbaren Backup-Richtlinien angezeigt.

AWS CLI & AWS SDKs

Erstellen Sie wie folgt eine Backup-Richtlinie:

Sie können eine der folgenden Optionen verwenden, um eine Backup-Richtlinie zu erstellen:

- AWS CLI: create-policy

  Erstellen Sie einen Backup-Plan als JSON-Text ähnlich dem folgenden und speichern Sie ihn in einer Textdatei. Vollständige Regeln für die Syntax finden Sie unter Syntax und Beispiele für Backup-Richtlinien.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
```

```
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

Dieser Backup-Plan legt fest, dass AWS alle Ressourcen in den betroffenen AWS-Konten sichern soll, die sich in den angegebenen AWS-Regionen befinden und das Tag `dataType` mit dem Wert `PII` aufweisen.

Importieren Sie als Nächstes den Backup-Plan der JSON-Richtliniendatei, um eine neue Backup-Richtlinie in der Organisation zu erstellen. Notieren Sie die Richtlinien-ID am Ende des Richtlinien-ARN in der Ausgabe.

```
$ aws organizations create-policy \
```

```
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWS-SDKs: CreatePolicy

Weitere Vorgehensweisen

Nachdem Sie eine Backup-Richtlinie erstellt haben, können Sie Ihre Richtlinie in Kraft setzen. Dies ist möglich durch Anfügen der Richtlinie an den Organisationsstamm, die Organisationseinheiten (OUs), die AWS-Konten innerhalb Ihrer Organisation oder einer Kombination hiervon.

Aktualisieren einer Backup-Richtlinie

Wenn Sie sich im Verwaltungskonto Ihrer Organisation angemeldet haben, können Sie eine Richtlinie bearbeiten, die in Ihrer Organisation Änderungen erfordert.

Mindestberechtigungen

Um eine Backup-Richtlinie zu aktualisieren, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:

- `organizations:UpdatePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN der zu aktualisierenden Richtlinie enthält (oder "*")
- `organizations:DescribePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN der zu aktualisierenden Richtlinie enthält (oder "*")

AWS Management Console

Aktualisieren Sie wie folgt eine Backup-Richtlinie:

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Backup policies (Backup-Richtlinien) den Namen der Richtlinie aus, die Sie aktualisieren möchten.
3. Wählen Sie Edit policy (Richtlinie bearbeiten).
4. Sie können einen neuen Richtliniennamen, Richtlinienbeschreibung, eingeben. Sie können den Richtlinieninhalt ändern, indem Sie entweder den visuellen Editor verwenden oder die JSON direkt bearbeiten.
5. Wenn Sie mit der Aktualisierung der Richtlinie fertig sind, wählen Sie Save changes (Änderungen speichern) aus.

AWS CLI & AWS SDKs

Aktualisieren Sie wie folgt eine Backup-Richtlinie:

Zum Aktualisieren einer Backup-Richtlinie können Sie einen der folgenden Befehle verwenden:

- AWS CLI: update-policy

  Im folgenden Beispiel wird eine Backup-Richtlinie umbenannt.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

Im folgenden Beispiel wird die Beschreibung einer Backup-Richtlinie hinzugefügt oder geändert.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

Im folgenden Beispiel wird das JSON-Richtliniendokument geändert, das einer Backup-Richtlinie zugeordnet ist. In diesem Beispiel wird der Inhalt einer Datei namens `policy.json` mit folgendem Text entnommen:

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
```

```
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWS-SDKs: UpdatePolicy

Bearbeiten von Tags, die an eine Backup-Richtlinie angehängt sind

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie die einer Backup-Richtlinie angefügten Tags hinzufügen oder entfernen. Weitere Informationen über das Markieren mit Tags finden Sie unter Markieren von AWS Organizations-Ressourcen.

Mindestberechtigungen

Um die an eine Backup-Richtlinie in Ihrer AWS-Organisation angefügten Tags zu bearbeiten, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeOrganization` (Nur Konsole – um zur Richtlinie zu navigieren)
- `organizations:DescribePolicy` (Nur Konsole – um zur Richtlinie zu navigieren)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

So bearbeiten Sie die Tags, die einer Backup-Richtlinie zugeordnet sind

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Backup-Richtlinien-Seite
3. Wählen Sie den Namen der Richtlinie mit den Tags aus, die Sie bearbeiten möchten.

   Die Richtliniendetailseite wird angezeigt.
4. Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).
5. Sie können eine der folgenden Aktionen auf dieser Seite ausführen:

- Bearbeiten Sie den Wert für ein beliebiges Tag, indem Sie einen neuen Wert über dem alten eingeben. Sie können den Schlüssel nicht ändern. Um einen Schlüssel zu ändern, müssen Sie das Tag mit dem alten Schlüssel löschen und ein Tag mit dem neuen Schlüssel hinzufügen.
- Entfernen Sie ein vorhandenes Tag, indem Sie Entfernen wählen.
- Fügen Sie ein neues Tag-Schlüssel-Wert-Paar hinzu. Wählen Sie Tag hinzufügen aus und geben Sie dann den neuen Schlüsselnamen und den optionalen Wert in die bereitgestellten Felder ein. Wenn Sie das Feld Wert leer lassen, ist der Wert eine leere Zeichenfolge; er ist nicht `null`.

6. Wählen Sie Änderungen speichern, nachdem Sie alle gewünschten Ergänzungen, Entfernungen und Änderungen vorgenommen haben.

AWS CLI & AWS SDKs

So bearbeiten Sie die Tags, die einer Backup-Richtlinie zugeordnet sind

Sie können einen der folgenden Befehle verwenden, um die einer Backup-Richtlinie zugeordneten Tags zu bearbeiten:

- AWS CLI: tag-resource und untag-resource
- AWS-SDKs: TagResource und UntagResource

Löschen einer Backup-Richtlinie

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Richtlinie löschen, die Sie in Ihrer Organisation nicht mehr benötigen.

Bevor Sie eine Richtlinie löschen können, müssen Sie sie zuerst von allen angehängten Elementen trennen.

> **Mindestberechtigungen**
>
> Um eine Richtlinie zu löschen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:
>
> - `organizations:DeletePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die zu löschende Richtlinie enthält (oder "*")

AWS Management Console

So löschen Sie eine Backup-Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Backup-Richtlinien den Namen der Backup-Richtlinie aus, die Sie löschen möchten.
3. Sie müssen zuerst die Backup-Richtlinie, die Sie löschen möchten, von allen Stammverzeichnissen, Organisationseinheiten und Konten trennen. Wählen Sie die Registerkarte Ziele aus, wählen Sie das Optionsfeld neben jedem Stamm, jeder OU oder jedem Konto aus, die in der Liste Ziele angezeigt werden und wählen Sie dann Trennen. Wählen Sie im Bestätigungsdialogfeld Trennen aus. Wiederholen Sie dies, bis Sie alle Ziele entfernt haben.
4. Wählen Sie oben auf der Seite Löschen.
5. Geben Sie im Bestätigungsdialogfeld den Namen der Richtlinie ein und wählen Sie dann Löschen aus.

AWS CLI & AWS SDKs

So löschen Sie eine Backup-Richtlinie

Zum Löschen einer Tag-Richtlinie können Sie eine der folgenden Optionen verwenden:

- AWS CLI: delete-policy

  Im folgenden Beispiel wird die angegebene Richtlinie gelöscht. Sie funktioniert nur, wenn die Richtlinie keinem Stamm, keiner Organisationseinheit oder keinem Konto angefügt ist.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: DeletePolicy

Anfügen und Trennen von Backup-Richtlinien

Sie können Backup-Richtlinien sowohl für eine ganze Organisation als auch für Organisationseinheiten (OUs) und einzelne Konten verwenden. Beachten Sie die folgenden Punkte:

- Wenn Sie eine Backup-Richtlinie an den Organisationsstamm anfügen, gilt die Backup-Richtlinie für alle Organisationseinheiten und Konten der Stammmitglieder.
- Wenn Sie eine Backup-Richtlinie an eine Organisationseinheit (OU) anfügen, gilt diese Richtlinie für die Konten, die zu der OU oder einer ihrer untergeordneten Organisationseinheiten gehören. Diese Konten unterliegen auch jeder Richtlinie, die an den Organisationsstamm angefügt ist.
- Wenn Sie eine Backup-Richtlinie an ein Konto, anfügen, gilt diese Richtlinie nur für dieses Konto. Das Konto unterliegt auch jeder Richtlinie, die an den Organisationsstamm und alle Organisationseinheiten angefügt ist, zu denen das Konto gehört.

Die Aggregation aller Backup-Richtlinien, die das Konto vom Stamm und den übergeordneten Organisationseinheiten erbt, sowie aller Richtlinien, die direkt an das Konto angefügt sind, ist die effektive Richtlinie. Weitere Informationen zur Zusammenführung von Richtlinien zu einer effektiven Richtlinie finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

Anfügen einer Backup-Richtlinie

Wenn Sie sich beim Verwaltungskonto Ihrer Organisation angemeldet haben, können Sie eine Backup-Richtlinie an den Organisationsstamm, eine OU oder direkt an ein Konto anfügen.

> **Mindestberechtigungen**
>
> Um Backup-Richtlinien anzufügen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:
>
> - `organizations:AttachPolicy`

AWS Management Console

Sie können eine Backuprichtlinie anfügen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, an das Sie die Richtlinie anfügen möchten, navigieren.

So fügen Sie eine Backup-Richtlinie an, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, dem Sie eine Richtlinie anfügen möchten, und wählen Sie dann den Namen aus. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Eintrag für Backup-Richtlinien die Option Anfügen.
4. Suchen Sie die gewünschte Richtlinie und wählen Sie Richtlinie anfügen aus.

   Die Liste der angehängten Backup-Richtlinien auf der Registerkarte Richtlinien wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

So fügen Sie eine Backup-Richtlinie durch Navigieren zur Richtlinie an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Backuprichtlinien den Namen der Richtlinie aus, die Sie aktualisieren möchten.
3. Klicken Sie in der Registerkarte Ziele auf Anfügen.
4. Aktivieren Sie das Optionsfeld neben dem Stammverzeichnis, der Organisationseinheit oder dem Konto, an das bzw. die Sie die Richtlinie anfügen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
5. Wählen Sie Attach policy (Richtlinie anfügen) aus.

   Die Liste der angehängten Backup-Richtlinien auf der Registerkarte Ziele wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So fügen Sie eine Backup-Richtlinie an den Organisationsstamm, die OU oder das Konto an

Sie können zum Anfügen einer Backup-Richtlinie einen der folgenden Befehle verwenden:

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWS-SDKs: AttachPolicy

Die Richtlinienänderung wird sofort wirksam.

Trennen einer Backup-Richtlinie

Wenn Sie im Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Backup-Richtlinie vom Organisationsstamm, von der OU oder dem Konto, dem/der sie angefügt ist, trennen. Nach dem Trennen der Backup-Richtlinie von einem Element, gilt diese Richtlinie nicht mehr für Konten, auf die sich das jetzt getrennte Element zuvor ausgewirkt hat. Führen Sie zum Trennen einer Richtlinie die folgenden Schritte aus.

Mindestberechtigungen

Um eine Backup-Richtlinie vom Organisationsstamm, der OU oder dem Konto zu trennen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:

- `organizations:DetachPolicy`

AWS Management Console

Sie können eine Backup-Richtlinie trennen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, von denen Sie die Richtlinie trennen möchten, navigieren.

So trennen Sie eine Backup-Richtlinie, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren, an die sie angefügt ist

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, von dem Sie eine Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. Wählen Sie den Namen des Stammes, der Organisationseinheit oder des Kontos aus.
3. Wählen Sie auf der Registerkarte Richtlinien das Optionsfeld neben der Backup-Richtlinie aus, die Sie trennen möchten und wählen Sie dann Trennen aus.
4. Wählen Sie im Bestätigungsdialogfeld Richtlinie trennen aus.

   Die Liste der angehängten Backup-Richtlinien wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

So trennen Sie eine Backup-Richtlinie durch Navigieren zur Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Backup-Richtlinien den Namen der Richtlinie aus, die Sie von einem Stamm, einer OU oder einem Konto trennen möchten.
3. Wählen Sie auf der Registerkarte Ziele das Optionsfeld neben dem Stamm, der OU oder dem Konto aus, von dem Sie die Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
4. Wählen Sie Detach (Trennen) aus.
5. Wählen Sie im Bestätigungsdialogfeld Trennen aus.

   Die Liste der angehängten Backup-Richtlinien wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So trennen Sie eine Backup-Richtlinie vom Organisationsstamm, der OU oder dem Konto

Sie können zum Trennen einer Backup-Richtlinie einen der folgenden Befehle verwenden:

- AWS CLI: detach-policy

  Im folgenden Beispiel wird eine Richtlinie von einer Organisationseinheit entfernt.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-SDKs: DetachPolicy

Die Richtlinienänderung wird sofort wirksam.

Anzeigen effektiver Backup-Richtlinien

Sie können die effektive Backup-Richtlinie für ein Konto über die AWS-Managementkonsole, AWS-API oder die AWS-Befehlszeilenschnittstelle anzeigen. Der folgende Abschnitt enthält eine kurze Übersicht über die effektive Backup-Richtlinie, einschließlich eines Beispiels.

Was ist die effektive Backup-Richtlinie?

Die effektive Backup-Richtlinie gibt die endgültigen Backupplaneinstellungen an, die für ein AWS-Konto gelten. Es handelt sich um die Aggregation aller von dem Konto geerbten Backup-Richtlinien sowie aller Backup-Richtlinien, die direkt an das Konto angefügt sind. Wenn Sie eine Backup-Richtlinie an den Organisationsstamm anfügen, gilt diese für alle Konten in Ihrer Organisation. Wenn Sie eine Backup-Richtlinie an eine Organisationseinheit (OU) anfügen, gilt diese für alle Konten und OUs, die zu der OU gehören. Wenn Sie eine Richtlinie direkt an ein Konto anfügen, gilt diese nur für das betreffende AWS-Konto.

So könnte die an den Organisationsstamm angefügte Backup-Richtlinie beispielsweise angeben, dass alle Konten in der Organisation alle Amazon-DynamoDB-Tabellen mit einer Standard-Backup-Häufigkeit von einmal pro Woche sichern. Eine separate Backup-Richtlinie, die direkt an ein Mitgliedskonto mit wichtigen Informationen in einer Tabelle angefügt ist, kann die Häufigkeit mit

einem Wert von einmal pro Tag überschreiben. Die Kombination dieser Backup-Richtlinien bildet die effektive Backup-Richtlinie. Diese effektive Backup-Richtlinie wird für jedes Konto in der Organisation individuell festgelegt. In diesem Beispiel ist das Ergebnis, dass alle Konten in der Organisation ihre DynamoDB-Tabellen einmal pro Woche sichern, mit Ausnahme eines Kontos, das seine Tabellen täglich sichert.

Weitere Informationen dazu, wie Backup-Richtlinien zu der endgültigen effektiven Backup-Richtlinie kombiniert werden, finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

Anzeigen der effektiven Backup-Richtlinie

Sie können die effektive Backup-Richtlinie für ein Konto über die AWS Management Console, AWS-API oder AWS Command Line Interface anzeigen.

Mindestberechtigungen

Um die effektive Backup-Richtlinie für ein Konto anzuzeigen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

AWS Management Console

So zeigen Sie die effektive Backup-Richtlinie für ein Konto an

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite AWS-Konten den Namen des Kontos aus, für das Sie die effektive Backup-Richtlinie anzeigen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Abschnitt Backup-Richtlinien die Option Effektive Backup-Richtlinie für dieses AWS-Konto anzeigen aus.

Die Konsole zeigt die effektive Richtlinie an, die auf das angegebene Konto angewendet wird.

> **Note**
>
> Sie können eine effektive Richtlinie nicht kopieren und einfügen und sie ohne wesentliche Änderungen als JSON für eine andere Backup-Richtlinie verwenden. Backup-Richtliniendokumente müssen die Vererbungsoperatoren enthalten, die angeben, wie jede Einstellung in die endgültige effektive Richtlinie zusammengeführt wird.

AWS CLI & AWS SDKs

So zeigen Sie die effektive Backup-Richtlinie für ein Konto an

Sie können eine der folgenden Befehle zum Anzeigen der effektiven Backup-Richtlinie verwenden:

- AWS CLI: describe-effective-policy

  Das folgende Beispiel zeigt die Details einer Backup-Richtlinie an.

```
$ aws organizations describe-effective-policy \
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
```

```
}}}}}}}"
    }
}
```

- AWS-SDKs: DescribeEffectivePolicy

Verwenden von AWS CloudTrail-Ereignissen zur Überwachung von Backup-Richtlinien in Ihrem Unternehmen

Mithilfe von AWS CloudTrail-Ereignissen können Sie überwachen, wann Backup-Richtlinien für Konten in Ihrer AWS-Organisation erstellt, aktualisiert oder gelöscht werden oder wann ein ungültiger organisatorischer Backup-Plan vorliegt. Weitere Informationen finden Sie unter Protokollieren von Ereignissen der kontenübergreifenden Verwaltung im AWS Backup-Entwicklerhandbuch.

Syntax und Beispiele für Backup-Richtlinien

Auf dieser Seite wird die Syntax für Backup-Richtlinien beschrieben und durch Beispiele illustriert.

Syntax für Backup-Richtlinien

Eine Backup-Richtlinie ist eine Textdatei, die den JSON-Regeln entsprechend strukturiert ist. Die Syntax für Backup-Richtlinien folgt der Syntax für alle Verwaltungsrichtlinientypen. Eine umfassende Erläuterung dieser Syntax finden Sie unter Richtliniensyntax und Vererbung für Verwaltungsrichtlinientypen. Dieses Thema konzentriert sich auf die Anwendung dieser allgemeinen Syntax auf die spezifischen Anforderungen des Backup-Richtlinientyps.

Der Großteil einer Backup-Richtlinie besteht aus dem Backup-Plan und seinen Regeln. Die Syntax für den Backup-Plan innerhalb einer AWS Organizations Backup-Richtlinie ist strukturell identisch mit der Syntax, die von verwendet wird AWS Backup, aber die Schlüsselnamen unterscheiden sich. In den Beschreibungen der folgenden Richtlinienschlüsselnamen enthält jeder den entsprechenden AWS Backup Planschlüsselnamen. Weitere Informationen zu - AWS Backup Plänen finden Sie unter CreateBackupPlan im AWS Backup -Entwicklerhandbuch.

> **Note**
>
> Bei Verwendung von JSON werden doppelte Schlüsselnamen abgelehnt. Wenn Sie mehrere Pläne, Regeln oder Auswahlen in eine einzelne Richtlinie aufnehmen möchten, stellen Sie sicher, dass der Name jedes Schlüssels eindeutig ist.

Um vollständig und funktionsfähig zu sein, muss eine effektive Backup-Richtlinie mehr als nur einen Backupplan mit seinem Zeitplan und seinen Regeln enthalten. Die Richtlinie muss auch die AWS-Regionen und die zu sichernden Ressourcen sowie die AWS Identity and Access Management (IAM)-Rolle identifizieren, die zur Durchführung des Backups verwenden AWS Backup kann.

Die folgende funktionell vollständige Richtlinie zeigt die grundlegende Syntax von Backup-Richtlinien. Wenn dieses Beispiel direkt an ein -Konto angehängt wurde, AWS Backup sichert alle Ressourcen für dieses Konto in den `eu-north-1` Regionen `us-east-1` und `RED` , die das -Tag `dataType` mit dem Wert `PII` oder haben. Diese Ressourcen werden täglich um 5:00 Uhr in `My_Backup_Vault` gesichert und zudem wird eine Kopie in `My_Secondary_Vault` gespeichert. Beide Tresore befinden sich im gleichen Konto wie die Ressource. Es speichert auch eine Kopie des Backups im `My_Tertiary_Vault` in einem anderen, explizit angegebenen Konto. Die Tresore müssen bereits in jedem der angegebenen AWS-Regionen für jeden vorhanden sein AWS-Konto , der die effektive Richtlinie erhält. Wenn eine der gesicherten Ressourcen EC2-Instances sind, wird die Unterstützung für den Microsoft Volume Shadow Copy Service (VSS) für die Backups auf diesen Instances aktiviert. Der Backup wendet das Tag `Owner:Backup` auf jeden Wiederherstellungspunkt an.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
```

```
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
```

```
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

Zur Syntax der Backup-Richtlinie gehören die folgenden Komponenten:

- `$account`-Variablen – In bestimmten Textzeichenfolgen in den Richtlinien können Sie die `$account`-Variable verwenden, um das aktuelle AWS-Kontodarzustellen. Wenn einen Plan in der effektiven Richtlinie AWS Backup ausführt, ersetzt es diese Variable automatisch durch das aktuelle , AWS-Konto in dem die effektive Richtlinie und ihre Pläne ausgeführt werden.

  > **Important**
  >
  > Sie können die `$account`-Variable nur in Richtlinienelementen verwenden, die einen Amazon-Ressourcennamen (ARN) enthalten können, beispielsweise in Elementen, die den Backup-Tresor, in dem der Backup gespeichert werden soll, oder die IAM-Rolle mit Berechtigungen zum Ausführen der Sicherung angeben.

  Im Folgenden wird beispielsweise vorausgesetzt, dass in jeder , für die die Richtlinie gilt AWS-Konto , ein Tresor mit dem Namen `My_Vault` vorhanden ist.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  Wir empfehlen Ihnen, AWS CloudFormation Stack-Sets und ihre Integration mit Organizations zu verwenden, um automatisch Backup-Tresore und IAM-Rollen für jedes Mitgliedskonto in der Organisation zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen im AWS CloudFormation - Benutzerhandbuch.

- Vererbungsoperatoren – Backup-Richtlinien können sowohl die wertbestimmenden Faktoren für die Vererbung als auch die untergeordneten Steuerungsoperatoren verwenden.
- `plans`

  Der Schlüssel der obersten Ebene der Richtlinie ist der Schlüssel `plans`. Eine Backup-Richtlinie muss immer mit diesem festen Schlüsselnamen oben in der Richtliniendatei beginnen. Unter diesem Schlüssel können Sie einen oder mehrere Backup-Pläne haben.
- Jeder Plan unter dem Schlüssel der obersten Ebene `plans` hat einen Schlüsselnamen, der aus dem vom Benutzer zugewiesenen Namen des Backup-Plans besteht. Im obigen Beispiel lautet der Name des Backup-Plans `PII_Backup_Plan`. In einer Richtlinie kann es mehrere Pläne geben, jeweils mit eigenen `rules`, `regions`, `selections` und `tags`.

  Dieser Schlüsselname des Backup-Plans in einer Backup-Richtlinie entspricht dem Wert des `BackupPlanName` Schlüssels in einem - AWS Backup Plan.

  Jeder Plan kann die folgenden Elemente enthalten:

  - `rules` – Dieser Schlüssel enthält eine Sammlung von Regeln. Jede Regel wird in eine geplante Aufgabe übersetzt, mit einer Startzeit und einem Fenster, in dem die durch die Elemente `regions` und `selections` in der effektiven Backup-Richtlinie angegebenen Ressourcen zu sichern sind.
  - `regions` – Dieser Schlüssel enthält eine Array-Liste von AWS-Regionen , deren Ressourcen durch diese Richtlinie gesichert werden können.
  - `selections` – Dieser Schlüssel enthält eine oder mehrere Sammlungen von Ressourcen (innerhalb der angegebenen `regions`), die durch die angegebenen `rules` gesichert werden.
  - `advanced_backup_settings` – Dieser Schlüssel enthält Einstellungen für Backups, die auf bestimmten Ressourcen ausgeführt werden.
  - `backup_plan_tags` – Gibt Tags an, die dem Backup-Plan selbst angefügt sind.
- `rules`

  Der Richtlinienschlüssel `rules` wird dem Schlüssel `Rules` in einem AWS Backup -Plan zugeordnet. Unter dem Schlüssel `rules` kann es eine oder mehrere Regeln geben. Jede Regel wird zu einer geplanten Aufgabe zur Durchführung eines Backups der ausgewählten Ressourcen.

  Jede Regel enthält einen Schlüssel, dessen Name der Name der Regel ist. Im vorherigen Beispiel lautet der Regelname „My_Hourly_Rule“. Der Wert des Regelschlüssels ist die folgende Sammlung von Regelelementen:

- `schedule_expression` – Dieser Richtlinienschlüssel wird dem `ScheduleExpression` Schlüssel in einem - AWS Backup Plan zugeordnet.

  Gibt die Startzeit des Backups an. Dieser Schlüssel enthält den `@@assign` Vererbungswert-Operator und einen Zeichenfolgewert mit einem CRON-Ausdruck, der angibt, wann einen Backup-Auftrag initiieren AWS Backup soll. Das allgemeine Format der CRON-Zeichenfolge lautet „cron( )“. Dabei ist jeweils eine Zahl oder ein Platzhalter angegeben. Bei Angabe von `cron(0 5 ? * 1,3,5 *)` beispielsweise wird die Sicherung jeden Montag, Mittwoch und Freitag um 5 Uhr morgens gestartet. Bei Angabe von `cron(0 0/1 ? * * *)` wird der Backup stündlich zur vollen Stunde an jedem Wochentag gestartet.

- `target_backup_vault_name` – Dieser Richtlinienschlüssel wird dem `TargetBackupVaultName` Schlüssel in einem - AWS Backup Plan zugeordnet.

  Gibt den Namen des Backup-Tresors an, in dem der Backup gespeichert werden soll. Sie erstellen den Wert mithilfe von AWS Backup. Dieser Schlüssel enthält den `@@assign` - Vererbungswert-Operator und einen Zeichenfolgewert mit einem Tresornamen.

  > **Important**
  >
  > Der Tresor muss bereits vorhanden sein, wenn der Backup-Plan zum ersten Mal gestartet wird. Wir empfehlen Ihnen, AWS CloudFormation Stack-Sets und ihre Integration mit Organizations zu verwenden, um automatisch Backup-Tresore und IAM-Rollen für jedes Mitgliedskonto in der Organisation zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen im AWS CloudFormation -Benutzerhandbuch.

- `start_backup_window_minutes` – Dieser Richtlinienschlüssel wird dem `StartWindowMinutes` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt an, wie viele Minuten gewartet werden soll, bevor eine Aufgabe abgebrochen wird, die nicht erfolgreich gestartet wurde. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Minutenangabe.

- `complete_backup_window_minutes` – Dieser Richtlinienschlüssel wird dem Schlüssel `CompletionWindowMinutes` in einem AWS Backup -Plan zugeordnet.

  (Optional) Gibt an, nach wie vielen Minuten eine Backup-Aufgabe, die erfolgreich gestartet wurde, abgeschlossen werden muss oder von AWS Backupabgebrochen wird. Dieser Schlüssel

enthält den @@assign-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Minutenangabe.

- `enable_continuous_backup` – Dieser Richtlinienschlüssel wird dem `EnableContinuousBackup` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt an, ob kontinuierliche Backups AWS Backup erstellt. `True` bewirkt AWS Backup , dass kontinuierliche Backups erstellt, die point-in-time wiederhergestellt werden können (PITR). `False` (oder nicht angegeben), bewirkt AWS Backup , dass Snapshot-Backups erstellt.

  > **Note**
  >
  > Da PITR-aktivierte Backups maximal 35 Tage aufbewahrt werden können, müssen Sie entweder `False` auswählen oder keinen Wert angeben, wenn Sie eine der folgenden Optionen festlegen:
  >
  > - Legen Sie für `delete_after_days` größer als 35 fest.
  > - Legen Sie `move_to_cold_storage_after_days` auf einen beliebigen Wert fest.

  Weitere Informationen zu kontinuierlichen Backups finden Sie unter P-oint-in-time Wiederherstellung im AWS Backup -Entwicklerhandbuch.

- `lifecycle` – Dieser Richtlinienschlüssel wird dem `Lifecycle` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt an, wann dieses Backup in den Cold Storage AWS Backup überführt und wann es abläuft.

  - `move_to_cold_storage_after_days` – Dieser Richtlinienschlüssel wird dem `MoveToColdStorageAfterDays` Schlüssel in einem - AWS Backup Plan zugeordnet.

    Gibt an, wie viele Tage nach dem Backup AWS Backup den Wiederherstellungspunkt in den Cold Storage verschiebt. Dieser Schlüssel enthält den @@assign-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Angabe der Tage.

  - `delete_after_days` – Dieser Richtlinienschlüssel wird dem `DeleteAfterDays` Schlüssel in einem - AWS Backup Plan zugeordnet.

    Gibt an, wie viele Tage nach dem Backup AWS Backup den Wiederherstellungspunkt löscht. Dieser Schlüssel enthält den @@assign-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Angabe der Tage. Wenn Sie ein Backup in den Cold Storage übertragen, muss

sie dort mindestens 90 Tage bleiben. Dieser Wert muss also mindestens um 90 Tage höher als der Wert für `move_to_cold_storage_after_days` sein.

- `copy_actions` – Dieser Richtlinienschlüssel wird dem `CopyActions` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt an, dass das Backup an einen oder mehrere zusätzliche Speicherorte kopieren AWS Backup soll. Jeder Speicherort der Backup-Kopie wird wie folgt beschrieben:

  - Ein Schlüssel, dessen Name diese Kopieraktion eindeutig kennzeichnet. Zu diesem Zeitpunkt muss der Schlüsselname dem Amazon-Ressourcennamen (ARN) des Backup-Tresors entsprechen. Dieser Schlüssel enthält zwei Einträge.
    - `target_backup_vault_arn` – Dieser Richtlinienschlüssel wird dem Schlüssel `DestinationBackupVaultArn` in einem AWS Backup -Plan zugeordnet.

      (Optional) Gibt den Tresor an, in dem eine zusätzliche Kopie des Backups AWS Backup speichert. Der Wert dieses Schlüssels enthält den Vererbungswert-Operator `@@assign` und den ARN des Tresors.

      - Um auf einen Tresor in der zu verweisen AWS-Konto , in der die Backup-Richtlinie ausgeführt wird, verwenden Sie die `$account` Variable im ARN anstelle der Konto-ID-Nummer. Wenn den Backup-Plan AWS Backup ausführt, ersetzt es die Variable automatisch durch die Konto-ID-Nummer des , AWS-Konto in dem die Richtlinie ausgeführt wird. Dadurch kann das Backup ordnungsgemäß ausgeführt werden, wenn die Backup-Richtlinie für mehr als ein Konto in einer Organisation gilt.
      - Um auf einen Tresor in einem anderen AWS-Konto in derselben Organisation zu verweisen, verwenden Sie die tatsächliche Konto-ID-Nummer im ARN.

      > **Important**
      >
      > - Wenn dieser Schlüssel fehlt, wird eine Version des ARN in Kleinbuchstaben im Namen des übergeordneten Schlüssels verwendet. Da bei ARNs die Groß-/Kleinschreibung beachtet wird, stimmt diese Zeichenfolge möglicherweise nicht mit dem tatsächlichen ARN des Fehlers überein und der Plan schlägt fehl. Aus diesem Grund raten wir davon ab, dass Sie diesen Schlüssel und Wert angeben.
      > - Der Backup-Tresor, in den Sie das Backup kopieren möchten, muss beim ersten Start des Backup-Plans bereits vorhanden sein. Wir empfehlen Ihnen, AWS CloudFormation -Stack-Sets und ihre Integration mit Organizations zu verwenden, um automatisch Backup-Tresore und IAM-Rollen für jedes Mitgliedskonto in der

Organisation zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen im AWS CloudFormation -Benutzerhandbuch.

- `lifecycle` – Dieser Richtlinienschlüssel wird dem `Lifecycle` Schlüssel unter dem `CopyAction` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt an, wann diese Kopie eines Backups in den Cold Storage AWS Backup überführt und wann sie abläuft.

  - `move_to_cold_storage_after_days` – Dieser Richtlinienschlüssel wird dem Schlüssel `MoveToColdStorageAfterDays` in einem AWS Backup -Plan zugeordnet.

    Gibt die Anzahl der Tage nach dem Backup an, bevor den Wiederherstellungspunkt in den Cold Storage AWS Backup verschiebt. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Angabe der Tage.

  - `delete_after_days` – Dieser Richtlinienschlüssel wird dem Schlüssel `DeleteAfterDays` in einem AWS Backup -Plan zugeordnet.

    Gibt die Anzahl der Tage nach dem Backup an, bevor den Wiederherstellungspunkt AWS Backup löscht. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Wert mit einer ganzzahligen Angabe der Tage. Wenn Sie ein Backup in den Cold Storage übertragen, muss sie dort mindestens 90 Tage bleiben. Dieser Wert muss also mindestens um 90 Tage höher als der Wert für `move_to_cold_storage_after_days` sein.

- `recovery_point_tags` – Dieser Richtlinienschlüssel wird dem `RecoveryPointTags` Schlüssel in einem - AWS Backup Plan zugeordnet.

  (Optional) Gibt Tags an, die an jedes Backup AWS Backup angefügt werden, das es aus diesem Plan erstellt. Der Wert dieses Schlüssels enthält eines oder mehrere der folgenden Elemente:

  - Einen Bezeichner für dieses Schlüsselname-Wert-Paar. Dieser Name für jedes Element unter `recovery_point_tags` ist der Tag-Schlüsselname in Kleinbuchstaben, auch wenn `tag_key` eine andere Groß-/Kleinschreibung hat. Bei diesem Bezeichner wird nicht zwischen Groß- und Kleinschreibung unterschieden. Im vorherigen Beispiel wurde dieses Schlüsselpaar durch den Namen `0wner` bezeichnet. Jedes Schlüsselpaar enthält die folgenden Elemente:

    - `tag_key` – Gibt den Tag-Schlüsselnamen an, der dem Backupplan angefügt werden soll. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Zeichenfolgewert. Beim -Wert ist die Groß- und Kleinschreibung zu beachten.

    - `tag_value` – Gibt den Wert an, der dem Backup-Plan angefügt und dem zugeordnet ist `tag_key`. Dieser Schlüssel enthält alle Vererbungswert-Operatoren sowie einen oder mehrere Werte, die in der effektiven Richtlinie ersetzt, angehängt oder entfernt werden sollen. Bei den Werten muss die Groß- und Kleinschreibung beachtet werden.

- `regions`

  Der `regions` Richtlinienschlüssel gibt an AWS-Regionen , AWS Backup in welcher nach Ressourcen sucht, die den Bedingungen im `selections` Schlüssel entsprechen. Dieser Schlüssel enthält einen der Vererbungswertoperatoren und einen oder mehrere Zeichenfolgenwerte für AWS-Region Codes, zum Beispiel: `["us-east-1", "eu-north-1"]`.

- `selections`

  Der Richtlinienschlüssel `selections` gibt die Ressourcen an, die durch die Planregeln in dieser Richtlinie gesichert werden. Dieser Schlüssel entspricht ungefähr dem BackupSelection Objekt in AWS Backup. Die Ressourcen werden durch eine Abfrage nach übereinstimmenden Tag-Schlüsselnamen und -werten angegeben. Der Schlüssel `selections` enthält einen darunterliegenden Schlüssel – `tags`.

  - `tags` – Gibt die Tags an, die die Ressourcen identifizieren, sowie die IAM-Rolle, die berechtigt ist, die Ressourcen abzufragen und zu sichern. Der Wert dieses Schlüssels enthält eines oder mehrere der folgenden Elemente:

    - Ein Bezeichner für dieses Tag-Element. Dieser Bezeichner unter `tags` ist der Tag-Schlüsselname in Kleinbuchstaben, auch wenn das abzufragende Tag eine andere Groß-/Kleinschreibung hat. Bei diesem Bezeichner wird nicht zwischen Groß- und Kleinschreibung unterschieden. Im vorherigen Beispiel wurde ein Element durch den Namen `My_Backup_Assignment` bezeichnet. Jeder Bezeichner unter `tags` enthält die folgenden Elemente:

      - `iam_role_arn` – Gibt die IAM-Rolle an, die über die Berechtigung zum Zugriff auf die Ressourcen verfügt, die durch die Tag-Abfrage in den durch den Schlüssel AWS-Regionen angegebenen `regions`-Regionen identifiziert wurden. Dieser Wert enthält den `@@assign` Vererbungswert-Operator und einen Zeichenfolgenwert, der den ARN der Rolle enthält. AWS Backup verwendet diese Rolle, um die Ressourcen abzufragen und zu ermitteln und das Backup durchzuführen.

        Anstelle der Konto-ID-Nummer können Sie die `$account`-Variable im ARN verwenden. Wenn der Backup-Plan von ausgeführt wird AWS Backup, ersetzt er die Variable

automatisch durch die tatsächliche Konto-ID-Nummer des , AWS-Konto in dem die Richtlinie ausgeführt wird.

> **Important**
>
> Die Rolle muss bereits vorhanden sein, wenn Sie den Backup-Plan zum ersten Mal starten. Wir empfehlen Ihnen, AWS CloudFormation Stack-Sets und ihre Integration mit Organizations zu verwenden, um automatisch Backup-Tresore und IAM-Rollen für jedes Mitgliedskonto in der Organisation zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter Erstellen eines Stack-Sets mit selbstverwalteten Berechtigungen im AWS CloudFormation -Benutzerhandbuch.

- `tag_key` – Gibt den Tag-Schlüsselnamen an, nach dem gesucht werden soll. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Zeichenfolgewert. Beim -Wert ist die Groß- und Kleinschreibung zu beachten.
- `tag_value` – Gibt den Wert an, der einem Schlüsselnamen zugeordnet werden muss, der mit übereinstimmt`tag_key`. AWS Backup schließt die Ressource im Backup nur ein, wenn `tag_key` sowohl als auch `tag_value` übereinstimmen. Dieser Schlüssel enthält alle Vererbungswert-Operatoren sowie einen oder mehrere Werte, die in der effektiven Richtlinie ersetzt, angehängt oder entfernt werden sollen. Bei den Werten muss die Groß- und Kleinschreibung beachtet werden.

- `advanced_backup_settings` – Gibt Einstellungen für bestimmte Backup-Szenarien an. Dieser Schlüssel enthält eine oder mehrere Einstellungen. Jede Einstellung ist eine JSON-Objektzeichenfolge mit den folgenden Elementen:
  - Objektschlüsselname – Eine Zeichenfolge, die den Ressourcentyp angibt, für den die folgenden erweiterten Einstellungen gelten.
  - Objektwert – Eine JSON-Objektzeichenfolge, die eine oder mehrere Backup-Einstellungen enthält, die für den zugehörigen Ressourcentyp spezifisch sind.

  Derzeit ermöglicht die einzige unterstützte erweiterte Backup-Einstellung Backups des Microsoft Volume Shadow Copy Service (VSS) für Windows oder SQL Server, die auf einer Amazon-EC2-Instance ausgeführt werden. Der Schlüsselname muss der Ressourcentyp `"ec2"` sein, und der Wert gibt an, dass `"windows_vss"`-Support entweder `enabled` oder `disabled` für Backups ist, die auf diesen Amazon-EC2-Instances ausgeführt werden. Weitere Informationen zu dieser Feature finden Sie unter Erstellen eines VSS-aktivierten Windows-Backups im AWS Backup -Entwicklerhandbuch.

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
}
```

- `backup_plan_tags` – Gibt Tags an, die dem Backup-Plan selbst angefügt sind. Dies wirkt sich nicht auf die Tags aus, die in Regeln oder in der Auswahl angegeben sind.

  (Optional) Sie können Tags an Ihre Backup-Pläne anfügen. Der Wert dieses Schlüssels ist eine Sammlung von Elementen.

  Der Schlüsselname für jedes Element unter `backup_plan_tags` ist der Tag-Schlüsselname in Kleinbuchstaben, auch wenn das abzufragende Tag eine andere Groß-/Kleinschreibung hat. Bei diesem Bezeichner wird nicht zwischen Groß- und Kleinschreibung unterschieden. Der Wert für jeden dieser Einträge besteht aus den folgenden Schlüsseln:

  - `tag_key` – Gibt den Tag-Schlüsselnamen an, der dem Backupplan angefügt werden soll. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Zeichenfolgewert. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten.
  - `tag_value` – Gibt den Wert an, der dem Backup-Plan angefügt und dem zugeordnet ist `tag_key`. Dieser Schlüssel enthält den `@@assign`-Vererbungswert-Operator und einen Zeichenfolgewert. Bei diesem Wert ist die Groß- und Kleinschreibung zu beachten.

Beispiele für Backup-Richtlinien

Die folgenden Backup-Richtlinienbeispiele dienen nur zu Informationszwecken. In einigen der folgenden Beispiele kann die JSON-Leerzeichenformatierung komprimiert sein, um Platz zu sparen.

Beispiel 1: Richtlinie, die einem übergeordneten Knoten zugewiesen ist

Das folgende Beispiel zeigt eine Backup-Richtlinie, die einem der übergeordneten Knoten eines Kontos zugewiesen ist.

Übergeordnete Richtlinie – Diese Richtlinie kann an den Organisationsstamm oder an eine Organisationseinheit angefügt werden, bei der es sich um eine übergeordnete Organisationseinheit aller betreffenden Konten handelt.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
```

```
                            "delete_after_days": {
                                "@@assign": "120"
                            }
                        }
                    },
                    "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                        "target_backup_vault_arn": {
                            "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                        },
                        "lifecycle": {
                            "move_to_cold_storage_after_days": {
                                "@@assign": "30"
                            },
                            "delete_after_days": {
                                "@@assign": "120"
                            }
                        }
                    }                   }
            }
        },
        "selections": {
            "tags": {
                "datatype": {
                    "iam_role_arn": {
                        "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                    },
                    "tag_key": {
                        "@@assign": "dataType"
                    },
                    "tag_value": {
                        "@@assign": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        },
        "advanced_backup_settings": {
            "ec2": {
                "windows_vss": {
                    "@@assign": "enabled"
```

```
                    }
                }
            }
        }
    }
}
```

Wenn keine anderen Richtlinien geerbt oder an die Konten angefügt werden, AWS-Konto sieht die effektive Richtlinie, die in jedem zutreffenden gerendert wird, wie im folgenden Beispiel aus. Der CRON Ausdruck bewirkt, dass der Backup einmal pro Stunde zur vollen Stunde ausgeführt wird. Die Konto-ID 123456789012 ist die tatsächliche Konto-ID für jedes Konto.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
```

```
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": "enabled"
                }
            }
        }
    }
}
```

Beispiel 2: Eine übergeordnete Richtlinie wird mit einer untergeordneten Richtlinie zusammengeführt

Im folgenden Beispiel werden eine geerbte übergeordnete Richtlinie und eine untergeordnete Richtlinie entweder geerbt oder direkt an eine AWS-Konto Zusammenführung angehängt, um die effektive Richtlinie zu bilden.

Übergeordnete Richtlinie – Diese Richtlinie kann an den Organisationsstamm oder an eine übergeordnete Organisationseinheit angefügt werden.

```
{
    "plans": {
```

```
       "PII_Backup_Plan": {
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

Untergeordnete Richtlinie – Diese Richtlinie kann direkt an das Konto oder an eine Organisationseinheit auf einer Ebene unterhalb der Organisationseinheit, an die die übergeordnete Richtlinie angefügt ist, angefügt werden.

```
{
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Resultierende effektive Richtlinie – Die effektive Richtlinie, die auf die Konten angewendet wird, enthält zwei Pläne mit jeweils eigenen Regeln und Ressourcen, auf die die Regeln angewendet werden sollen.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [ "PII", "RED" ]
                    }
                }
            }
        },
        "Monthly_Backup_Plan": {
            "regions": [ "us-east-1", "eu-central-1" ],
```

```
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "monthlydatatype": {
                            "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                            "tag_key": "BackupType",
                            "tag_value": [ "MONTHLY", "RED" ]
                        }
                    }
                }
            }
        }
}
```

Beispiel 3: Eine übergeordnete Richtlinie verhindert Änderungen durch eine untergeordnete Richtlinie

Im folgenden Beispiel verwendet eine geerbte übergeordnete Richtlinie die untergeordneten Steuerungsoperatoren, um alle Einstellungen zu erzwingen, und verhindert, dass diese durch eine untergeordnete Richtlinie geändert oder überschrieben werden.

Übergeordnete Richtlinie – Diese Richtlinie kann an den Organisationsstamm oder an eine übergeordnete Organisationseinheit angefügt werden. Das Vorhandensein von `"@@operators_allowed_for_child_policies": ["@@none"]` an jedem Knoten der Richtlinie bedeutet, dass eine untergeordnete Richtlinie keine Änderungen an dem Plan vornehmen kann. Auch kann eine untergeordnete Richtlinie der effektiven Richtlinie keine zusätzlichen Pläne hinzufügen. Diese Richtlinie wird zur effektiven Richtlinie für jede Organisationseinheit und jedes Konto unter der Organisationseinheit, an die sie angefügt ist.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
```

```
                        },
                        "to_delete_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
```

```
                        "@@assign": "dataType"
                    },
                    "tag_value": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        },
        "advanced_backup_settings": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "ec2": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "windows_vss": {
                    "@@assign": "enabled",
                    "@@operators_allowed_for_child_policies": ["@@none"]
                }
            }
        }
    }
}
```

Resultierende effektive Richtlinie – Wenn untergeordnete Backup-Richtlinien vorhanden sind, werden sie ignoriert und die übergeordnete Richtlinie wird zur effektiven Richtlinie.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
```

```
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Beispiel 4: Eine übergeordnete Richtlinie verhindert Änderungen an einem einzelnen Backup-Plan durch eine untergeordnete Richtlinie

Im folgenden Beispiel verwendet eine geerbte übergeordnete Richtlinie die untergeordneten Steuerungsoperatoren, um die Einstellungen für einen einzelnen Plan zu erzwingen, und verhindert, dass diese durch eine untergeordnete Richtlinie geändert oder überschrieben werden. Die untergeordnete Richtlinie kann weiterhin zusätzliche Pläne hinzufügen.

Übergeordnete Richtlinie – Diese Richtlinie kann an den Organisationsstamm oder an eine übergeordnete Organisationseinheit angefügt werden. Dieses Beispiel ähnelt dem vorherigen Beispiel, in dem alle untergeordneten Vererbungsoperatoren blockiert wurden, außer auf der

obersten Ebene `plans`. Mit der Einstellung `@@append` auf dieser Ebene können untergeordnete Richtlinien der Sammlung in der effektiven Richtlinie weitere Pläne hinzufügen. Alle Änderungen an dem geerbten Plan werden weiterhin blockiert.

Die Abschnitte in dem Plan sind aus Gründen der Übersichtlichkeit abgeschnitten.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Untergeordnete Richtlinie – Diese Richtlinie kann direkt an das Konto oder an eine Organisationseinheit auf einer Ebene unterhalb der Organisationseinheit, an die die übergeordnete Richtlinie angefügt ist, angefügt werden. Diese untergeordnete Richtlinie definiert einen neuen Plan.

Die Abschnitte in dem Plan sind aus Gründen der Übersichtlichkeit abgeschnitten.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Resultierende effektive Richtlinie – Die effektive Richtlinie umfasst beide Pläne.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
```

```
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Beispiel 5: Eine untergeordnete Richtlinie überschreibt Einstellungen in einer übergeordneten Richtlinie

Im folgenden Beispiel verwendet eine untergeordnete Richtlinie wertbestimmende Operatoren, um einige der Einstellungen, die von einer übergeordneten Richtlinie geerbt wurden, außer Kraft zu setzen.

Übergeordnete Richtlinie – Diese Richtlinie kann an den Organisationsstamm oder an eine übergeordnete Organisationseinheit angefügt werden. Jede der Einstellungen kann von einer untergeordneten Richtlinie außer Kraft gesetzt werden, da das Standardverhalten in Abwesenheit eines untergeordneten Steuerungsoperators, der dies verhindert, darin besteht, `@@assign`, `@@append` oder `@@remove` durch die untergeordnete Richtlinie zuzulassen. Die übergeordnete Richtlinie enthält alle erforderlichen Elemente für einen gültigen Backup-Plan, sodass Ihre Ressourcen erfolgreich gesichert werden, wenn die Richtlinie unverändert geerbt wird.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
```

```
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Untergeordnete Richtlinie – Die untergeordnete Richtlinie enthält nur die Einstellungen, die von der geerbten übergeordneten Richtlinie abweichen müssen. Es muss eine geerbte übergeordnete Richtlinie vorhanden sein, die die anderen erforderlichen Einstellungen bereitstellt, wenn eine Zusammenführung zu einer effektiven Richtlinie erfolgt. Andernfalls enthält die effektive Backup-Richtlinie einen ungültigen Backupplan, der Ihre Ressourcen nicht wie erwartet sichert.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
```

```
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

Resultierende effektive Richtlinie – Die effektive Richtlinie enthält Einstellungen aus beiden Richtlinien, wobei die von der untergeordneten Richtlinie bereitgestellten Einstellungen die von der übergeordneten Richtlinie geerbten Einstellungen außer Kraft setzen. In diesem Beispiel kommt es zu folgenden Änderungen:

- Die Liste der Regionen wird durch eine völlig andere Liste ersetzt. Wenn Sie der geerbten Liste eine Region hinzufügen möchten, verwenden Sie in der untergeordneten Richtlinie `@@append` anstelle von `@@assign`.
- AWS Backup führt jede zweite Stunde statt stündlich aus.
- AWS Backup erlaubt 80 Minuten, bis das Backup gestartet wird, anstatt 60 Minuten.
- AWS Backup verwendet den `Default` Tresor anstelle von `FortKnox`.
- Der Lebenszyklus wird sowohl für die Übertragung in den Cold Storage als auch für die letztendliche Löschung des Backups verlängert.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
```

```
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Tag-Richtlinien

Sie können mit Tag-Richtlinien eine konsistente Tag-Verwaltung sicherstellen, auch in Bezug auf die bevorzugte Fallbehandlung von Tag-Schlüsseln und Tag-Werten.

Was sind Tags?

Tags sind benutzerdefinierte Attributbezeichnungen, die Sie oder AWS einer AWS-Ressource zuweisen. Jedes Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- einem optionalen Feld, dem sogenannten Tag-Wert (z. B. `111122223333` oder `Production`). Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge. Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Auf dem Rest dieser Seite werden Tag-Richtlinien beschrieben. Weitere Informationen zu Tags finden Sie in den folgenden Quellen:

- Allgemeine Informationen zum Markieren, einschließlich Namens- und Nutzungskonventionen, finden Sie im Benutzerhandbuch zum Markieren von -AWSRessourcen.
- Eine Liste der Services, die die Verwendung von Tags unterstützen, finden Sie in der Resource Groups Tagging API-Referenz.
- Informationen zur Verwendung von Tags zur Kategorisierung von Ressourcen finden Sie im Whitepaper Bewährte Methoden für das Markieren von AWS Ressourcen.
- Weitere Informationen zum Taggen von Organizations Ressourcen finden Sie unter Markieren von AWS Organizations-Ressourcen.
- Informationen zum Markieren von Ressourcen in anderen AWS Services finden Sie in der Dokumentation für diesen Service.

Was sind Tag-Richtlinien?

Tag-Richtlinien sind eine Richtlinienart, mit der Sie Tags für alle Ressourcen in den Konten Ihrer Organisation standardisieren können. In einer Tag-Richtlinie geben Sie Tagging-Regeln für mit Tags versehene Ressourcen an.

In einer Tag-Richtlinie kann beispielsweise angeben werden, dass eine Ressource, an die das Tag `CostCenter` angehängt ist, die in der Tag-Richtlinie definierte Fallbehandlung und die dort definierten Tag-Werte verwenden muss. Ferner kann in einer Tag-Richtlinie angegeben werden, dass für bestimmte Ressourcentypen nicht regelkonforme Tagging-Vorgänge erzwungen werden. Mit anderen Worten: Es wird verhindert, dass für bestimmte Ressourcentypen nicht regelkonforme

Tagging-Anforderungen durchgeführt werden. Mit Tags versehene Ressourcen oder Tags, die nicht in der Tag-Richtlinie definiert wurden, werden nicht auf Übereinstimmung mit der Tag-Richtlinie ausgewertet.

Die Verwendung von Tag-Richtlinien beinhaltet die Arbeit mit mehreren AWS-Services:

- Verwenden Sie AWS Organizations zum Verwalten von Tag-Richtlinien. Wenn Sie sich beim Verwaltungskonto der Organisation angemeldet haben, aktivieren Sie die Tag-Richtlinienfunktion mithilfe von Organizations. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Stammbenutzer anmelden (nicht empfohlen). Anschließend können Sie Tag-Richtlinien erstellen und sie an die Entitäten der Organisation anfügen, damit die Tagging-Regeln wirksam werden.
- Verwenden Sie AWS Resource Groups, um die Einhaltung der Tag-Richtlinien zu verwalten. Wenn Sie sich bei einem Konto in Ihrer Organisation angemeldet haben, können Sie mit Resource Groups nicht regelkonforme Tags in Ressourcen im Konto suchen. Sie können die nicht regelkonformen Tags in dem AWS-Service korrigieren, in dem Sie die Ressource erstellt haben.

  Wenn Sie sich beim Verwaltungskonto Ihrer Organisation anmelden, können Sie die Informationen zur Regelkonformität aller Konten Ihrer Organisation anzeigen.

Tag-Richtlinien stehen nur in Organisationen zur Verfügung, in der alle Funktionen aktiviert sind. Weitere Informationen zur Verwendung von Tag-Richtlinien finden Sie unter Voraussetzungen und Berechtigungen zum Verwalten von Tag-Richtlinien.

> **Important**
>
> Wenn Sie noch nicht mit der Verwendung von Tag-Richtlinien vertraut sind, empfiehlt AWS, die unter Erste Schritte mit Tag-Richtlinien beschriebenen Beispielworkflows zu befolgen; erst danach sollten Sie sich mit fortgeschritteneren Tag-Richtlinien beschäftigen. Sie sollten sich zunächst damit vertraut machen, welche Auswirkungen das Anfügen einer einfachen Tag-Richtlinie an ein einzelnes Konto hat, bevor Sie Tag-Richtlinien auf eine gesamte Organisationseinheit oder Organisation anwenden. Es ist sehr wichtig, dass Sie die Auswirkungen einer Tag-Richtlinie verstehen, bevor Sie ihre Umsetzung erzwingen. In den Tabellen auf der Erste Schritte mit Tag-Richtlinien-Seite finden Sie Links zu Anweisungen für fortgeschrittenere richtlinienbezogene Aufgaben.

Voraussetzungen und Berechtigungen zum Verwalten von Tag-Richtlinien

Auf dieser Seite werden die Voraussetzungen und erforderlichen Berechtigungen zur Verwaltung von Tag-Richtlinien in beschrieben AWS Organizations.

Themen

- Voraussetzungen zur Verwaltung von Tag-Richtlinien
- Berechtigungen zur Verwaltung von Tag-Richtlinien

Voraussetzungen zur Verwaltung von Tag-Richtlinien

Die Verwendung von Tag-Richtlinien erfordert Folgendes:

- Für Ihre Organisation müssen alle Funktionen aktiviert sein.
- Sie müssen im Verwaltungskonto Ihrer Organisation angemeldet sein.
- Sie benötigen die in aufgeführten Berechtigungen Berechtigungen zur Verwaltung von Tag-Richtlinien.

Um die Compliance mit Tag-Richtlinien zu evaluieren, verwenden Sie AWS Resource Groups. Informationen zu den Anforderungen zur Evaluierung der Compliance finden Sie unter Voraussetzungen und Berechtigungen im AWS Resource Groups Benutzerhandbuch.

Berechtigungen zur Verwaltung von Tag-Richtlinien

Die folgende IAM-Beispielrichtlinie enthält Berechtigungen zur Verwaltung von Tag-Richtlinien.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
```

```
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zu IAM-Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch.

Bewährte Methoden zur Verwendung von Tag-Richtlinien

AWS empfiehlt die folgenden bewährten Methoden zur Verwendung von Tag-Richtlinien:

Entscheiden Sie sich für eine Strategie bei der Tag-Großschreibung

Legen Sie die gewünschte Großschreibung von Tags und implementieren Sie diese Strategie über alle Ressourcentypen hinweg. Entscheiden Sie sich beispielsweise für `Costcenter`, `costcenter` oder `CostCenter` und verwenden Sie diese Konvention für alle Tags. Um konsistente Ergebnisse in Compliance-Berichten zu erhalten, sollten Sie die Verwendung ähnlicher Tags mit inkonsistenter Fallbehandlung vermeiden. Diese Strategie hilft Ihnen bei der Definition von Tag-Richtlinien für Ihre Organisation.

Verwenden des empfohlenen Workflows

Fangen Sie klein an, indem Sie eine einfache Tag-Richtlinie erstellen. Fügen Sie diese dann einem Mitgliedskonto hinzu, das Sie für Testzwecke verwenden können. Verwenden Sie die unter beschriebenen Workflows Erste Schritte mit Tag-Richtlinien.

Bestimmen von Tagging-Regeln

Dies hängt von den Anforderungen Ihrer Organisation ab. Sie möchten beispielsweise festlegen, dass ein ein `CostCenter`-Tag, der AWS Secrets Manager-Geheimnissen zugeordnet ist, die angegebene Fallbehandlung verwenden muss. Erstellen Sie Tag-Richtlinien, die konforme Tags definieren, und fügen Sie diese Organisations-Entitäten hinzu, in denen diese Tagging-Regeln wirksam werden sollen.

Schulung von Kontoadministratoren

Wenn Sie bereit sind, die Verwendung von Tag-Richtlinien auszuweiten, informieren Sie Kontoadministratoren wie folgt:

- Kommunizieren Sie Ihre Tagging-Strategie.
- Betonen Sie, dass Administratoren Tags für bestimmte Ressourcentypen verwenden müssen.

  Dies ist wichtig, da nicht getaggte Ressourcen in den Compliance-Ergebnissen nicht als „nicht konform“ angezeigt werden.
- Geben Sie Hilfestellung bei der Überprüfung von Compliance mit Tag-Richtlinien. Weisen Sie Administratoren an, nicht konforme Tags für Ressourcen in ihrem Konto zu finden und zu korrigieren, indem Sie das Verfahren in Evaluieren der Compliance für ein Konto im AWS Resource Groups Benutzerhandbuch verwenden. Teilen Sie ihnen mit, wie oft Sie möchten, dass sie auf Compliance überprüfen.

Gehen Sie bei der Durchsetzung der Compliance mit Bedacht vor.

Das Erzwingen von Compliance könnte verhindern, dass Benutzer in den Konten Ihrer Organisation die benötigten Ressourcen kennzeichnen. Lesen Sie die Informationen in Grundlegendes zur Durchsetzung. Beachten Sie auch die in beschriebenen Workflows Erste Schritte mit Tag-Richtlinien.

Erwägen Sie, einen SCP zu erstellen, um Guardrails um Ressourcenerstellungsanforderungen zu setzen

Ressourcen, denen noch nie Tags zugewiesen wurden, werden in Berichten nicht als nicht konform angezeigt. Kontoadministratoren können weiterhin nicht getaggte Ressourcen erstellen. In einigen Fällen können Sie eine Service-Kontrollrichtlinie (Service Control Policy, SCP) verwenden, um Anforderungen bei der Ressourcenerstellung einzugrenzen. Ein Beispiel für SCP finden Sie unter Benötigen Sie ein Tag für angegebene erstellte Ressourcen. Informationen darüber, ob ein AWS-Service die Steuerung des Zugriffs mithilfe von Tags unterstützt, finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch. Suchen Sie nach den Services mit Ja in der Spalte Autorisierung basierend auf Tags. Wählen Sie den Namen des Service, um die Dokumentation zur Autorisierung und Zugriffssteuerung für diesen Service anzuzeigen.

Erste Schritte mit Tag-Richtlinien

Die Verwendung von Tag-Richtlinien beinhaltet die Arbeit mit mehreren AWS-Services. Lesen Sie die folgenden Seiten, um zu beginnen. Folgen Sie anschließend den Workflows auf dieser Seite, um sich mit Tag-Richtlinien und deren Auswirkungen vertraut zu machen.

- Voraussetzungen und Berechtigungen zum Verwalten von Tag-Richtlinien
- Bewährte Methoden zur Verwendung von Tag-Richtlinien

Erstmalige Verwendung von Tag-Richtlinien

Führen Sie diese Schritte aus, um zum ersten Mal Tag-Richtlinien zu verwenden.

Aufgabe	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Schritt 1: Aktivieren Sie Tag-Richtlinien für Ihre Organisation.	Das Management-Konto der Organisation.[1]	AWS Organizations
Schritt 2: Erstellen Sie eine Tag-Richtlinie. Halten Sie Ihre erste Tag-Richtlinie einfach. Geben	Das Management-Konto der Organisation.[1]	AWS Organizations

Aufgabe	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Sie einen Tag-Schlüssel in der Fallbehandlung ein, die Sie verwenden möchten, und lassen Sie alle anderen Optionen in ihren Standardeinstellungen.		
Schritt 3: Fügen Sie einer Tag-Richtlinie ein einzelnes Mitgliedskonto hinzu, das Sie zum Testen verwenden können. Sie müssen sich im nächsten Schritt bei diesem Konto anmelden.	Das Management-Konto der Organisation.[1]	AWS Organizations
Schritt 4: Erstellen Sie einige Ressourcen mit konformen Tags und einige mit nicht konformen Tags.	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Jeder AWS Service, mit dem Sie sich wohl fühlen. Sie können beispielsweise AWS Secrets Manager verwenden und das Verfahren unter Erstellung eines Basisgeheimnisses befolgen, um Geheimnisse mit konformen und nicht konformen Geheimnissen zu erstellen.

Aufgabe	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Schritt 5: Lesen Sie die effektive Tag-Richtlinie und evaluieren Sie den Compliance-Status des Kontos.	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Resource Groups und der AWS-Service, in dem die Ressource erstellt wurde. Wenn Sie Ressourcen mit konformen und nicht konformen Tags erstellt haben, sollten die nicht kompatiblen Tags in den Ergebnissen angezeigt werden.
Schritt 6: Wiederholen Sie das Verfahren zum Suchen und Beheben von Compliance-Problemen, bis die Ressourcen im Testkonto mit Ihrer Tag-Richtlinie übereinstimmen.	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Resource Groups und der AWS-Service, in dem die Ressource erstellt wurde.
Sie können jederzeit die unternehmensweite Compliance evaluieren.	Das Management-Konto der Organisation.[1]	Ressourcengruppen

[1] Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

Erweiterte Verwendung von Tag-Richtlinien

Folgende Aufgaben können Sie in beliebiger Reihenfolge ausführen, um die Verwendung von Tag-Richtlinien zu erweitern.

Erweiterte Aufgabe	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Erstellen Sie fortgeschrittene Tag-Richtlinien. Befolgen Sie dasselbe Verfahren wie bei Erstbenutzern, probieren Sie jedoch andere Aufgaben aus. Definieren Sie beispielsweise zusätzliche Schlüssel oder Werte, oder geben Sie eine andere Fallbehandlung für einen Tag-Schlüssel an. Sie können die Informationen in Vererbung von Verwaltungsrichtlinien verstehen und Syntax für Tag-Richtlinien zum Erstellen detaillierterer Tag-Richtlinien verwenden.	Das Management-Konto der Organisation.[1]	AWS Organizations
Fügen Sie zusätzlichen Konten oder OUs Tag-Richtlinien hinzu. Überprüfen Sie die effektive Tag-Richtlinie für ein Konto, nachdem Sie dem Konto oder einer OU, in der das Konto Mitglied ist, weitere Richtlinien hinzugefügt haben.	Das Management-Konto der Organisation.[1]	AWS Organizations
Erstellen Sie eine SCP zum Fordern von Tags, wenn jemand neue Ressourcen erstellt. Ein Beispiel finden	Das Management-Konto der Organisation.[1]	AWS Organizations

Erweiterte Aufgabe	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Sie unter Benötigen Sie ein Tag für angegebene erstellte Ressourcen.		
Fahren Sie fort, den Compliance-Status des Kontos anhand der effektiven Tag-Richtlinie zu evaluieren, sobald es sich ändert. Korrigieren Sie nicht konforme Tags.	Ein Mitgliedskonto mit einer effektiven Tag-Richtlinie.	Resource Groups und der AWS-Service, in dem die Ressource erstellt wurde.
Evaluieren Sie die unternehmensweite Compliance.	Das Management-Konto der Organisation.[1]	Ressourcengruppen

[1] Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

Erstmalige Durchsetzung von Tag-Richtlinien

Wenn Sie Tag-Richtlinien zum ersten Mal durchsetzen, befolgen Sie einen Workflow, der der ersten Verwendung von Tag-Richtlinien ähnelt, und verwenden Sie ein Testkonto.

> **Warning**
>
> Gehen Sie bei der Durchsetzung der Compliance mit Bedacht vor. Stellen Sie sicher, dass Ihnen die Auswirkungen der Verwendung von Tag-Richtlinien geläufig sind und Sie den empfohlenen Workflow befolgen. Probieren Sie die Durchsetzung auf einem Testkonto aus, bevor Sie sie auf weitere Konten ausweiten. Andernfalls verhindern Sie, dass Benutzer in den Konten Ihrer Organisation die benötigten Ressourcen kennzeichnen. Weitere Informationen finden Sie unter Grundlegendes zur Durchsetzung.

Aufgaben zur Durchsetzung	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
Schritt 1: Erstellen Sie eine Tag-Richtlinie. Halten Sie Ihre erste durchgesetzte Tag-Richtlinie einfach. Geben Sie einen Tag-Schlüssel in der Fallbehandlung ein, die Sie verwenden möchten, und wählen Sie die Option Prevent noncompliant operations for this tag (Nicht konforme Vorgänge für dieses Tag verhindern). Geben Sie anschließend einen Ressourcentyp an, um es durchzusetzen. Wenn Sie mit unserem früheren Beispiel fortfahren, können Sie es auf Secrets-Manager-Geheimnisse durchsetzen.	Das Management-Konto der Organisation.[1]	AWS Organizations
Schritt 2: Fügen Sie einem einzelnen Testkonto eine Tag-Richtlinie hinzu.	Das Management-Konto der Organisation.[1]	AWS Organizations
Schritt 3: Versuchen Sie, einige Ressourcen mit konformen Tags und einige mit nicht konformen Tags zu erstellen. Sie sollten nicht berechtigt sein, ein Tag als Ressource des in der Tag-Richtlinie angegebenen Typs	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Jeder AWS Service, mit dem Sie sich wohl fühlen. Sie können beispielsweise AWS Secrets Manager verwenden und das Verfahren unter Erstellung eines Basisgeheimnisses befolgen, um Geheimnisse mit konformen

Aufgaben zur Durchsetzung	Konto, bei dem Sie sich anmelden möchten	Zu verwendende AWS-Servicekonsole
mit einem nicht konformen Tag zu erstellen.		und nicht konformen Geheimnissen zu erstellen.
Schritt 4: Evaluieren Sie den Compliance-Status des Kontos anhand der effektiven Tag-Richtlinie, und korrigieren Sie nicht konforme Tags.	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Resource Groups und der AWS-Service, in dem die Ressource erstellt wurde.
Schritt 5: Wiederholen Sie das Verfahren zum Suchen und Beheben von Compliance-Problemen, bis die Ressourcen im Testkonto mit Ihrer Tag-Richtlinie übereinstimmen.	Das Mitgliedskonto, das Sie zu Testzwecken verwenden.	Resource Groups und der AWS-Service, in dem die Ressource erstellt wurde.
Sie können jederzeit die unternehmensweite Compliance evaluieren.	Das Management-Konto der Organisation.[1]	Ressourcengruppen

[1] Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

Erstellen, Aktualisieren und Löschen von Tag-Richtlinien

In diesem Thema:

- Nach der Aktivierung von Tag-Richtlinien für Ihre Organisation, können Sie eine Tag-Richtlinie erstellen.
- Wenn sich Ihre Tagging-Anforderungen ändern, können Sie eine vorhandene Richtlinie aktualisieren.
- Wenn Sie eine Richtlinie nicht mehr benötigen, können Sie sie löschen., nachdem Sie sie von allen Organisationseinheiten (Organizational Units OUs) und Konten getrennt haben.

> **Important**
>
> Ressourcen ohne Tags werden in den Ergebnisses nicht als nichtkonform angezeigt.

Erstellen einer Tag-Richtlinie

> **Mindestberechtigungen**
>
> Zum Erstellen von Tag-Richtlinien benötigen Sie die Berechtigung zur Ausführung folgender Aktion:
>
> - `organizations:CreatePolicy`

Sie können eine Tag-Richtlinie in der AWS Management Console auf zwei Arten erstellen:

- Mit einem visuellen Editor, bei dem Sie Optionen auswählen können und der JSON-Richtlinientext für Sie generiert wird.
- Mit einem Texteditor, bei dem Sie den JSON-Richtlinientext direkt selbst erstellen können.

Der visuelle Editor macht den Prozess einfach, schränkt aber Ihre Flexibilität ein. Er ist sehr gut geeignet, um Ihre ersten Richtlinien zu erstellen und sich mit deren Verwendung vertraut zu machen. Wenn Sie die Funktionsweise der Richtlinien verstanden haben und allmählich durch die Möglichkeiten des visuellen Editors eingeschränkt sind, können Sie Ihren Richtlinien erweiterte Funktionen hinzufügen, indem Sie den JSON-Richtlinientext selbst bearbeiten. Der visuelle Editor verwendet nur den @@assign-Werteinstellungsoperator und bietet keinen Zugriff auf die untergeordneten Steuerungsoperatoren. Sie können die Operatoren des untergeordneten Steuerelements nur hinzufügen, wenn Sie den JSON-Richtlinientext manuell bearbeiten.

AWS Management Console

So erstellen Sie eine Tag-Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Wählen Sie auf der Seite Tag policies (Tag-Richtlinien) die Option Create policy (Richtlinie erstellen).
3. Geben Sie auf der Seite Richtlinie erstellen unter Richtliniename einen Namen und unter Richtlinienbeschreibung eine optionale Beschreibung für die Richtlinie ein.
4. (Optional) Sie können dem Richtlinienobjekt selbst ein oder mehrere Tags hinzufügen. Diese Tags sind nicht Teil der Richtlinie. Wählen Sie dazu Tag hinzufügen und geben Sie dann einen Schlüssel und einen optionalen Wert ein. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einer Richtlinie bis zu 50 Tags hinzufügen. Weitere Informationen finden Sie unter Markieren von AWS Organizations-Ressourcen.
5. Sie können die Tag-Richtlinie mithilfe des Visual Editors (Visuellen Editors) erstellen, wie in diesem Verfahren beschrieben. Sie können eine Tag-Richtlinie auch auf der Registerkarte JSON eingeben oder einfügen. Hinweise zur Syntax der Tag-Richtlinie finden Sie unter Syntax für Tag-Richtlinien.

   Geben Sie für New Tag Key 1 (Neuer Tag-Schlüssel 1) den Namen eines hinzuzufügenden Tag-Schlüssels an.
6. Lassen Sie zur Tag key capitalization compliance (Groß-/Kleinschreibungs-Compliance des Tag-Schlüssels) diese Option deaktiviert (Standardeinstellung), um anzugeben, dass die vererbte übergeordnete Tag-Richtlinie, falls vorhanden, die Groß-/Kleinschreibung für den Tag-Schlüssel definieren soll.

   Aktivieren Sie diese Option, wenn Sie eine bestimmte Groß-/Kleinschreibungsoption für den Tag-Schlüssel mit dieser Richtlinie vorschreiben möchten. Wenn Sie diese Option auswählen, überschreibt die Groß-/Kleinschreibung, die Sie für den Tag Key (Tag-Schlüssel) angegeben haben, die in einer übergeordneten, vererbten Richtlinie angegebene Fallbehandlung.

   Wenn keine übergeordnete Richtlinie vorhanden ist und Sie diese Option nicht aktivieren, werden nur Tag-Schlüssel in Kleinbuchstaben als konform angesehen. Weitere Informationen zur Vererbung von übergeordneten Richtlinien finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

   > **Tip**
   >
   > Verwenden Sie die Beispiel-Tag-Richtlinie, die in Beispiel 1: Festlegen eines organisationsweiten Tag-Schlüssels gezeigt wird, als Leitfaden zum Erstellen einer Tag-Richtlinie, die Tag-Schlüssel und deren Fallbehandlung definiert. Fügen Sie sie

zum Organisations-Root hinzu. Später können Sie zusätzliche Tag-Richtlinien, OUs oder Konten erstellen und hinzufügen, um zusätzliche Tagging-Regeln zu erstellen.

7. Aktivieren Sie diese Option für Tag-Wert-Compliance, wenn Sie zulässige Werte für diesen Tag-Schlüssel allen Werten hinzufügen möchten, die von einer übergeordneten Richtlinie geerbt wurden.

   Standardmäßig ist diese Option deaktiviert, was bedeutet, dass nur die Werte, die in einer übergeordneten Richtlinie definiert und von dieser übernommen wurden, als konform betrachtet werden. Wenn keine übergeordnete Richtlinie vorhanden ist und Sie keine Tag-Werte angeben, gilt jeder Wert (einschließlich überhaupt kein Wert) als konform.

   Um die Liste der zulässigen Tag-Werte zu aktualisieren, wählen Sie Specify allowed values for this tag key (Zulässige Werte für diesen Tag-Schlüssel angeben) und dann wählen Sie Specify values (Werte angeben) aus. Wenn Sie dazu aufgefordert werden, geben Sie die neuen Werte (ein Wert pro Box) ein und wählen Sie dann Save changes (Änderungen speichern).

8. Wir empfehlen, dass Sie diese Option für Prevent noncompliant operations for this tag (Nicht konforme Vorgänge für dieses Tag verhindern) deaktivieren (Standardeinstellung), es sei denn, Sie haben Erfahrung mit der Verwendung von Tag-Richtlinien. Stellen Sie sicher, dass Sie die Empfehlungen in Grundlegendes zur Durchsetzung gelesen haben und testen Sie sie gründlich. Andernfalls verhindern Sie, dass Benutzer in den Konten Ihrer Organisation die benötigten Ressourcen kennzeichnen.

   Wenn Sie die Compliance mit diesem Tag-Schlüssel durchsetzen möchten, aktivieren Sie das Kontrollkästchen und anschließend Ressourcentypen angeben. Wählen Sie bei entsprechender Aufforderung die Ressourcentypen aus, die in die Richtlinie aufgenommen werden sollen. Wählen Sie dann Save changes (Änderungen speichern).

   > **Important**
   >
   > Wenn Sie diese Option auswählen, werden alle Vorgänge, die Tags für Ressourcen der angegebenen Typen bearbeiten, nur erfolgreich ausgeführt, wenn der Vorgang zu Tags führt, die mit der Richtlinie konform sind.

9. (Optional) Um dieser Tag-Richtlinie einen weiteren Tag-Schlüssel hinzuzufügen, wählen Sie Add tag key (Tag-Schlüssel hinzufügen). Führen Sie dann die Schritte 6-9 aus, um den Tag-Schlüssel zu definieren.

10. Wenn Sie mit dem Erstellen der Tag-Richtlinie fertig sind, wählen Sie Save changes (Änderungen speichern).

AWS CLI & AWS SDKs

So erstellen Sie eine Tag-Richtlinie

Sie können eine der folgenden Optionen verwenden, um eine Tag-Richtlinie zu erstellen:

- AWS CLI: create-policy

  Zum Erstellen der Tag-Richtlinie können Sie jeden beliebigen Texteditor verwenden. Verwenden Sie die JSON-Syntax, und speichern Sie die Tag-Richtlinie als Datei mit einem beliebigen Namen und einer beliebigen Erweiterung an einem Speicherort Ihrer Wahl. Tag-Richtlinien können maximal 2.500 Zeichen umfassen, einschließlich Leerzeichen. Hinweise zur Syntax der Tag-Richtlinie finden Sie unter Syntax für Tag-Richtlinien.

  So erstellen Sie eine Tag-Richtlinie

  1. Erstellen Sie eine Tag-Richtlinie in einer Textdatei, die der folgenden ähnelt:

     Inhalt von `testpolicy.json`:

     ```
     {
         "tags": {
             "CostCenter": {
                 "tag_key": {
                     "@@assign": "CostCenter"
                 }
             }
         }
     }
     ```

     Diese Tag-Richtlinie definiert den `CostCenter`-Tag-Schlüssel. Das Tag akzeptiert einen beliebigen Wert oder keinen Wert. Eine Richtlinie wie diese bedeutet, dass eine Ressource, bei der das CostCenter-Tag mit oder ohne einen Wert verknüpft ist, konform ist.

  2. Erstellen Sie eine Richtlinie, die den Richtlinieninhalt aus der Datei enthält. Das zusätzliche Leerzeichen in der Ausgabe wurde zur Lesbarkeit gekürzt.

     ```
     $ aws organizations create-policy \
     ```

```
    --name "MyTestTagPolicy" \
    --description "My Test policy" \
    --content file://testpolicy.json \
    --type TAG_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-a1b2c3d4e5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-a1b2c3d4e5",
            "Name": "MyTestTagPolicy",
            "Description": "My Test policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
\":\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

- AWS-SDKs: CreatePolicy

Weitere Vorgehensweisen

Nach der Erstellung einer Tag-Richtlinie können Sie Ihre Tagging-Regeln in Kraft setzen. Dazu fügen Sie die Richtlinie dem Organisationsstamm, den Organisationseinheiten (OUs), den AWS-Konten innerhalb Ihrer Organisation oder einer Kombination von Organisationsentitäten hinzu.

Aktualisieren einer Tag-Richtlinie

> **Mindestberechtigungen**
>
> Um eine Tag-Richtlinie zu aktualisieren, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:
>
> - `organizations:UpdatePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")
> - `organizations:DescribePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")

AWS Management Console

So aktualisieren Sie eine Tag-Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Tag policies page (Tag-Richtlinien) die Tag-Richtlinie aus, die Sie aktualisieren möchten.
3. Wählen Sie Edit policy (Richtlinie bearbeiten).
4. Sie können einen neuen Richtliniennamen, Richtlinienbeschreibung, eingeben. Sie können den Richtlinieninhalt ändern, indem Sie entweder den visuellen Editor verwenden oder die JSON bearbeiten.
5. Wenn Sie mit der Aktualisierung der Tag-Richtlinie fertig sind, wählen Sie Save changes (Änderungen speichern).

AWS CLI & AWS SDKs

So aktualisieren Sie eine Richtlinie

Zum Aktualisieren einer Richtlinie können Sie einen der folgenden Befehle verwenden:

- AWS CLI: update-policy

  Im folgenden Beispiel wird eine Tag-Richtlinie umbenannt.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

Im folgenden Beispiel wird die Beschreibung einer Tag-Richtlinie hinzugefügt oder geändert.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

Im folgenden Beispiel wird das JSON-Richtliniendokument geändert, das einer KI-Service-Opt-Out-Richtlinie zugeordnet ist. In diesem Beispiel wird der Inhalt einer Datei namens `policy.json` mit folgendem Text entnommen:

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
```

```
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWS-SDKs: UpdatePolicy

Bearbeiten von Tags, die einer Tag-Richtlinie zugeordnet sind

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie die Tags hinzufügen oder entfernen, die einer Tag-Richtlinie zugeordnet sind. Führen Sie dazu die folgenden Schritte aus.

Mindestberechtigungen

Um die an eine Tag-Richtlinie in Ihrer AWS-Organisation angefügten Tags zu bearbeiten, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeOrganization` (Nur Konsole – um zur Richtlinie zu navigieren)
- `organizations:DescribePolicy` (Nur Konsole – um zur Richtlinie zu navigieren)
- `organizations:TagResource`

- `organizations:UntagResource`

AWS Management Console

So bearbeiten Sie die Tags, die an eine AI-Service-Opt-Out-Richtlinie angehängt sind

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Tag-Richtlinien den Namen der Richtlinie mit den Tags aus, die Sie bearbeiten möchten.
3. Wählen Sie auf der Detailseite der ausgewählten Richtlinie die Registerkarte Tags und dann Tags verwalten aus.
4. Sie können auf dieser Seite eine der folgenden Aktionen ausführen:
   - Bearbeiten Sie den Wert für ein beliebiges Tag, indem Sie einen neuen Wert über dem alten eingeben. Sie können den Schlüssel nicht ändern. Um einen Schlüssel zu ändern, müssen Sie das Tag mit dem alten Schlüssel löschen und ein Tag mit dem neuen Schlüssel hinzufügen.
   - Entfernen Sie ein vorhandenes Tag, indem Sie Entfernen wählen.
   - Fügen Sie ein neues Tag-Schlüssel-Wert-Paar hinzu. Wählen Sie Tag hinzufügen aus und geben Sie dann den neuen Schlüsselnamen und den optionalen Wert in die bereitgestellten Felder ein. Wenn Sie das Feld Wert leer lassen, ist der Wert eine leere Zeichenfolge; er ist nicht `null`.
5. Wählen Sie Änderungen speichern, nachdem Sie alle gewünschten Ergänzungen, Entfernungen und Änderungen vorgenommen haben.

AWS CLI & AWS SDKs

So bearbeiten Sie die Tags, die an eine Tag-Richtlinie angefügt sind

Sie können einen der folgenden Befehle verwenden, um die einer Tag-Richtlinie zugeordneten Tags zu bearbeiten:

- AWS CLI: tag-resource und untag-resource
- AWS-SDKs: TagResource und UntagResource

Löschen einer Tag-Richtlinie

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Richtlinie löschen, die Sie in Ihrer Organisation nicht mehr benötigen.

Bevor Sie eine Richtlinie löschen können, müssen Sie sie zuerst von allen angehängten Elementen trennen.

> **Mindestberechtigungen**
>
> Um eine Tag-Richtlinie zu löschen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:
>
> - `organizations:DeletePolicy`

AWS Management Console

So löschen Sie eine Tag-Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2.
3. Wählen Sie auf der Seite Tag-Richtlinien die Richtlinie aus, die Sie löschen möchten.
4. Sie müssen zuerst die Richtlinie, die Sie löschen möchten, von allen Stammverzeichnissen, Organisationseinheiten und Konten trennen. Wählen Sie die Registerkarte Ziele aus, wählen Sie das Optionsfeld neben jedem Stamm, jeder OU oder jedem Konto aus, die in der Liste Ziele angezeigt werden und wählen Sie dann Trennen. Wählen Sie im Bestätigungsdialogfeld Trennen aus.
5. Wählen Sie oben auf der Seite Löschen.
6. Geben Sie im Bestätigungsdialogfeld den Namen der Richtlinie ein und wählen Sie dann Löschen aus.

AWS CLI & AWS SDKs

So löschen Sie eine Tag-Richtlinie

Zum Löschen einer Tag-Richtlinie können Sie eine der folgenden Optionen verwenden:

- AWS CLI: delete-policy

  Im folgenden Beispiel wird die angegebene Richtlinie gelöscht. Sie funktioniert nur, wenn die Richtlinie keinem Stamm, keiner Organisationseinheit oder keinem Konto angefügt ist.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: DeletePolicy

Anfügen und Trennen von Tag-Richtlinien

Sie können Tag-Richtlinien sowohl für eine ganze Organisation als auch für Organisationseinheiten (OUs) sowie einzelne Konten verwenden.

- Wenn Sie eine Tag-Richtlinie an den Organisationsstamm anhängen, gilt die Tag-Richtlinie für alle Organisationseinheiten und -Konten der Stammmitglieder.
- Wenn Sie eine Tag-Richtlinie an eine OU anhängen, gilt diese Tag-Richtlinie für die Konten, die zur OU gehören. Diese Konten unterliegen auch jeder Tag-Richtlinie, die mit dem Organisationsstamm verknüpft ist.
- Wenn Sie eine Tag-Richtlinie an ein Konto anhängen, gilt diese Tag-Richtlinie für das Konto. Darüber hinaus unterliegt dieses Konto allen Tag-Richtlinien, die mit dem Organisationsstamm verknüpft sind, sowie allen Tag-Richtlinien, die einer OU zugeordnet sind, zu der das Konto gehört.

Die Aggregation aller Tag-Richtlinien, die das Konto erbt, sowie jede direkt mit dem Konto verknüpfte Tag-Richtlinie ist die effektive Tag-Richtlinie. Weitere Informationen finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

> **Important**
>
> Ressourcen ohne Tags werden in den Ergebnisses nicht als nichtkonform angezeigt.

Mindestberechtigungen

Um Tag-Richtlinien anzuhängen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:

- `organizations:AttachPolicy`

AWS Management Console

Sie können eine Tag-Richtlinie anfügen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto navigieren, an das bzw. die Sie die Richtlinie anfügen möchten.

So fügen Sie eine Tag-Richtlinie an, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, dem Sie eine Richtlinie anfügen möchten, und wählen Sie dann den Namen aus. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Eintrag für Tag-Richtlinien die Option Anfügen.
4. Suchen Sie die gewünschte Richtlinie und wählen Sie Richtlinie anfügen aus.

   Die Liste der angehängten Tag-Richtlinien auf der Registerkarte Richtlinien wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

So fügen Sie eine Tag-Richtlinie hinzu, indem Sie zur Richtlinie navigieren

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Wählen Sie auf der Seite Tag-Richtlinien den Namen der Richtlinie aus, die Sie anfügen möchten.
3. Klicken Sie in der Registerkarte Ziele auf Anfügen.
4. Aktivieren Sie das Optionsfeld neben dem Stammverzeichnis, der Organisationseinheit oder dem Konto, an das bzw. die Sie die Richtlinie anfügen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
5. Wählen Sie Attach policy (Richtlinie anfügen) aus.

   Die Liste der angehängten Tag-Richtlinien auf der Registerkarte Ziele wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So fügen Sie dem Organisationsstamm, der OU oder dem Konto eine Tag-Richtlinie hinzu

Sie können eine der folgenden Optionen verwenden, um eine Tag-Richtlinie hinzuzufügen:

- AWS CLI: attach-policy

  Das folgende Verfahren veranschaulicht, wie Sie die gerade erstellte Tag-Richtlinie einem einzelnen Testkonto hinzufügen.

  - Fügen Sie Ihrem Testkonto die Tag-Richtlinie hinzu, indem Sie einen Befehl wie den folgenden ausführen:

    ```
    $ aws organizations attach-policy \
        --target-id <account-id> \
        --policy-id p-a1b2c3d4e5
    ```

    Dieser Befehl hat keine Ausgabe, wenn er erfolgreich ist.
- AWS-SDKs: AttachPolicy

Die Richtlinienänderung wird sofort wirksam.

Weitere Vorgehensweisen

Nach dem Hinzufügen einer Tag-Richtlinie, können Sie herausfinden, wie konform Ihre Ressourcen mit dieser Tag-Richtlinie sind. Verwenden Sie dazu die Resource-Groups-Konsole. Weitere Informationen finden Sie unter Evaluieren der Compliance eines Kontos im AWS Resource GroupsBenutzerhandbuch.

Trennen einer Tag-Richtlinie

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Tag-Richtlinie vom Organisationsstamm, von der Organisationseinheit oder vom Konto trennen. Nach dem Trennen der Tag-Richtlinie von einem Element, gilt diese Richtlinie nicht mehr für Konten, auf die sich das jetzt getrennte Element ausgewirkt hat. Führen Sie zum Trennen einer Richtlinie die folgenden Schritte aus.

> **Mindestberechtigungen**
>
> Um eine Tag-Richtlinie vom Organisationsstamm, der OU oder dem Konto zu trennen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktion verfügen:
>
> - `organizations:DetachPolicy`

AWS Management Console

Sie können eine Tag-Richtlinie trennen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto navigieren, von dem bzw. der Sie die Richtlinie trennen möchten.

So trennen Sie eine Tag-Richtlinie durch Navigieren zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, dem sie angefügt ist

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, von dem Sie eine Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. Wählen Sie den Namen des Stammes, der Organisationseinheit oder des Kontos aus.

3. Wählen Sie auf der Registerkarte Richtlinien das Optionsfeld neben der Tag-Richtlinie aus, die Sie trennen möchten und wählen Sie dann Trennen aus.
4. Wählen Sie im Bestätigungsdialogfeld Richtlinie trennen aus.

   Die Liste der angehängten Tag-Richtlinien wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

So trennen Sie eine Tag-Richtlinie durch Navigieren zur Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Tag-Richtlinien den Namen der Richtlinie aus, die Sie von einem Stamm, einer OU oder einem Konto trennen möchten.
3. Wählen Sie auf der Registerkarte Ziele das Optionsfeld neben dem Stamm, der OU oder dem Konto aus, von dem Sie die Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
4. Wählen Sie Detach (Trennen) aus.
5. Wählen Sie im Bestätigungsdialogfeld Trennen aus.

   Die Liste der angehängten Tag-Richtlinien wird aktualisiert. Die Richtlinienänderung wird sofort wirksam.

AWS CLI & AWS SDKs

So trennen Sie eine Tag-Richtlinie vom Organisationsstamm, der OU oder dem Konto

Sie können eine der folgenden Optionen verwenden, um eine Tag-Richtlinie zu trennen:

- AWS CLI: detach-policy
- AWS-SDKs: DetachPolicy

Die Richtlinienänderung wird sofort wirksam.

Anzeigen effektiver Tag-Richtlinien

Bevor Sie mit der Überprüfung des Compliance-Status für getaggte Ressourcen in einem Konto beginnen, ist es hilfreich, zuerst die effektive Tag-Richtlinie eines Kontos zu ermitteln.

Was ist die effektive Tag-Richtlinie?

Die effektive Tag-Richtlinie gibt die Tagging-Regeln an, die für ein Konto gelten. Es handelt sich um die Aggregation aller Tag-Richtlinien, die das Konto erbt, sowie jede Tag-Richtlinie, die direkt mit dem Konto verknüpft ist. Wenn Sie dem Organisationsstamm eine Tag-Richtlinie hinzufügen, gilt dies für alle Konten in Ihrer Organisation. Wenn Sie eine Tag-Richtlinie einer OU hinzufügen, gilt dies für alle Konten und OUs, die zur OU gehören.

Beispielsweise kann die dem Organisationsstamm hinzugefügte Tag-Richtlinie ein `CostCenter`-Tag mit vier kompatiblen Werten definieren. Eine separate Tag-Richtlinie, die dem Konto zugeordnet ist, kann den `CostCenter`-Schlüssel auf nur zwei der vier kompatiblen Werte beschränken. Die Kombination dieser Tag-Richtlinien umfasst die effektive Tag-Richtlinie. Im Ergebnis sind nur zwei der vier konformen Tag-Werte des Kontos, die in der Tag-Richtlinie des Organisationsstamms definiert sind, konform.

Weitere Informationen und weitergehende Beispiele dafür, wie effektive Tag-Richtlinien generiert werden, finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

Anzeigen der effektiven Tag-Richtlinie

Sie können die effektive Tag-Richtlinie für ein Konto über die AWS Management Console, AWS API oder AWS Command Line Interface anzeigen.

Mindestberechtigungen

Um die effektive Tag-Richtlinie für ein Konto anzuzeigen, müssen Sie über die Berechtigung zum Ausführen der folgenden Aktionen verfügen:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization`

AWS Management Console

Anzeigen der effektiven Tag-Richtlinie für ein Konto

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite AWS-Konten den Namen des Kontos aus, für das Sie die effektive Tag-Richtlinie anzeigen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Abschnitt Tag-Richtlinien die Option Effektive Tag-Richtlinie für dieses AWS-Konto anzeigen aus.

   Die Konsole zeigt die effektive Richtlinie an, die auf das angegebene Konto angewendet wird.

   > **Note**
   >
   > Es ist nicht möglich, eine effektive Richtlinie zu kopieren und einzufügen und ohne wesentliche Änderungen als JSON für eine andere Tagrichtlinie zu verwenden. Tagrichtliniendokumente müssen die Vererbungsoperatoren enthalten, die angeben, wie die einzelnen Einstellungen zu der endgültigen effektiven Richtlinie zusammengeführt werden.

AWS CLI & AWS SDKs

Anzeigen der effektiven Tag-Richtlinie für ein Konto

Sie können eine der folgenden Optionen zum Anzeigen der effektiven Tag-Richtlinie verwenden:

- AWS CLI: describe-effective-policy

  Um zu ermitteln, welche Tagging-Regeln einem Konto vererbt oder zugeordnet sind, führen Sie folgende Schritte aus dem Konto heraus aus und speichern die Ergebnisse in einer Datei:

```
$ aws organizations describe-effective-policy \
    --policy-type TAG_POLICY
```

```
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

Wenn eine Tag-Richtlinie sowohl an das Konto als auch an den Stamm oder eine beliebige Organisationseinheit angehängt ist, definiert die Kombination aller übernommenen Richtlinien die effektive Tag-Richtlinie des Kontos. In diesen Fällen gibt das Ausführen von `describe-effective-policy` über das Konto den zusammengeführten Inhalt aller Tag-Richtlinien in der Kontohierarchie zurück.

- AWS-SDKs: DescribeEffectivePolicy

Verwenden von Amazon EventBridge zum Überwachen nicht konformer Tags

Sie können Amazon EventBridge, früher Amazon CloudWatch Events, verwenden, um zu überwachen, wenn nicht konforme Tags eingeführt werden. Im folgenden Beispielereignis gibt der `"false"` Wert für `tag-policy-compliant` an, dass ein neues Tag nicht mit der effektiven Tag-Richtlinie konform ist.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
```

```
  }
}
```

Sie können Ereignisse abonnieren und Zeichenfolgen oder Muster angeben, die überwacht werden sollen. Weitere Informationen zu EventBridge finden Sie im Benutzerhandbuch für Amazon EventBridge.

Grundlegendes zur Durchsetzung

In einer Tag-Richtlinie kann angegeben werden, dass für bestimmte Ressourcentypen nicht-regelkonforme Tagging-Vorgänge erzwungen werden. Mit anderen Worten: Es wird verhindert, dass für bestimmte Ressourcentypen nicht regelkonforme Tagging-Anforderungen durchgeführt werden.

> **Important**
>
> Die Erzwingung hat keine Auswirkungen auf Ressourcen, die ohne Tags erstellt werden.

Führen Sie beim Erstellen einer Tag-Richtlinie eine der folgenden Aktionen aus, um die Compliance mit Tag-Richtlinien zu erzwingen:

- Wählen Sie auf der Registerkarte Visual editor (Visueller Editor) die Option Prevent noncompliant operations for this tag (Nicht-konforme Operationen für dieses Tag verhindern) aus.
- Verwenden Sie in der Registerkarte JSON das Feld `enforced_for`. Hinweise zur Syntax der Tag-Richtlinie finden Sie unter Syntax und Beispiele für Tag-Richtlinien.

Befolgen Sie die folgenden bewährten Methoden, um die Compliance von Tag-Richtlinien durchzusetzen:

- Vorsicht beim Durchsetzen der Compliance – Es ist wichtig, dass Sie die Auswirkungen der Verwendung von Tag-Richtlinien verstehen und die empfohlenen, in Erste Schritte mit Tag-Richtlinien beschriebenen Workflows befolgen. Probieren Sie die Durchsetzung auf einem Testkonto aus, bevor Sie sie auf weitere Konten ausweiten. Andernfalls verhindern Sie, dass Benutzer in den Konten Ihrer Organisation die benötigten Ressourcen kennzeichnen.
- Achten Sie darauf, welche Ressourcentypen Sie durchsetzen können – Sie können die Compliance von Tag-Richtlinien nur für unterstützte Ressourcentypen durchsetzen. Ressourcentypen, die das Durchsetzen der Compliance unterstützen, werden aufgelistet, wenn Sie den visuellen Editor zum Erstellen einer Tag-Richtlinie verwenden.

- Grundlegendes zu Interaktionen mit einigen Services – Einige AWS-Services verfügen über containerähnliche Ressourcengruppierungen, die automatisch Ressourcen für Sie erstellen. Tags können von einer Ressource eines Services zu einer anderen weitergeleitet werden. Tags in Amazon-EC2-Auto-Scaling-Gruppen und Amazon-EMR-Clustern können beispielsweise automatisch an die enthaltenen Amazon-EC2-Instances weitergegeben werden. Sie verfügen möglicherweise über Tag-Richtlinien für Amazon EC2, die strenger sind als diejenigen für Auto-Scaling-Gruppen oder EMR-Cluster. Wenn Sie die Durchsetzung aktivieren, verhindert die Tag-Richtlinie, dass Ressourcen getaggt werden, und blockiert möglicherweise die dynamische Skalierung und Bereitstellung.

In den folgenden Abschnitten wird gezeigt, wie Sie nicht konforme Ressourcen finden und diese entsprechend korrigieren können.

Suchen nicht konformer Ressourcen für ein Konto

Für jedes Konto können Sie Informationen über nicht konforme Ressourcen abrufen. Sie sollten diesen Befehl in jeder Region ausführen, in der das Konto über Ressourcen verfügt.

Um nicht konforme Ressourcen für ein Konto mit einer Tag-Richtlinie zu finden, können Sie den folgenden Befehl ausführen, wenn Sie sich beim Konto anmelden und die Ergebnisse in einer Datei speichern:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Korrigieren nicht konformer Tags in Ressourcen

Nach dem Auffinden nicht konformer Tags, nehmen Sie Korrekturen mithilfe einer der folgenden Methoden vor. Sie müssen in dem Konto angemeldet sein, das die Ressource mit nicht konformen Tags enthält:

- Verwenden Sie die Konsolen- oder Tagging-API-Operationen des AWS-Services, der die nicht konformen Ressourcen erstellt hat.
- Verwenden Sie die AWS Resource Groups-Operationen TagResources und UntagResources, um Tags hinzuzufügen, die mit der gültigen Richtlinie konform sind, oder um nicht konforme Tags zu entfernen.

Auffindung und Behebung zusätzlicher Probleme bei Compliance-Problemen.

Das Auffinden und Korrigieren von Compliance-Problemen ist ein iterativer Prozess. Wiederholen Sie die Schritte in den beiden vorherigen Abschnitten, bis die Ressourcen, die Sie interessieren, mit Ihrer Tag-Richtlinie konform sind.

Erstellung eines organisationsweiten Compliance-Berichts

Sie können jederzeit einen Bericht erstellen, der alle getaggten Ressourcen in AWS-Konten Ihrer gesamten Organisation auflistet. Der Bericht zeigt an, ob die Ressourcen mit der effektiven Tag-Richtlinie konform sind. Beachten Sie, dass es bis zu 48 Stunden dauern kann, bis Änderungen, die Sie an einer Tag-Richtlinie oder Ressourcen vornehmen, im organisationsweiten Compliance-Bericht berücksichtigt werden. Angenommen, Sie haben eine Tag-Richtlinie, die ein neues standardisiertes Tag für einen Ressourcentyp definiert. Ressourcen dieses Typs, die nicht über dieses Tag verfügen, werden im Bericht für bis zu 48 Stunden als konform angezeigt.

Sie können den Bericht aus dem Verwaltungskonto Ihrer Organisation in der `us-east-1`-Region generieren, sofern er Zugriff auf einen Amazon-S3-Bucket hat. Der Bucket muss über eine angehängte Bucket-Richtlinie verfügen, wie in Amazon-S3-Bucket-Richtlinie zum Speichern von Berichten dargestellt. Zum Generieren des Berichts führen Sie folgenden Befehl aus:

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

Sie können jeweils einen Bericht erstellen.

Es kann etwas dauern, bis dieser Bericht fertiggestellt ist. Sie können den Status überprüfen, indem Sie den folgenden Befehl ausführen:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Nachdem der obige Befehl erneut `SUCCEEDED` zurückgibt, können Sie den Bericht aus dem Amazon-S3-Bucket öffnen.

Services und Ressourcentypen, die die Durchsetzung unterstützen

Die folgenden Services und Ressourcentypen unterstützen die Erzwingung mit Tag-Richtlinien:

Service-Name	Ressourcentyp	JSON-Syntax
Amazon API Gateway	• API-Schlüssel • Domänennamen • REST API-Operationen • Phasen	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Komponente • Thema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Anwendung • Konfigurationsprofil • Bereitstellung • Bereitstellungsstrategie • Umgebung	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Alle • Gateway-Route • Mesh • Route • Virtuelles Gateway • Virtueller Knoten	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"`

Service-Name	Ressourcentyp	JSON-Syntax
	• Virtueller Router • Virtueller Service	• `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Alle • Arbeitsgruppe	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• Bewertung • Bewertungs-Framework • Kontrolle	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Backup-Plan • Vault • Gateway • Hyper Visor • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• Aufgabe • Auftragsdefinition • Auftragswarteschlange	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Ereignis	• `"bugbust:event"`
AWS Certificate Manager	• Alle • Zertifikate • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Chime	• Anwendungs-Instance • Kanal • Medienpipeline • Meeting • SIP-Medie nanwendungen • Benutzera nwendungs-Instance • Sprachanschluss	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Zusammenarbeit • Konfigurierte Tabelle • Mitgliedschaften • Konfigurierte Tabellenzuordnung	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/conf iguredtableassociation"`
AWS Cloud9	• Umgebung	• `"cloud9:environment"`
Amazon CloudFront	• Alle • Distribution • Streaming-Distribu tion	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distr ibution"`
AWS CloudTrail	• Alle • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon CloudWatch	• Alle • Alarm • Contributor Insights-Regel • Metrik-Stream	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`
Amazon CloudWatch Internetmonitor	• Überwachen	• `"internetmonitor:monitor"`
CloudWatch Amazon-Protokolle	• Protokollgruppe	• `"logs:log-group"`
Amazon CloudWatch Observability Access Manager	• Link • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Alle • Projekt	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Verbindungen	• `"codecatalyst:connections"`
AWS CodeCommit	• Alle • Repository	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Alle • Aktionstyp • Pipeline • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Amazon Cognito Identity	• Alle • Identitäten-Pool	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Amazon-Cognito-Benutzerpools	• Alle • Benutzerpool	• `"cognito-idp:*"` • `"cognito-idp:userpool"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Comprehend	• Alle • Dokumenten-Classifier • Entity-Erkennung	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Alle • Aggregationsautorisierung • Config-Aggregator • Config-Regel	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Amazon-Rezensent	• Zuordnung	• `"codeguru-reviewer:association"`
CodeGuru Sicherheit bei Amazon	• Scan	• `"codeguru-security:scans"`
CodeConnections	• Verbindung • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`
Amazon Connect	• Gesprächsablauf • Integration Association • Warteschlange • Quick Connect • Routing Profile (Weiterleitungsprofil) • Benutzer	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Connect Wisdom	• Assistent • Zuordnung • Inhalt • Wissensbasis • Sitzung	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Alle • Endpunkt • ES • Rep. • Untergrp. • Aufgabe	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Amazon Data Lifecycle Manager	• Richtlinie	• `"dlm:policy"`
AWS Direct Connect	• Alle • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Alle • Tabelle	• `"dynamodb:*"` • `"dynamodb:table"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon EC2	• Kapazitätsreservierung • Client-VPN-Endpunkt • Kunden-Gateway • DHCP-Optionen • Elastic IP-Adressen • Flotte • FPGA-Image • Host-Reservierung • Image • Instance • Internet-Gateway • Startvorlage • NAT-Gateway • Netzwerk-ACL • Netzwerkschnittstelle • Reserved Instances • Routing-Tabelle • Sicherheitsgruppe • Snapshot • Spot-Instance-Anforderung • Subnetz • Traffic Mirror-Filter • Traffic Mirror-Sitzung • Traffic Mirror-Ziel • Volume	• `"ec2:capacity-reservation"` • `"ec2:client-vpn-endpoint"` • `"ec2:customer-gateway"` • `"ec2:dhcp-options"` • `"ec2:elastic-ip"` • `"ec2:fleet"` • `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"` • `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:launch-template"` • `"ec2:natgateway"` • `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"` • `"ec2:snapshot"` • `"ec2:spot-instances-request"` • `"ec2:subnet"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"` • `"ec2:traffic-mirror-target"` • `"ec2:volume"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"` • `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"`

Service-Name	Ressourcentyp	JSON-Syntax
	• VPC • VPC-Endpunkt • VPC-Endpunktservice • VPC-Peering-Verbindung • VPN-Verbindung • VPN-Gateway	• `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`
Amazon-EC2-Papierkorb	• Regel	• `"rbin:rule"`
Amazon Elastic Container Registry	• Repository	• `"ecr:repository"`
AWS Elastic Beanstalk	• Anwendung • Anwendungsversion • Konfigurationsvorlage • Plattform	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Service	• Cluster • Service • Aufgabensatz	• `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-set"`
Amazon Elastic File System	• Alle • Dateisystem	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon Elastic Inference	• Accelerator	• `"elastic-inference:elastic-inference-accelerator"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Elastic Kubernetes Service	• Cluster	• `"eks:cluster"`
Amazon Elastic Search	• Domain	• `"es:domain"`
Amazon EMR	• Cluster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR Serverless	• Anwendung	• `"emr-serverless:applications"`
AWS Auflösung der Entität	• Abgleich-Workflow • Schemazuordnung	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Cluster	• `"elasticache:cluster"`
Amazon EventBridge	• Alle • Event Bus • Regel	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
EventBridge Amazon-Pfeifen	• Pipe	• `"pipes:pipe"`
Amazon EventBridge Scheduler	• Gruppe planen	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• Detektor • Detektor-Version • Modell • Regel • Variable	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Global Accelerator	• Accelerator	• `"globalaccelerator:accelerator"`
Elastic Load Balancing	• Alle • Load Balancer • Zielgruppe	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Alle • Backup • Dateisystem	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Detektor • Filter • IP-Satz • Threat-Intelligence-Satz	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Datenspeicher	• `"healthlake:datastore  "`

Service-Name	Ressourcentyp	JSON-Syntax
AWS HealthOmics	• Annotationsspeicher • Version des Anmerkungs-Speicher • Referenzspeicher • Referenz • Ausführen • Gruppe ausführen • Sequenzspeicher • Satz lesen • Variantenspeicher • Workflow	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filter	• `"inspector2:filter "`
AWS Identity and Access Management	• Instance-Profil • MFA • OIDC-Anbieter • Richtlinie • SAML-Anbieter • Serverzertifikat	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• Alle • Kanal • Datensatz • Datenspeicher • Pipeline	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`

Service-Name	Ressourcentyp	JSON-Syntax
AWS IoT Events	• Alle • Detektormodell • Eingabe	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Anwendung	• `"iotfleethub:application"`
AWS IoT SiteWise	• Komponente • Komponent enmodell	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Massenbereitstellung • Konnektordefinition • Kerndefinition • Gerätedefinition • Funktionsdefinition • Logger-Definition • Ressourcendefinition • Abonnementdefinition	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Alle • Schlüssel	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Alle • Anwendung	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Data Firehose	• Alle • Bereitstellungsstream	• `"firehose:*"` • `"firehose:deliverystream"`

Service-Name	Ressourcentyp	JSON-Syntax
AWS Lambda	• Alle • Funktion	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Benutzerdefinierte Datenkennung	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Container	• `"mediastore:container"`
Amazon MQ	• Broker • Konfiguration	• `"mq:broker"` • `"mq:configuration"`
Amazon Network Firewall	• Firewall • Firewall-Richtlinie • Zustandsbehaftete Regelgruppe • Zustandslose Regelgruppe	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon OpenSearch Serverlos	• Sammlung	• `"aoss:collection"`
AWS Organizations	• Account • Organisationseinheit • Richtlinie • Root	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`
Amazon Pinpoint SMS Voice V2	• Konfigurationssatz • Abmeldeliste • Telefonnummer • Pool • Sender-ID	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon RDS	• Cluster-Parametergruppe • Cluster-Endpunkt • Ereignisabonnement • DB-Optionsgruppe • DB-Parametergruppe • DB-Proxy • DB-Proxy-Endpunkt • Reservierte DB-Instance • DB-Sicherheitsgruppe • DB subnet group (DB-Subnetzgruppe) • Zielgruppe	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Redshift	• Alle • Cluster • DB-Gruppe • DB-Name • DB-Benutzer • Ereignisabonnement • HSM-Clientzertifikat • HSM-Konfiguration • Parametergruppe • Snapshot • Snapshot-Kopie-Berechtigung • Snapshot-Zeitplan • Subnetzgruppe	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`
Amazon Redshift Serverless	• Namespace • Arbeitsgruppe	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Alle • Ressourcenfreigabe	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Alle • Gruppe	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Gehostete Zone	• `"route53:hostedzone"`

Service-Name	Ressourcentyp	JSON-Syntax
Amazon Route 53 Resolver	• Alle • Resolver-Endpunkt • Resolver-Regel	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Bucket • Speicherlinse	• `"s3:bucket"` • `"s3:storage-lens"`
Amazon SageMaker	• App-Image-Konfiguration • Artefakt • Kontext • Trainingsauftrag • Auftrag verarbeiten • Modellpaketgruppe • Benutzeroberfläche für menschliche Aufgaben • Modellpaket • Aktion • Pipeline • Experiment • Flow-Definition • Projekt	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Alle • Secret	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS Sicherheit, Lake	• Data Lake • Subscriber	• `"securitylake:data-lake"` • `"securitylake:subscriber"`

Service-Name	Ressourcentyp	JSON-Syntax
AWS Service Catalog	• Anwendung • Attribut-Gruppe • Portfolio • Produkt	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service (SNS)	• Thema	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Warteschlange	• `"sqs:queue"`
Amazon States Language	• Alle • Aktivität • State Machine (Zustandsautomat)	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Aktivität	• `"states:activity"`
AWS Storage Gateway	• Alle • Gateway • Freigeben • Band • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`

Service-Name	Ressourcentyp	JSON-Syntax
AWS Systems Manager	• Zuordnung • Automatisierungsausführung • Dokument • Wartungsfenster • Verwaltete Instance • Ops-Element • Patch-Baseline • Sitzung • Kontakte	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
AWS Transfer Family	• Server • Benutzer • Workflow	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Architected	• Workload	• `"wellarchitected:workload"`
AWS Wickr	• Network (Netzwerk)	• `"wickr:network"`
Amazon WorkSpaces	• Alle • Verzeichnis • WorkSpace • WorkSpaces bündeln • WorkSpaces Bild • WorkSpaces IP-Gruppe	• `"workspaces:*"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
Amazon WorkLink	• Flotte	• `"worklink:fleet"`

Syntax und Beispiele für Tag-Richtlinien

Auf dieser Seite wird die Syntax für Tag-Richtlinien beschrieben und durch Beispiele illustriert.

Syntax für Tag-Richtlinien

Eine Tag-Richtlinie ist eine Textdatei, die den Regeln der JSON-Struktur folgt. Die Syntax für Tag-Richtlinien folgt der Syntax für Verwaltungsrichtlinientypen. Eine umfassende Erläuterung dieser Syntax finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen. Dieses Thema konzentriert sich auf die Anwendung dieser allgemeinen Syntax auf die spezifischen Anforderungen des Tagrichtlinientyps.

Die folgende Tag-Richtlinie zeigt die Basissyntax:

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

Zur Syntax der Tag-Richtlinie gehören die folgenden Elemente:

- Der Schlüsselname des Feldes `tags`. Tag-Richtlinien beginnen immer mit diesem feststehenden Schlüsselnamen. Er befindet sich in der obersten Zeile der aufgeführten Beispielrichtlinie.
- Ein Richtlinienschlüssel zur eindeutigen Kennzeichnung der Richtlinienanweisung. Mit Ausnahme der Fallbehandlung muss er mit dem Wert für den Tag-Schlüssel übereinstimmen. Im Gegensatz

zu dem (als nächstes beschriebenen) Tag-Wert wird bei dem Richtlinienschlüssel nicht zwischen Groß- und Kleinschreibung unterschieden.

In diesem Beispiel ist `costcenter` der Richtlinienschlüssel.

- Mindestens ein Tag-Schlüssel als Angabe des zulässigen Tag-Schlüssels mit der Groß-/Kleinschreibung, der die Ressourcen entsprechen sollen. Wenn keine Fallbehandlung definiert ist, wird für Tag-Schlüssel standardmäßig die Kleinschreibung verwendet. Der Wert für den Tag-Schlüssel muss mit dem Wert für den Richtlinienschlüssel übereinstimmen. Die Schreibung des Werts kann allerdings unterschiedlich sein, da hier nicht zwischen Groß- und Kleinschreibung unterschieden wird.

  In diesem Beispiel ist `CostCenter` der Tag-Schlüssel. Dies ist die Fallbehandlung, die für die Einhaltung der Tag-Richtlinie erforderlich ist. Ressourcen mit alternativer Fallbehandlung für diesen Tag-Schlüssel sind nicht mit der Tag-Richtlinie konform.

  Sie können in einer Tag-Richtlinie mehrere Tag-Schlüssel definieren.

- (Optional) Eine Liste mit einem oder mehreren zulässigen Tag-Werten für den Tag-Schlüssel. Wenn in der Tag-Richtlinie kein Tag-Wert für einen Tag-Schlüssel angegeben wird, gilt jeder Wert (auch kein Wert) als regelkonform.

  In diesem Beispiel sind `100` und `200` zulässige Werte für den Tag-Schlüssel `CostCenter`.

- (Optional) Eine `enforced_for`-Option, die angibt, ob nicht regelkonforme Tagging-Vorgänge für bestimmte Services und Ressourcen unterbunden werden sollen. In der Konsole ist dies die Option Prevent noncompliant operations for this tag (Nicht regelkonforme Vorgänge für dieses Tag verhindern) im visuellen Editor für die Erstellung von Tag-Richtlinien. Die Standardeinstellung für diese Option ist Null.

  In der Tag-Beispielrichtlinie wird angegeben, dass dieses Tag für alle AWS Secrets Manager-Ressourcen erforderlich ist.

  > **Warning**
  >
  > Sie sollten diese Option nur dann ändern, wenn Sie mit der Verwendung von Tag-Richtlinien vertraut sind. Andernfalls riskieren Sie, dass Benutzer die benötigten Ressourcen in den Konten Ihrer Organisation nicht erstellen können.

- Operatoren, die angeben, wie diese Tag-Richtlinie mit anderen Tag-Richtlinien in der Organisationsstruktur zu einer effektiven Tag-Richtlinie für das Konto zusammengeführt wird. In

diesem Beispiel dient `@@assign` dazu, `tag_key`, `tag_value` und `enforced_for` Zeichenfolgen zuzuweisen. Weitere Informationen zu Operatoren finden Sie unter Vererbungsoperatoren.

- – Sie können den Platzhalter `*` in Tag-Werten und `enforced_for`-Feldern verwenden.
  - Je Tag-Wert ist nur ein Platzhalter zulässig. `*@example.com` ist beispielsweise zulässig, aber `*@*.com` ist es nicht.
  - Für `enforced_for` können Sie bei einigen Services `<service>:*` verwenden, um die Durchsetzung für alle Ressourcen für diesen Service zu ermöglichen. Eine Liste der Services und Ressourcentypen, die `enforced_for` unterstützen, finden Sie unter Services und Ressourcentypen, die die Durchsetzung unterstützen.

    Sie können keinen Platzhalter verwenden, um alle Services oder eine Ressource für alle Services anzugeben.

Tag-Richtlinienbeispiele

Die folgenden Tag-Richtlinienbeispiele dienen nur zu Informationszwecken.

> **Note**
>
> Bevor Sie diese Beispiel-Tag-Richtlinien in Ihrer Organisation verwenden, beachten Sie Folgendes:
>
> - Befolgen Sie unbedingt den empfohlenen Workflow, um sich mit Tag-Richtlinien vertraut zu machen.
> - Überprüfen Sie diese Tag-Richtlinien sorgfältig, und passen Sie sie an Ihre individuellen Anforderungen an.
> - Alle Zeichen, die Sie in Ihrer Tag-Richtlinie verwenden, unterliegen einer maximalen Größe. In den Beispielen in diesem Handbuch sind die dargestellten Tag-Richtlinien mit zusätzlichen Leerraumzeichen formatiert, um ihre Lesbarkeit zu verbessern. Sie können die Leerraumzeichen löschen, um Speicherplatz zu sparen, wenn sich die Größe Ihrer Richtlinie der maximalen Größe nähert. Beispiele für Leerraumzeichen sind Leerzeichen und Zeilenumbrüche außerhalb von Anführungszeichen.
> - Ressourcen ohne Tags werden in den Ergebnisses nicht als nichtkonform angezeigt.

Beispiel 1: Festlegen eines organisationsweiten Tag-Schlüssels

Das folgende Beispiel zeigt eine Tag-Richtlinie, die nur zwei Tag-Schlüssel und die Groß-/Kleinschreibung definiert, die Sie als Standard für die Konten in Ihrer Organisation verwenden möchten.

Richtlinie A – Tag-Richtlinie des Organisationsstamms

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Diese Tag-Richtlinie definiert zwei Tag-Schlüssel: `CostCenter` und `Project`. Das Anhängen dieser Tag-Richtlinie an den Organisationsstamm hat folgende Auswirkungen:

- Alle Konten in Ihrer Organisation übernehmen diese Tag-Richtlinie.
- Alle Konten in Ihrer Organisation müssen zur Konformität die definierte Fallbehandlung verwenden. Ressourcen mit `CostCenter`- und `Project`-Tags sind konform. Ressourcen mit alternativer Fallbehandlung für den Tag-Schlüssel (z. B. `costcenter`, `Costcenter` oder `COSTCENTER`) sind nicht konform.
- Durch die `@@operators_allowed_for_child_policies": ["@@none"]`-Zeilen werden die Tag-Schlüssel „gesperrt“. In Tag-Richtlinien, die in einer der unteren Ebenen in der Organisationsstruktur angesiedelt sind (untergeordnete Richtlinien), sind keine Operatoren zulässig, durch die Werte festgelegt und durch die der Tag-Schlüssel und die Fallbehandlung geändert werden.
- Wie bei allen Tag-Richtlinien werden nicht mit Tags versehene Ressourcen oder Tags, die nicht in der Tag-Richtlinie definiert sind, nicht auf Übereinstimmung mit der Tag-Richtlinie ausgewertet.

AWS empfiehlt, dieses Beispiel als Leitfaden für die Erstellung einer ähnlichen Tag-Richtlinie für die gewünschten Tag-Schlüssel zu verwenden. Fügen Sie sie zum Organisations-Root hinzu. Erstellen Sie anschließend eine Tag-Richtlinie ähnlich dem nächsten Beispiel, die nur die zulässigen Werte für die definierten Tag-Schlüssel definiert.

Nächster Schritt: Werte definieren

Angenommen, Sie haben die vorherige Tag-Richtlinie an den Organisations-Root angehängt. Als Nächstes können Sie wie folgt eine Tag-Richtlinie erstellen und sie an ein Konto anfügen. In dieser werden zulässige Werte für die Tag-Schlüssel `CostCenter` und `Project` definiert.

Richtlinie B – Tag-Richtlinie für Konten

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Wenn Sie die Richtlinie A an den Organisations-Root und die Richtlinie B an ein Konto anfügen, werden beide Richtlinien miteinander kombiniert, sodass sich die folgende effektive Tag-Richtlinie für das Konto ergibt:

Richtlinie A + Richtlinie B = effektive Tag-Richtlinie für Konto

```
{
    "tags": {
```

```
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Weitere Informationen zur Vererbung von Richtlinien sowie Beispiele für die Funktionsweise der Vererbungsoperatoren und für effektive Tag-Richtlinien finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

Beispiel 2: Verwendung eines Tag-Schlüssels verhindern

Um zu verhindern, dass ein Tag-Schlüssel verwendet wird, können Sie einer Organisations-Entität eine Tag-Richtlinie wie die folgende zuordnen.

In dieser Beispielrichtlinie wird angegeben, dass für den `Color`-Tag-Schlüssel keine Werte akzeptabel sind. Sie gibt auch an, dass in untergeordneten Tag-Richtlinien keine Operatoren zulässig sind. Daher werden alle `Color`-Tags für Ressourcen in betroffenen Konten als nicht konform angesehen. Jedoch wird durch die Option `enforced_for` wirksam verhindert, dass betroffene Konten nur Amazon-DynamoDB-Tabellen mit dem `Color`-Tag versehen.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
```

```
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Unterstützte Regionen

Tag-Richtlinienfunktionen sind in den folgenden Regionen verfügbar:

Name der Region	Regionsparameter
Region USA Ost (Nord-Virginia)[1]	**us-east-1**
Region USA Ost (Ohio)	us-east-2
Region US West (N. California)	us-west-1
Region USA West (Oregon)	us-west-2
Region[2] Afrika (Kapstadt)	af-south-1
Region Asien-Pazifik (Hongkong)[2]	ap-east-1
Region Asien-Pazifik (Mumbai)	ap-south-1
Asien-Pazifik (Hyderabad)2	ap-south-2
Region Asien-Pazifik (Tokio)	ap-northeast-1
Asia Pacific (Seoul) Region	ap-northeast-2
Region Asien-Pazifik (Osaka)	ap-northeast-3

Name der Region	Regionsparameter
Region Asien-Pazifik (Singapur)	`ap-southeast-1`
Region Asien-Pazifik (Sydney)	`ap-southeast-2`
Region2 Asien-Pazifik (Jakarta)	`ap-southeast-3`
Asien-Pazifik (Melbourne)2	`ap-southeast-4`
Kanada West (Calgary)2	`ca-west-1`
Region Kanada (Zentral)	`ca-central-1`
Region Europa (Frankfurt)	`eu-central-1`
Region2 Europa (Zürich)	`eu-central-2`
Region² Europa (Mailand)	`eu-south-1`
Europa (Spanien)2	`eu-south-2`
Region Europa (Irland)	`eu-west-1`
Europe (London) Region	`eu-west-2`
Region Europa (Paris)	`eu-west-3`
Region Europa (Stockholm)	`eu-north-1`
Region2 Naher Osten (VAE)	`me-central-1`
Region² Naher Osten (Bahrain)	`me-south-1`
Region Südamerika (São Paulo)	`sa-east-1`
Israel (Tel Aviv)2	`il-central-1`

[1]Sie müssen die **`us-east-1`**-Region angeben, wenn Sie die folgenden Organizations-Operationen aufrufen:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Alle anderen Operationen im Organisationsstamm, z. B. ListRoots.

Sie müssen auch die **`us-east-1`** Region angeben, wenn Sie die folgenden Ressourcengruppen-Tagging-API-Vorgänge aufrufen, die Bestandteil der Tag-Richtlinienfunktion sind:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Um die unternehmensweite Einhaltung von Tag-Richtlinien zu bewerten, müssen Sie zum Speichern von Berichten zudem Zugriff auf einen Amazon-S3-Bucket in der Region USA Ost (Nord-Virginia) haben. Weitere Informationen finden Sie unter Amazon S3-Bucket-Richtlinie für die Berichtsspeicherung im Benutzerhandbuch zum Markieren von - AWS Ressourcen.

²Diese Regionen müssen manuell aktiviert werden. Weitere Informationen zum Aktivieren und Deaktivieren von finden Sie unter Angeben AWS-Regionen, welche Ihr Konto verwenden kann im AWS Referenzhandbuch zur Kontoverwaltung. AWS-Regionen In diesen Regionen ist die Konsole für Resource Groups nicht verfügbar.

Service-Kontrollrichtlinien (SCPs)

Service-Kontrollrichtlinien (Service Control Policies, SCPs) sind eine Art von Organisationsrichtlinien, die Sie zum Verwalten von Berechtigungen in Ihrer Organisation verwenden können. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen für die IAM-Benutzer und IAM-Rollen in Ihrer Organisation. Mithilfe von SCPs können Sie sicherstellen, dass Ihre Konten innerhalb der Zugriffssteuerungsrichtlinien Ihrer Organisation bleiben. SCPs stehen nur in Organisationen zur Verfügung, in der alle Features aktiviert sind. Service-Kontrollrichtlinien sind nicht verfügbar, wenn

in einer Organisation nur Features für die konsolidierte Abrechnung aktiviert sind. Anleitungen zum Aktivieren von SCPs finden Sie unter Aktivieren und Deaktivieren von Richtlinientypen.

SCPs gewähren den IAM-Benutzern und IAM-Rollen in Ihrer Organisation keine Berechtigungen. Von einem SCP werden keine Berechtigungen erteilt. Ein SCP definiert für die Aktionen, die die IAM-Benutzer und IAM-Rollen in Ihrer Organisation ausführen können, eine Berechtigungsleitplanke oder legt Grenzwerte fest. Um Berechtigungen zu gewähren, muss der Administrator Richtlinien zur Zugriffskontrolle anhängen, z. B. identitätsbasierte Richtlinien, die IAM-Benutzern und IAM-Rollen zugewiesen sind, und ressourcenbasierte Richtlinien, die den Ressourcen in Ihren Konten zugewiesen sind. Die effektiven Berechtigungen stellen die logische Schnittstelle zwischen den vom SCP erlaubten Rechten und den Anforderungen der identitäts- und ressourcenbasierten Richtlinien dar.

> **Important**
>
> SCPs haben keine Auswirkungen auf Benutzer oder Rollen im Verwaltungskonto. Sie wirken sich nur auf die Mitgliedskonten Ihrer Organisation aus.

Themen auf dieser Seite

- Testen der Auswirkungen von SCPs
- Maximalgröße von SCPs
- Anfügen von SCPs an verschiedene Ebenen in der Organisation
- SCP-Auswirkungen auf Berechtigungen
- Verwenden von Zugriffsdaten zur Verbesserung von SCPs
- Aufgaben und Einheiten, die nicht durch SCPs eingeschränkt sind
- So erstellen, aktualisieren und löschen Sie Service-Kontrollrichtlinien
- Anfügen und Trennen von Service-Kontrollrichtlinien
- SCP-Bewertung
- SCP-Syntax
- Beispiele für Service-Kontrollrichtlinie

Testen der Auswirkungen von SCPs

AWS empfiehlt dringend, SCPs nicht an das Stammverzeichnis Ihrer Organisation anzuhängen, ohne die Auswirkungen der Richtlinie auf Konten gründlich zu testen. Erstellen Sie stattdessen eine Organisationseinheit, in die Sie Ihre Konten einzeln oder in geringer Anzahl verschieben können. So stellen Sie sicher, dass kein Benutzer versehentlich von wichtigen Services ausgesperrt wird. Ob ein Service von einem Konto verwendet wird, können Sie herausfinden, indem Sie sich die Daten zum letzten Servicezugriff in IAM ansehen. Eine andere Möglichkeit besteht darin, AWS CloudTrail die Nutzung von Diensten auf API-Ebene zu protokollieren.

> **Note**
>
> Sie sollten die vollständige AWSAccess Richtlinie nur entfernen, wenn Sie sie ändern oder durch eine separate Richtlinie mit zulässigen Aktionen ersetzen. Andernfalls schlagen alle AWS Aktionen von Mitgliedskonten fehl.

Maximalgröße von SCPs

Alle Zeichen in Ihrer SCP werden auf deren Maximalgröße angerechnet. In den Beispiele in diesem Handbuch sind die dargestellten Service-Kontrollrichtlinien mit zusätzlichen Leerzeichen formatiert, um die Lesbarkeit zu verbessern. Um Platz zu sparen, wenn sich die Größe Ihrer Richtlinie der Maximalgröße nähert, können Sie aber alle Leerraumzeichen, wie z. B. Leerzeichen und Zeilenumbrüche, außerhalb von Anführungszeichen löschen.

> **Tip**
>
> Verwenden Sie den visuellen Editor zum Erstellen Ihrer SCP. Hier werden zusätzliche Leerzeichen automatisch entfernt.

Anfügen von SCPs an verschiedene Ebenen in der Organisation

Eine detaillierte Erklärung der Funktionsweise der SCP-Vererbung finden Sie unter SCP-Bewertung.

SCP-Auswirkungen auf Berechtigungen

SCPs ähneln AWS Identity and Access Management (IAM-) Berechtigungsrichtlinien und verwenden fast dieselbe Syntax. Allerdings gewährt eine SCP nie Berechtigungen. Stattdessen sind SCPs

JSON-Richtlinien, die die maximalen Berechtigungen für die IAM-Benutzer und IAM-Rollen in Ihrer Organisation festlegen. Weitere Informationen finden Sie unter Auswertungslogik für Richtlinien im IAM-Benutzerhandbuch.

- SCPs betreffen nur IAM-Benutzer und -Rollen, die von Konten verwaltet werden, die zu der Organisation gehören. SCPs wirken sich nicht direkt auf ressourcenbasierte Richtlinien aus. Sie haben auch keine Auswirkungen auf Benutzer oder Rollen von Konten außerhalb der Organisation. Nehmen wir als Beispiel einen Amazon-S3-Bucket, der Konto A in einer Organisation gehört. Die Bucket-Richtlinie (eine ressourcenbasierte Richtlinie) gewährt Zugriff auf Benutzer von Konto B außerhalb der Organisation. Konto A ist eine Service-Kontrollrichtlinie zugeordnet. Diese SCP gilt nicht für externe Benutzer in Konto B. Der SCP gilt nur für Benutzer, die von Konto A in der Organisation verwaltet werden.
- Ein SCP beschränkt die Berechtigungen für IAM-Benutzer und -Rollen in Mitgliedskonten, einschließlich des Stammverzeichnisses des Mitgliedskonten. Jedes Konto weist nur die Berechtigungen auf, die ihm durch jedes einzelne übergeordnete Element gewährt wird. Wenn eine Berechtigung auf einer Ebene oberhalb des Kontos gesperrt ist, entweder stillschweigend (d. h., sie ist nicht in der Richtlinienanweisung `Allow` enthalten) oder explizit (d. h., sie ist in der Richtlinienanweisung `Deny` enthalten), kann ein Benutzer oder eine Rolle im betreffenden Konto diese Berechtigung nicht verwenden, auch wenn der Administrator des Kontos die IAM-Richtlinie `AdministratorAccess` mit */*-Berechtigungen an diesen Benutzer anhängt.
- SCPs wirken sich nur auf Mitglieds-Konten in der Organisation aus. Sie haben keine Auswirkungen auf Benutzer oder Rollen im Verwaltungskonto.
- Benutzer und Rollen müssen trotzdem mit Berechtigungen mit entsprechenden IAM-Berechtigungsrichtlinien ausgestattet werden. Ein Benutzer ohne IAM-Berechtigungsrichtlinien hat keinen Zugang, auch wenn die geltenden SCPs den Zugriff auf alle Services und Aktionen ermöglichen.
- Wenn einem Benutzer oder einer Rolle eine IAM-Berechtigungsrichtlinie zugeordnet wurde, die zum Zugriff auf eine Aktion berechtigt, welche auch mit den geltenden Service-Kontrollrichtlinien ausführbar wäre, darf der Benutzer oder die Rolle diese Aktion durchführen.
- Wenn einem Benutzer oder einer Rolle eine IAM-Berechtigungsrichtlinie zugeordnet wurde, die zum Zugriff auf eine Aktion berechtigt, welche gemäß den geltenden Service-Kontrollrichtlinien entweder unzulässig ist oder explizit verweigert wird, darf der Benutzer oder die Rolle diese Aktion nicht durchführen.
- Service-Kontrollrichtlinien wirken sich auf alle Benutzer und Rollen in angefügten Konten aus, einschließlich des Root-Benutzers. Die einzigen Ausnahmen sind die unter Aufgaben und Einheiten, die nicht durch SCPs eingeschränkt sind beschriebenen.

- SCPs haben keinen Einfluss auf eine servicegebundene Rolle. Mit Diensten verknüpfte Rollen ermöglichen die Integration anderer AWS Dienste in SCPs AWS Organizations und können nicht durch SCPs eingeschränkt werden.
- Wenn Sie den SCP-Richtlinientyp in einem Stamm deaktivieren, werden alle SCPs automatisch von allen AWS Organizations Entitäten in diesem Stamm getrennt. AWS Organizations Entitäten umfassen Organisationseinheiten, Organisationen und Konten. Bei einer erneuten Aktivierung der Service-Kontrollrichtlinien in einem Root-Benutzer wird für alle Entitäten lediglich die `FullAWSAccess`-Standardrichtlinie automatisch wiedergeherstellt. Alle Zuweisungen von SCPs für AWS Organizations -Entitäten von vor der Deaktivierung der SCPs gehen verloren und werden nicht automatisch wiederhergestellt. Die erneute Zuweisung muss manuell erfolgen.
- Wenn sowohl eine Berechtigungsgrenze (eine erweiterte IAM-Feature) als auch eine SCP vorhanden sind, müssen die Grenze, die SCP und die identitätsbasierte Richtlinie die Aktion zulassen.

Verwenden von Zugriffsdaten zur Verbesserung von SCPs

Wenn Sie mit den Anmeldeinformationen für das Verwaltungskonto angemeldet sind, können Sie im AWS OrganizationsBereich der IAM-Konsole die Daten anzeigen, auf die zuletzt zugegriffen wurde, für eine AWS Organizations Entität oder Richtlinie. Sie können auch die AWS Command Line Interface (AWS CLI) oder die AWS API in IAM verwenden, um die Daten des Dienstes abzurufen, auf den zuletzt zugegriffen wurde. Diese Daten enthalten Informationen darüber, auf welche zugelassenen Dienste die IAM-Benutzer und -Rollen in einem AWS Organizations Konto zuletzt zugegriffen haben und wann. Mit diesen Informationen können Sie ungenutzte Berechtigungen identifizieren, sodass Sie die SCPs besser an die Regel der geringsten Rechte anpassen können.

Möglicherweise haben Sie eine Sperrliste (SCP), die den Zugriff auf drei Dienste verbietet. AWS Alle Services, die nicht in der SCP-Anweisung `Deny` aufgeführt sind, sind zulässig. Die Daten des Dienstes, auf die in IAM zuletzt zugegriffen wurde, geben an, welche AWS Dienste vom SCP zugelassen, aber nie verwendet werden. Mit diesen Informationen können Sie die SCP so aktualisieren, dass sie den Zugriff auf nicht benötigte Services verweigert.

Weitere Informationen finden Sie unter folgenden Themen im IAM-Benutzerhandbuch:

- Anzeigen der Daten zum letzten Zugriff auf den Service für Organisationen
- Verwenden von Daten zum Optimieren von Berechtigungen für eine Organisationseinheit

Aufgaben und Einheiten, die nicht durch SCPs eingeschränkt sind

Sie können SCPs nicht verwenden, um die folgenden Aufgaben einzuschränken:

- Jede Aktion, die vom Verwaltungskonto ausgeführt wird
- Jede Aktion, die unter Verwendung von Berechtigungen ausgeführt wird, die mit einer servicegebundenen Rolle verknüpft sind
- Registrieren für den Enterprise Support-Plan als Root-Benutzer
- Ändern Sie die AWS Support-Stufe als Root-Benutzer
- Stellen Sie Funktionen für vertrauenswürdige Unterzeichner für CloudFront private Inhalte bereit
- Konfigurieren von Reverse-DNS für einen Amazon-Lightsail-E-Mail-Server und einer Amazon-EC2-Instance als Stammbenutzer
- Aufgaben im AWS Zusammenhang mit einigen verwandten Diensten:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - Amazon Product Marketing API

So erstellen, aktualisieren und löschen Sie Service-Kontrollrichtlinien

Wenn Sie sich beim Verwaltungskonto Ihrer Organisation anmelden, können Sie Service-Kontrollrichtlinien (SCPs) erstellen und aktualisieren. Sie erstellen SCPs, indem Sie Anweisungen schreiben, die den Zugriff auf von Ihnen definierte Services und Aktionen verweigern oder zulassen.

Die Standardkonfiguration für die Arbeit mit SCPs besteht darin, eine „Blockliste“-Strategie zu verwenden, bei der alle Aktionen implizit erlaubt sind, mit Ausnahme der Aktionen, die Sie blockieren möchten, indem Sie Anweisungen erstellen, die den Zugriff verweigern. Bei Anweisungen zur Zugriffsverweigerung („Deny“) können Sie Ressourcen und Bedingungen angeben und das Element NotAction verwenden. Bei Anweisungen mit Zugriffserlaubnis ("Allow") können Sie nur Services und Aktionen angeben. Weitere Informationen zu Anweisungen, die den Zugriff verweigern und den Zugriff erlauben, finden Sie unter SCP-Bewertung.

> **Tip**
>
> Sie können die Daten, auf die zuletzt zugegriffen wurde, in IAM verwenden, um Ihre SCPs zu aktualisieren, um den Zugriff auf die AWS-Services zu beschränken, die Sie benötigen.

Weitere Informationen finden Sie unter Anzeigen der Daten des letzten Zugriffs auf den Organizations-Service für Organizations im IAM-Benutzerhandbuch.

In diesem Thema:

- Nach der Aktivierung von Service-Kontrollrichtlinien für Ihre Organisation, können Sie eine Richtlinie erstellen.
- Wenn sich Ihre SCP-Anforderungen ändern, können Sie eine vorhandene Richtlinie aktualisieren.
- Wenn Sie eine Richtlinie nicht mehr benötigen, können Sie sie löschen, nachdem Sie sie von allen Organisationseinheiten (Organizational Units OUs) und Konten getrennt haben.

Erstellen einer SCP

Mindestberechtigungen

Für die Erstellung von SCPs benötigen Sie die Berechtigung zum Ausführen der folgenden Aktionen:

- `organizations:CreatePolicy`

AWS Management Console

So erstellen Sie eine Service-Kontrollrichtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien die Option Richtlinie erstellen aus.
3. Geben Sie auf der Seite Neue Service-Kontrollrichtlinie erstellen einen Richtliniennamen und eine optionale Richtlinienbeschreibung ein.
4. (Optional) Fügen Sie ein oder mehrere Tags hinzu, indem Sie Tag hinzufügen auswählen und dann einen Schlüssel und einen optionalen Wert eingeben. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einer Richtlinie bis zu 50 Tags hinzufügen. Weitere Informationen finden Sie unter Markieren von AWS Organizations-Ressourcen.

> **Note**
>
> In den meisten der folgenden Schritte besprechen wir die Verwendung der Steuerelemente auf der rechten Seite des JSON-Editors, um die Richtlinie Element für Element zu erstellen. Alternativ können Sie jederzeit einfach Text im JSON-Editor auf der linken Seite des Fensters eingeben. Sie können direkt eingeben oder kopieren und einfügen.

5. Bei der Erstellung der Richtlinie hängen Ihre nächsten Schritte davon ab, ob Sie eine Anweisung hinzufügen möchten, die den Zugriff verweigert oder zulässt. Weitere Informationen finden Sie unter SCP-Bewertung. Wenn Sie die `Deny`-Anweisungen benutzen, haben Sie zusätzliche Kontrolle, da Sie den Zugriff auf bestimmte Ressourcen beschränken, Bedingungen für die Gültigkeit von SCPs definieren und das Element NotAction verwenden können. Weitere Informationen zur Syntax finden Sie unter SCP-Syntax.

   So fügen Sie eine Anweisung hinzu, die den Zugriff verweigert:

   a. Wählen Sie im rechten Bereich Anweisung bearbeiten des Editors unter Aktionen hinzufügen einen AWS-Service aus.

      Wenn Sie rechts die Optionen auswählen, wird der JSON-Editor aktualisiert, um die entsprechende JSON-Richtlinie links anzuzeigen.

   b. Nachdem Sie einen Service ausgewählt haben, wird eine Liste mit den verfügbaren Aktionen für diesen Service geöffnet. Sie können Alle Aktionen auswählen oder eine oder mehrere einzelne Aktionen auswählen, die Sie verweigern möchten.

      Der JSON auf der linken Seite wird aktualisiert und enthält die ausgewählten Aktionen.

      > **Note**
      >
      > Wenn Sie eine einzelne Aktion auswählen und dann ebenfalls zurückgehen und auch Alle Aktionen auswählen, wird der erwartete Eintrag für *`servicename`*`/*` zum JSON hinzugefügt, aber die einzelnen Aktionen, die Sie zuvor ausgewählt haben, bleiben im JSON erhalten und werden nicht entfernt.

   c. Wenn Sie Aktionen von zusätzlichen Services hinzufügen möchten, können Sie oben im Feld Anweisung Alle Services auswählen und dann die vorherigen beiden Schritte nach Bedarf wiederholen.

d. Geben Sie die Ressourcen für die Anweisung an.

- Wählen Sie neben Eine Ressource hinzufügen die Option Hinzufügen aus.
- Wählen Sie im Dialogfeld Ressource hinzufügen den Service, dessen Ressourcen Sie steuern möchten, aus der Liste aus. Sie können nur unter den Services auswählen, die Sie im vorherigen Schritt ausgewählt haben.
- Wählen Sie unter Ressourcentyp den Ressourcentyp aus, den Sie steuern möchten.
- Vervollständigen Sie schließlich den Amazon-Ressourcennamen (ARN) im Ressourcen-ARN, um die spezifische Ressource zu identifizieren, auf die Sie den Zugriff steuern möchten. Sie müssen alle Platzhalter ersetzen, die von geschweiften Klammern `{}` umgeben sind. Sie können Platzhalter (`*`) angeben, wenn die ARN-Syntax dieses Ressourcentyps dies zulässt. Informationen darüber, wo Sie Platzhalter verwenden können, finden Sie in der Dokumentation zu einem bestimmten Ressourcentyp.
- Speichern Sie Ihre Ergänzung zur Richtlinie, indem Sie Ressource hinzufügen auswählen. Das `Resource`-Element im JSON spiegelt Ihre Ergänzungen oder Änderungen wider. Das Ressourcenelement ist erforderlich.

> **Tip**
>
> Wenn Sie alle Ressourcen für den ausgewählten Dienst angeben möchten, wählen Sie entweder die Option Alle Ressourcen in der Liste aus oder bearbeiten Sie die `Resource`-Anweisung direkt im JSON, um `"Resource":"*"` zu lesen.

e. (Optional) Um Bedingungen anzugeben, die die Gültigkeit einer Richtlinienanweisung einschränken, wählen Sie neben Bedingung hinzufügen die Option Hinzufügen aus.

- Bedingungsschlüssel – Aus der Liste können Sie einen beliebigen Bedingungsschlüssel auswählen, der für alle AWS-Services verfügbar ist (zum Beispiel, `aws:SourceIp`) oder einen leistungsspezifischen Schlüssel für nur einen der Services, die Sie für diese Anweisung ausgewählt haben.
- Qualifizierer – (Optional) Wenn Sie mehrere Werte für die Bedingung angeben (abhängig vom angegebenen Bedingungsschlüssel), können Sie einen Qualifizierer zum Testen von Anforderungen mit den Werten angeben.
  - Standard – Testet einen einzelnen Wert in der Anforderung gegen den Bedingungsschlüsselwert in der Richtlinie. Die Bedingung gibt „true“ zurück,

wenn der Wert in der Anfrage mit dem Wert in der Richtlinie übereinstimmt. Wenn die Richtlinie mehr als einen Wert angibt, werden sie als „oder“-Test behandelt, und die Bedingung gibt true zurück, wenn die Anforderungswerte mit einem der Richtlinienwerte übereinstimmen.

- Für jeden Wert in einer Anforderung – Wenn die Anforderung mehrere Werte haben kann, testet diese Option, ob mindestens einer der Anforderungswerte mit mindestens einem der Bedingungsschlüsselwerte in der Richtlinie übereinstimmt. Die Bedingung gibt "true" zurück, wenn ein Schlüsselwert in der Anforderung einem Bedingungswert in der Richtlinie entspricht. Bei keinem passenden Schlüssel oder einem leeren Datensatz gibt die Bedingung "false" zurück.
- Für alle Werte in einer Anforderung – Wenn die Anforderung mehrere Werte haben kann, testet diese Option, ob jeder Anforderungswert einem Bedingungsschlüsselwert in der Richtlinie entspricht. Die Bedingung gibt "true" zurück, wenn jeder Schlüsselwert in der Anforderung mindestens einem Wert in der Richtlinie entspricht. „true“ wird zudem zurückgegeben, wenn keine Schlüssel in der Anforderung vorhanden sind oder wenn die Schlüsselwerte zu einem Null-Dataset aufgelöst werden, z. B. einer leeren Zeichenfolge.

- Operator – Der Operator gibt die Art des durchzuführenden Vergleichs an. Die angezeigten Optionen hängen vom Datentyp des Bedingungsschlüssels ab. Mit dem globalen Bedingungsschlüssel `aws:CurrentTime` können Sie beispielsweise einen der Datumsvergleichsoperatoren oder `Null` auswählen, mit denen Sie testen können, ob der Wert in der Anforderung vorhanden ist.

  Sie können für jeden Bedingungsoperator, mit Ausnahme des Tests `Null`, die Option IfExists wählen.
- Wert – (Optional) Geben Sie einen oder mehrere Werte an, für die Sie die Anforderung testen möchten.

Klicken Sie auf Add condition.

Weitere Informationen zur Verwendung von Bedingungsschlüsseln finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

f. (Optional) Um das Element `NotAction` zu verwenden, um den Zugriff auf alle Aktionen mit Ausnahme der angegebenen zu verweigern, ersetzen Sie`Action` im linken Bereich direkt nach dem Element `"Effect": "Deny",` durch `NotAction`. Weitere

Informationen finden Sie unter IAM-JSON-Richtlinienelemente: NotAction im IAM-Benutzerhandbuch.

6. So fügen Sie eine Anweisung hinzu, die den Zugriff erlaubt:

   a. Ändern Sie im JSON-Editor links die Zeile `"Effect": "Deny"` in `"Effect": "Allow"`.

      Wenn Sie rechts die Optionen auswählen, wird der JSON-Editor aktualisiert, um die entsprechende JSON-Richtlinie links anzuzeigen.

   b. Nachdem Sie einen Service ausgewählt haben, wird eine Liste mit den verfügbaren Aktionen für diesen Service geöffnet. Sie können Alle Aktionen auswählen oder eine oder mehrere einzelne Aktionen auswählen, die Sie zulassen möchten.

      Der JSON auf der linken Seite wird aktualisiert und enthält die ausgewählten Aktionen.

      > **Note**
      >
      > Wenn Sie eine einzelne Aktion auswählen und dann ebenfalls zurückgehen und auch Alle Aktionen auswählen, wird der erwartete Eintrag für *`servicename`*`/*` zum JSON hinzugefügt, aber die einzelnen Aktionen, die Sie zuvor ausgewählt haben, bleiben im JSON erhalten und werden nicht entfernt.

   c. Wenn Sie Aktionen von zusätzlichen Services hinzufügen möchten, können Sie oben im Feld Anweisung Alle Services auswählen und dann die vorherigen beiden Schritte nach Bedarf wiederholen.

7. (Optional) Wenn Sie der Richtlinie eine weitere Anweisung hinzufügen möchten, wählen Sie Add statement (Anweisung hinzufügen) aus und verwenden Sie den visuellen Editor, um die nächste Anweisung zu erstellen.

8. Wenn Sie die gewünschten Anweisungen hinzugefügt haben, wählen Sie Create policy (Richtlinie erstellen) aus, um die fertige SCP zu speichern.

Die neue SCP wird in der Richtlinienliste der Organisation angezeigt. Sie können nun die SCP dem Stammverzeichnis, den Organisationseinheiten oder den Konten anfügen.

AWS CLI & AWS SDKs

So erstellen Sie eine Service-Kontrollrichtlinie

Sie können einen der folgenden Befehle verwenden, um eine Service-Kontrollrichtlinie zu erstellen:

- AWS CLI: create-policy

  Im folgenden Beispiel wird davon ausgegangen, dass Sie eine Datei mit dem Namen `Deny-IAM.json` mit dem darin enthaltenen JSON-Richtlinientext haben. Sie verwendet diese Datei, um eine neue Service-Kontrollrichtlinie zu erstellen.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWS-SDKs: CreatePolicy

> **Note**
>
> SCPs sind für das Verwaltungskonto und in einigen anderen Situationen nicht wirksam. Weitere Informationen finden Sie unter Aufgaben und Einheiten, die nicht durch SCPs eingeschränkt sind.

Aktualisieren einer SCP

Wenn Sie am Verwaltungskonto der Organisation angemeldet sind, können Sie eine Richtlinie umbenennen oder ändern. Das Ändern des Inhalts einer SCP wirkt sich unmittelbar auf alle Benutzer, Gruppen und Rollen in allen zugeordneten Konten aus.

> **Mindestberechtigungen**
>
> Für die Aktualisierung einer SCP benötigen Sie die Berechtigung zum Ausführen der folgenden Aktionen:
>
> - `organizations:UpdatePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")
> - `organizations:DescribePolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die den ARN für die angegebene Richtlinie enthält (oder "*")

AWS Management Console

So aktualisieren Sie eine Richtlinie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien den Namen der Richtlinie aus, die Sie aktualisieren möchten.
3. Wählen Sie auf der Detailseite der Richtlinie Richtlinie bearbeiten aus.
4. Nehmen Sie eine oder alle der folgenden Änderungen vor:
   - Sie können die Richtlinie umbenennen, indem Sie unter Richtlinienname einen neuen Namen eingeben.
   - Sie können die Beschreibung ändern, indem Sie einen neuen Text in der Richtlinienbeschreibung eingeben.
   - Sie können den Richtlinientext bearbeiten, indem Sie die Richtlinie im JSON-Format im linken Bereich bearbeiten. Alternativ können Sie im Editor auf der rechten Seite eine Anweisung auswählen und deren Elemente ebenfalls über die Steuerelemente ändern.

Weitere Einzelheiten zu den einzelnen Steuerelementen finden Sie im Abschnitt Erstellen einer SCP-Prozedur am Anfang dieses Themas.

5. Wenn Sie fertig sind, wählen Sie Save changes (Änderungen speichern) aus.

AWS CLI & AWS SDKs

So aktualisieren Sie eine Richtlinie

Sie können zum Aktualisieren einer Richtlinie einen der folgenden Befehle verwenden:

- AWS CLI: update-policy

Im folgenden Beispiel wird eine Richtlinie umbenannt.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

Im folgenden Beispiel wird die Beschreibung einer Service-Kontrollrichtlinie hinzugefügt oder geändert.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
```

```
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

Im folgenden Beispiel wird das Richtliniendokument des SCP geändert, indem eine Datei angegeben wird, die den neuen JSON-Richtlinientext enthält.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWS-SDKs: UpdatePolicy

Weitere Informationen

Weitere Informationen zum Erstellen von SCPs finden Sie in den folgenden Themen:

- Beispiele für Service-Kontrollrichtlinie
- SCP-Syntax

Bearbeiten von Tags, die an einen SCP angehängt sind

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie die Tags hinzufügen oder entfernen, die einer SCP zugeordnet sind. Weitere Informationen über das Markieren mit Tags finden Sie unter Markieren von AWS Organizations-Ressourcen.

Mindestberechtigungen

Um die an einer SCP in Ihrer AWS-Organisation angefügten Tags zu bearbeiten, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:DescribePolicy` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

So bearbeiten Sie die Tags, die einem SCP angehängt sind

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien den Namen der Richtlinie mit den Tags aus, die Sie bearbeiten möchten.
3. Wählen Sie auf der Seite mit den Richtliniendetails die Registerkarte Tags und dann Tags verwalten aus.
4. Nehmen Sie eine oder alle der folgenden Änderungen vor:

   - Ändern Sie den Wert eines Tags, indem Sie einen neuen Wert über dem alten Wert eingeben. Sie können den Tag-Schlüssel nicht direkt ändern. Um einen Schlüssel zu

ändern, müssen Sie das Tag mit dem alten Schlüssel löschen und dann ein Tag mit dem neuen Schlüssel hinzufügen.

- Entfernen Sie ein vorhandenes Tag, indem Sie Entfernen wählen.
- Fügen Sie ein neues Tag-Schlüssel-Wert-Paar hinzu. Wählen Sie Tag hinzufügen aus und geben Sie dann den neuen Schlüsselnamen und den optionalen Wert in die bereitgestellten Felder ein. Wenn Sie das Feld Wert leer lassen, ist der Wert eine leere Zeichenfolge; er ist nicht `null`.

5. Wenn Sie fertig sind, wählen Sie Save changes (Änderungen speichern) aus.

AWS CLI & AWS SDKs

So bearbeiten Sie die Tags, die einem SCP angehängt sind

Sie können einen der folgenden Befehle verwenden, um die einer SCP zugeordneten Tags zu bearbeiten:

- AWS CLI: tag-resource und untag-resource
- AWS-SDKs: TagResource und UntagResource

Löschen einer SCP

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine Richtlinie löschen, die Sie in Ihrer Organisation nicht mehr benötigen.

Hinweise

- Bevor Sie eine Richtlinie löschen können, müssen Sie sie zuerst von allen angehängten Elementen trennen.
- Sie können keine der von AWS verwalteten SCPs wie z. B. die SCP mit dem Namen `FullAWSAccess` löschen.

Mindestberechtigungen

Zum Löschen einer SCP benötigen Sie die Berechtigung zum Ausführen der folgenden Aktion:

- `organizations:DeletePolicy`

AWS Management Console

So löschen Sie ein SCP

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien den Namen der SCP aus, die Sie löschen möchten.
3. Sie müssen zuerst die Richtlinie, die Sie löschen möchten, von allen Stammverzeichnissen, Organisationseinheiten und Konten trennen. Wählen Sie die Registerkarte Ziele aus, wählen Sie das Optionsfeld neben jedem Stamm, jeder OU oder jedem Konto aus, die in der Liste Ziele angezeigt werden und wählen Sie dann Trennen. Wählen Sie im Bestätigungsdialogfeld Trennen aus. Wiederholen Sie dies, bis Sie alle Ziele entfernt haben.
4. Wählen Sie oben auf der Seite Löschen.
5. Geben Sie im Bestätigungsdialogfeld den Namen der Richtlinie ein und wählen Sie dann Löschen aus.

AWS CLI & AWS SDKs

So löschen Sie ein SCP

Sie können zum Löschen einer Richtlinie einen der folgenden Befehle verwenden:

- AWS CLI: delete-policy

  Das folgende Beispiel löscht die angegebene SCP.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-SDKs: DeletePolicy

Anfügen und Trennen von Service-Kontrollrichtlinien

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine zuvor erstellte Service-Kontrollrichtlinie (SCP) anfügen. Sie können eine SCP an den Organisationsstamm, eine Organisationseinheit (OU) oder direkt an ein Konto anfügen. Führen Sie zum Anfügen einer SCP folgende Schritte aus.

Mindestberechtigungen

Wenn Sie eine SCP an einen Stamm, eine Organisationseinheit oder ein Konto anfügen möchten, benötigen Sie die Berechtigung zum Ausführen der folgenden Aktion:

- `organizations:AttachPolicy` mit einem `Resource`-Element in derselben Richtlinienanweisung, die "*" oder den Amazon-Ressourcennamen (ARN) der angegebenen Richtlinie und den ARN des Stammverzeichnisses, der Organisationseinheit oder des Kontos, dem Sie die Richtlinie anfügen möchten, einschließt

AWS Management Console

Sie können eine SCP anfügen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, an das Sie die Richtlinie anfügen möchten, navigieren.

So fügen Sie eine SCP an, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Kontrollkästchen neben dem Stamm, der OU oder dem Konto, an das Sie einen SCP anhängen möchten und aktivieren Sie das Kontrollkästchen. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
3. Wählen Sie auf der Registerkarte Richtlinien im Eintrag für Service-Kontrollrichtlinien die Option Anfügen.
4. Suchen Sie die gewünschte Richtlinie und wählen Sie Richtlinie anfügen aus.

Die Liste der angehängten SCPs auf der Registerkarte Richtlinien wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam und wirkt sich auf die Berechtigungen von IAM-Benutzern und -Rollen im angehängten Konto oder allen Konten unter dem angehängten Stamm oder der angehängten OU aus.

So fügen Sie eine SCP durch Navigieren zur Richtlinie an

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien den Namen der Richtlinie aus, die Sie anfügen möchten.
3. Klicken Sie in der Registerkarte Ziele auf Anfügen.
4. Aktivieren Sie das Optionsfeld neben dem Stammverzeichnis, der Organisationseinheit oder dem Konto, an das bzw. die Sie die Richtlinie anfügen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.
5. Wählen Sie Richtlinie anfügen aus.

   Die Liste der angehängten SCPs auf der Registerkarte Ziele wird aktualisiert, um die neue Ergänzung aufzunehmen. Die Richtlinienänderung wird sofort wirksam und wirkt sich auf die Berechtigungen von IAM-Benutzern und -Rollen im angehängten Konto oder allen Konten unter dem angehängten Stamm oder der angehängten OU aus.

AWS CLI & AWS SDKs

So fügen Sie eine SCP an, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren

Sie können zum Anfügen einer SCP einen der folgenden Befehle verwenden:

- AWS CLI: attach-policy

  Im folgenden Beispiel wird eine SCP einer Organisationseinheit angefügt.

```
$ aws organizations attach-policy \
```

```
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS SDKs: AttachPolicy

Die Richtlinienänderung wird sofort wirksam und wirkt sich auf die Berechtigungen von IAM-Benutzern und -Rollen im angehängten Konto oder allen Konten unter dem angehängten Stamm oder der angehängten OU aus.

Trennen einer SCP vom Organisations-Root, von der Organisationseinheit oder von Konten

Wenn Sie am Verwaltungskonto Ihrer Organisation angemeldet sind, können Sie eine SCP vom Organisationsstamm, von der Organisationseinheit oder vom Konto trennen. Nachdem Sie ein SCP von einer Entität getrennt haben, gilt dieses SCP nicht mehr für IAM-Benutzer und IAM-Rollen, die von der jetzt getrennten Entität betroffen waren. Führen Sie zur Trennung einer SCP folgende Schritte aus.

> **Note**
>
> Sie können den letzten SCP nicht von einem Stamm, einer Organisationseinheit oder einem Konto trennen. An jeden Stamm, jede OU und jedes Konto muss zu jeder Zeit mindestens ein SCP angehängt sein.

> **Mindestberechtigungen**
>
> Wenn Sie eine SCP vom Stamm, von der Organisationseinheit oder vom Konto trennen möchten, benötigen Sie die Berechtigung zum Ausführen der folgenden Aktion:
>
> - `organizations:DetachPolicy`

AWS Management Console

Sie können eine SCP trennen, indem Sie entweder zur Richtlinie oder zum Stammverzeichnis, zur Organisationseinheit oder zum Konto, von dem Sie die Richtlinie trennen möchten, navigieren.

So trennen Sie eine SCP, indem Sie zum Stamm, zur Organisationseinheit oder zum Konto navigieren, an die sie angefügt ist

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zu dem Stamm, der OU oder dem Konto, von dem Sie eine Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option ▶), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden. Wählen Sie den Namen des Stamms, der Organisationseinheit oder des Kontos aus.
3. Wählen Sie auf der Registerkarte Richtlinien das Optionsfeld neben der SCP aus, die Sie trennen möchten und wählen Sie dann Trennen aus.
4. Wählen Sie im Bestätigungsdialogfeld Richtlinie trennen aus.

   Die Liste der angehängten SCPs wird aktualisiert. Die Richtlinien-Änderung, die sich durch das Trennen der Richtlinie ergibt, wird sofort wirksam. Das Trennen einer Service-Kontrollrichtlinie (SCP) wirkt sich beispielsweise unmittelbar auf die Berechtigungen von IAM-Benutzern und -Rollen in dem zuvor angefügten Konto bzw. in den Konten aus, die dem zuvor angefügten Organisations-Root oder der Organisationseinheit untergeordnet sind.

So trennen Sie eine SCP durch Navigieren zur Richtlinie

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite Service-Kontrollrichtlinien den Namen der Richtlinie aus, die Sie von einem Stamm, einer OU oder einem Konto trennen möchten.
3. Wählen Sie auf der Registerkarte Ziele das Optionsfeld neben dem Stamm, der OU oder dem Konto aus, von dem Sie die Richtlinie trennen möchten. Möglicherweise müssen Sie Organisationseinheiten erweitern (wählen Sie die Option

), um die gewünschte Organisationseinheit oder das gewünschte Konto zu finden.

4. Wählen Sie Detach (Trennen) aus.
5. Wählen Sie im Bestätigungsdialogfeld Trennen aus.

   Die Liste der angehängten SCPs wird aktualisiert. Die Richtlinien-Änderung, die sich durch das Trennen der Richtlinie ergibt, wird sofort wirksam. Das Trennen einer Service-Kontrollrichtlinie (SCP) wirkt sich beispielsweise unmittelbar auf die Berechtigungen von IAM-Benutzern und -Rollen in dem zuvor angefügten Konto bzw. in den Konten aus, die dem zuvor angefügten Organisations-Root oder der Organisationseinheit untergeordnet sind.

AWS CLI & AWS SDKs

So trennen Sie eine SCP von einem Stamm, einer Organisationseinheit oder einem Konto

Sie können zum Trennen einer SCP einen der folgenden Befehle verwenden:

- AWS CLI: detach-policy

  Im folgenden Beispiel wird der angegebene SCP von der angegebenen Organisationseinheit gelöst.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDKs: DetachPolicy

Die Richtlinienänderung wird sofort wirksam und wirkt sich auf die Berechtigungen von IAM-Benutzern und -Rollen im angehängten Konto oder allen Konten unter dem angehängten Stamm oder der angehängten OU aus

SCP-Bewertung

> **Note**
>
> Die Informationen in diesem Abschnitt gelten nicht für Verwaltungsrichtlinientypen, einschließlich Deaktivierungsrichtlinien für KI-Services, Backup-Richtlinien oder Tag-

Richtlinien. Weitere Informationen finden Sie unter Vererbung von Verwaltungsrichtlinien verstehen.

Da Sie in mehrere Service Control Policies (SCPs) auf unterschiedlichen Ebenen in AWS Organizations anfügen können, kann Ihnen das Verständnis, wie SCPs bewertet werden, helfen, SCPs zu erstellen, die zu den richtigen Ergebnissen führen.

Themen

- So funktionieren SCPs mit Allow
- So arbeiten SCPs mit Deny
- Strategie zur Verwendung von SCPs

So funktionieren SCPs mit Allow

Damit eine Berechtigung für ein bestimmtes Konto erteilt werden kann, muss auf jeder Ebene, vom Stamm bis hin zu jeder OU, im direkten Pfad zum Konto (einschließlich des Zielkontos selbst) eine ausdrückliche **`Allow`** Erklärung vorhanden sein. Aus diesem Grund wird bei der Aktivierung von SCPs eine AWS verwaltete SCP-Richtlinie AWS Organizations mit dem Namen FullAWSAccess angehängt, die alle Dienste und Aktionen zulässt. Wenn diese Richtlinie entfernt und auf keiner Organisationsebene ersetzt wird, werden alle OUs und Konten unter dieser Ebene daran gehindert, Maßnahmen zu ergreifen.

Sehen wir uns zum Beispiel das in den Abbildungen 1 und 2 gezeigte Szenario an. Damit eine Berechtigung oder ein Dienst für Konto B zugelassen werden kann, muss ein SCP, der die Erlaubnis oder den Dienst gewährt, an Root, die Produktionsorganisation und an Konto B selbst angehängt werden.

Die SCP-Evaluierung folgt einem standardmäßigen Verweigerungsmodell, was bedeutet, dass alle Berechtigungen, die in den SCPs nicht ausdrücklich erlaubt sind, verweigert werden. Wenn in den SCPs auf keiner der Ebenen wie Root, Production OU oder Account B eine Zulassungsanweisung vorhanden ist, wird der Zugriff verweigert.

Hinweise

- Eine `Allow`-Anweisung in einem SCP erlaubt es dem `Resource`-Element, nur einen `"*"`-Eintrag zu haben.

- Eine `Allow`-Anweisung in einer SCP kann überhaupt kein `Condition`-Element enthalten.

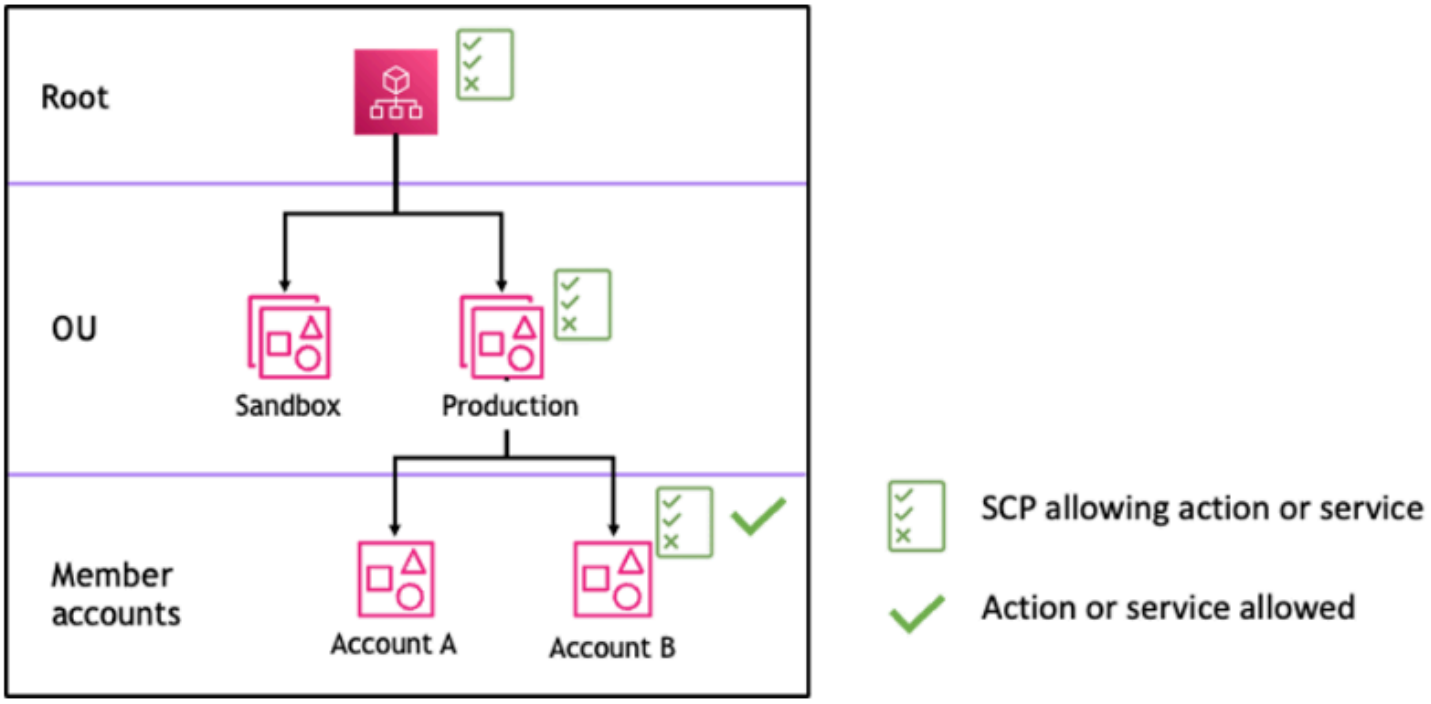


Abbildung 1: Beispiel für eine Organisationsstruktur mit einer *`Allow`* Erklärung, die an Root, Production OU und Account B angehängt ist

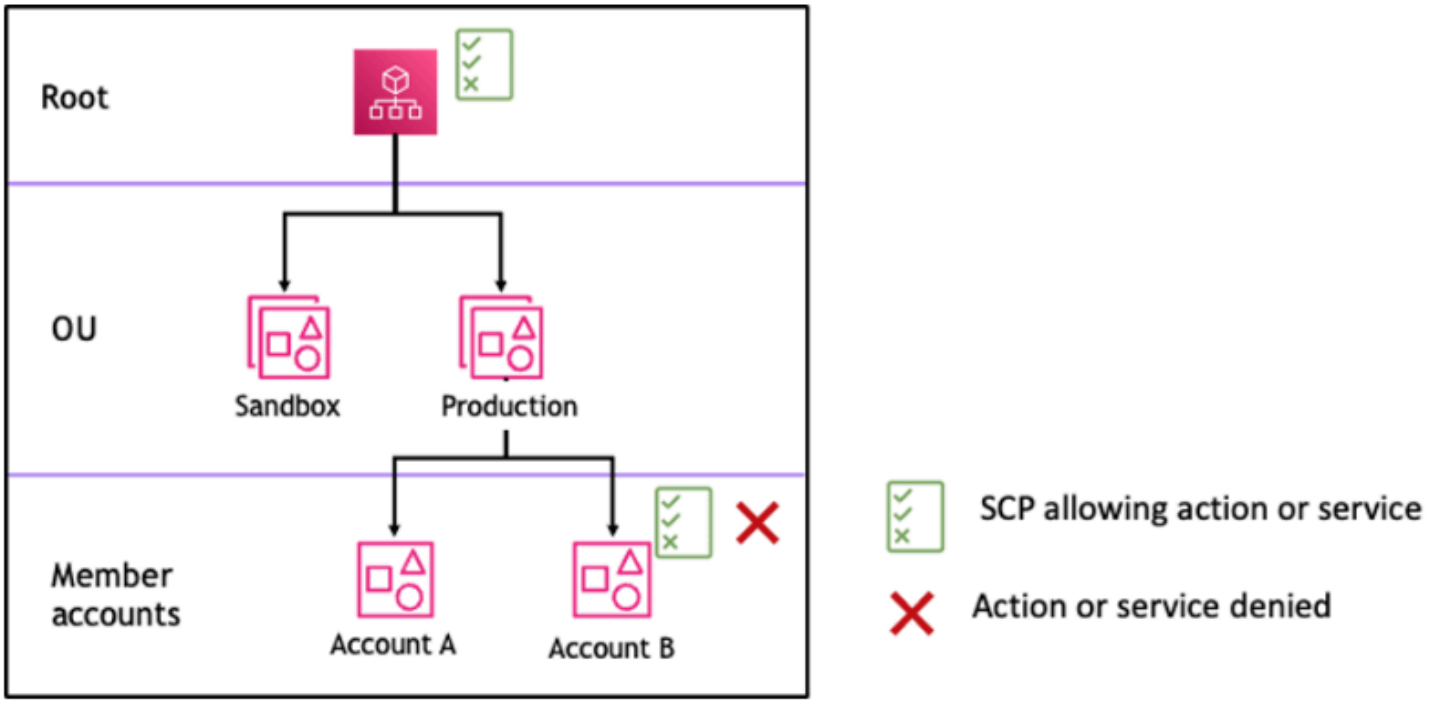


Abbildung 2: Beispiel für eine Organisationsstruktur mit fehlender *`Allow`* Erklärung bei Production OU und deren Auswirkung auf Account B

So arbeiten SCPs mit Deny

Damit eine Berechtigung für ein bestimmtes Konto verweigert werden kann, kann jeder SCP vom Stamm bis zu jeder OU im direkten Pfad zum Konto (einschließlich des Zielkontos selbst) diese Berechtigung verweigern.

Nehmen wir zum Beispiel an, der Produktionsorganisation ist ein SCP zugeordnet, für den eine ausdrückliche `Deny` Anweisung für einen bestimmten Dienst angegeben ist. Zufällig ist auch ein weiterer SCP an Root und Account B angehängt, der explizit den Zugriff auf denselben Dienst ermöglicht, wie in Abbildung 3 dargestellt. Infolgedessen wird sowohl Konto A als auch Konto B der Zugriff auf den Dienst verweigert, da eine Ablehnungsrichtlinie, die einer beliebigen Ebene in der Organisation zugewiesen ist, für alle untergeordneten Organisationseinheiten und Mitgliedskonten geprüft wird.

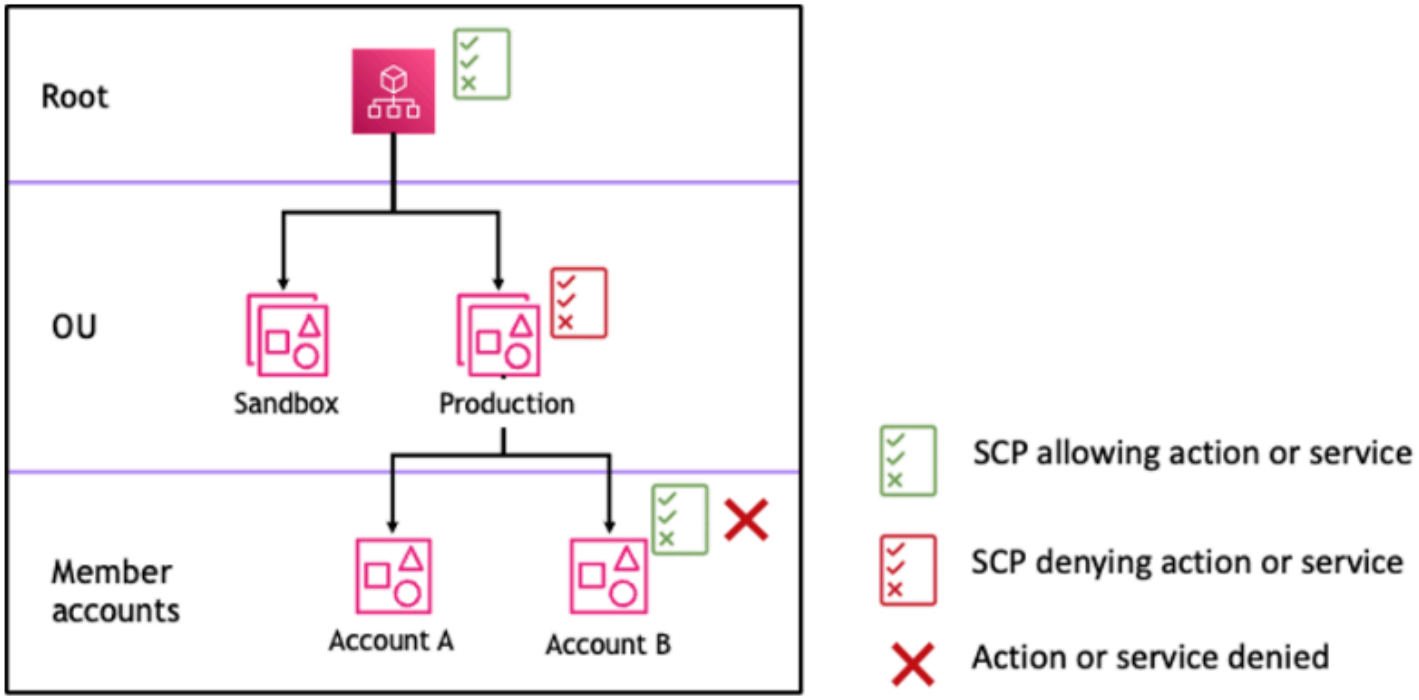


Abbildung 3: Beispiel für eine Organisationsstruktur mit einer *`Deny`*-Anweisung, die der Produktionsorganisation beigefügt ist, und deren Auswirkungen auf Konto B

Strategie zur Verwendung von SCPs

Beim Schreiben von SCPs können Sie eine Kombination aus `Allow` und `Deny`-Anweisungen verwenden, um beabsichtigte Aktionen und Dienste in Ihrer Organisation zu ermöglichen.

`Deny`Kontoauszüge sind ein wirksames Mittel zur Implementierung von Einschränkungen, die für einen größeren Teil Ihres Unternehmens oder Ihrer Organisationseinheiten gelten sollten, denn wenn sie auf Stamm- oder Organisationseinheitsebene angewendet werden, wirken sie sich auf alle Konten aus, denen sie unterstehen.

Sie können beispielsweise eine Richtlinie mithilfe von Verhindern, dass Mitgliedskonten die Organisation verlassen auf der Stammebene implementieren, die für alle Konten in der Organisation gilt. Ablehnungsaussagen unterstützen auch das Bedingungselement, das bei der Erstellung von Ausnahmen hilfreich sein kann.

> **Tip**
>
> Sie können die Daten, auf die zuletzt zugegriffen wurde, in IAM verwenden, um Ihre SCPs zu aktualisieren, um den Zugriff auf die AWS-Services zu beschränken, die Sie benötigen. Weitere Informationen finden Sie unter Anzeigen der Daten des letzten Zugriffs auf den Organizations-Service für Organizations im IAM-Benutzerhandbuch.

Um dies zu unterstützen, fügt AWS Organizations jedem Stamm, jeder OU und jedem Konto bei deren Erstellung eine von AWS verwaltete SCP mit dem Namen FullAWSAccess an. Diese Richtlinie lässt alle Services und Aktionen zu. Sie können FullAWSAccess eine Richtlinie ersetzen, die nur eine Reihe von Diensten zulässt, sodass neue AWS Dienste nur zulässig sind, wenn sie durch die Aktualisierung von SCPs ausdrücklich zugelassen werden. Wenn Ihre Organisation beispielsweise nur die Nutzung einer Teilmenge von Diensten in Ihrer Umgebung zulassen möchte, können Sie eine `Allow`-Anweisung verwenden, um nur bestimmte Dienste zuzulassen.

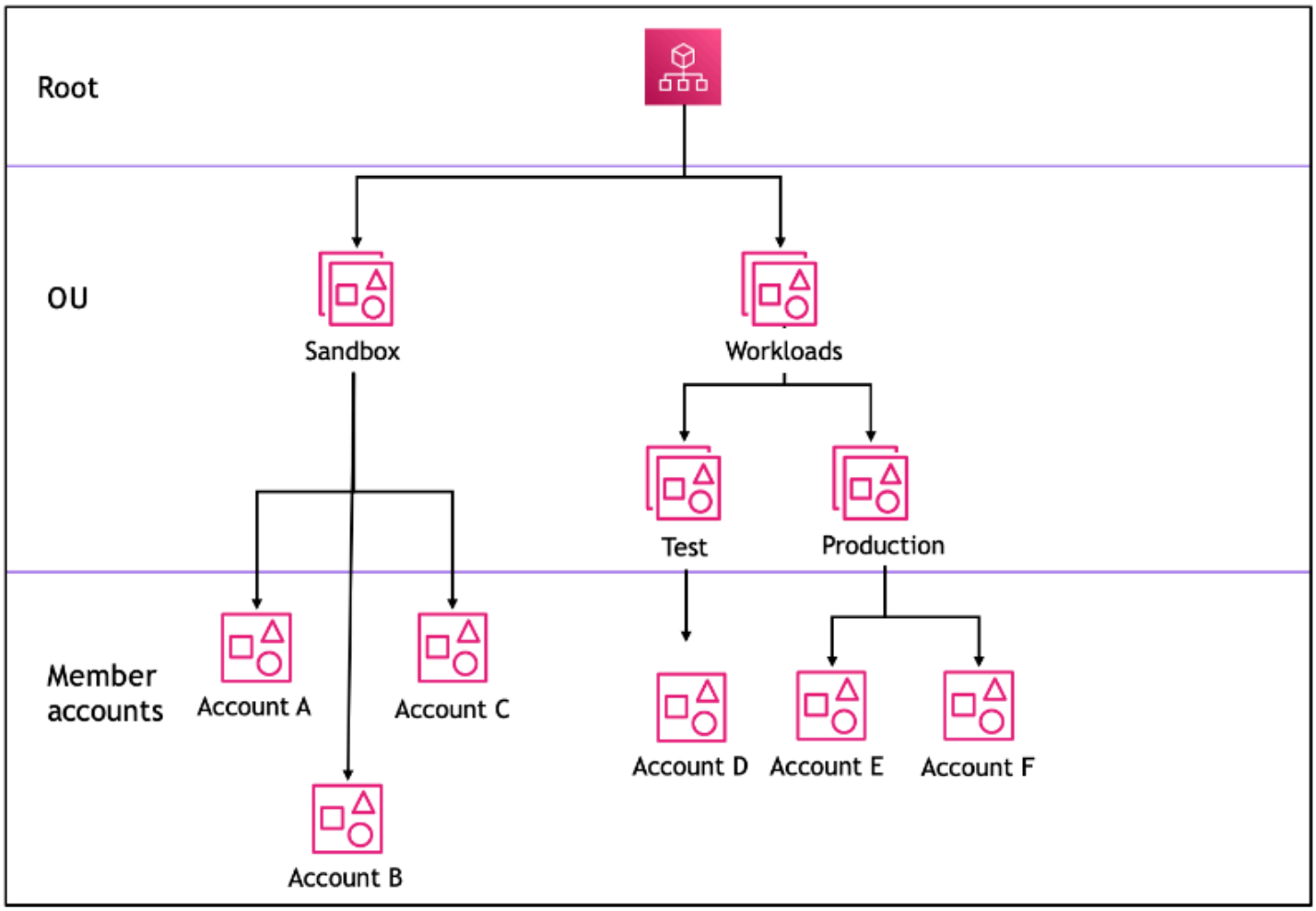
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Eine Richtlinie, die die beiden Aussagen kombiniert, könnte wie das folgende Beispiel aussehen. Sie verhindert, dass Mitgliedskonten die Organisation verlassen, und ermöglicht die Nutzung der gewünschten AWS-Dienste. Der Organisationsadministrator kann die FullAWSAccess-Richtlinie trennen und stattdessen diese Richtlinie anfügen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Betrachten Sie nun das folgende Beispiel für eine Organisationsstruktur, um zu verstehen, wie Sie mehrere SCPs auf verschiedenen Ebenen in einer Organisation einsetzen können.



Die folgende Tabelle zeigt die effektiven Richtlinien in der Organisationseinheit Sandbox.

Szenario	SCP bei Root	SCP bei Sandbox OU	SCP bei Konto A	Daraus resultierende Richtlinie für Konto A	Daraus resultierende Richtlinie für Konto B und Konto C
1	AWS Vollzugriff	AWS Vollzugriff + S3-Zugriff verweigern	AWS Vollzugriff + EC2-Zugriff verweigern	Kein S3, kein EC2-Zugriff	Kein S3-Zugriff
2	AWS Vollzugriff	Amazon Elastic	EC2-Zugriff zulassen	Erlaubt nur EC2-Zugriff	Erlaubt nur EC2-Zugriff

Szenario	SCP bei Root	SCP bei Sandbox OU	SCP bei Konto A	Daraus resultierende Richtlinie für Konto A	Daraus resultierende Richtlinie für Konto B und Konto C
		Compute Cloud (Amazon EC2)			
3	S3-Zugriff verweigern	S3-Zugriff zulassen	AWS Vollzugriff	Kein Zugriff auf Services	Kein Zugriff auf Services

Die folgende Tabelle zeigt die effektiven Richtlinien in der Organisationseinheit Workloads.

Szenario	SCP bei Root	SCP bei Workloads OU	SCP bei der Test OU	Daraus resultierende Richtlinie bei Konto D	Daraus resultierende Richtlinien bei Production OU, Account E und Account F
1	AWS Vollzugriff	AWS Vollzugriff	AWS Vollzugriff + EC2-Zugriff verweigern	Kein EC2-Zugriff	AWS Vollzugriff
2	AWS Vollzugriff	AWS Vollzugriff	EC2-Zugriff zulassen	EC2-Zugriff zulassen	AWS Vollzugriff
3	S3-Zugriff verweigern	AWS Vollzugriff	S3-Zugriff zulassen	Kein Zugriff auf Services	Kein Zugriff auf Services

SCP-Syntax

Service Control Policies (SCPs) verwenden eine ähnliche Syntax wie AWS Identity and Access Management (IAM) -Berechtigungsrichtlinien und ressourcenbasierte Richtlinien (wie Amazon S3 S3-Bucket-Richtlinien). Weitere Informationen über IAM-Richtlinien und ihre Syntax finden Sie in der Übersicht über IAM-Richtlinien im IAM-Benutzerhandbuch.

Eine Service-Kontrollrichtlinie ist eine Textdatei, die den Regeln der JSON-Struktur folgt. Sie verwendet die Elemente, die in diesem Thema beschrieben werden.

> **Note**
>
> Alle Zeichen in Ihrer SCP werden auf deren Maximalgröße angerechnet. In den Beispiele in diesem Handbuch sind die dargestellten Service-Kontrollrichtlinien mit zusätzlichen Leerzeichen formatiert, um die Lesbarkeit zu verbessern. Um Platz zu sparen, wenn sich die Größe Ihrer Richtlinie der Maximalgröße nähert, können Sie aber alle Leerraumzeichen, wie z. B. Leerzeichen und Zeilenumbrüche, außerhalb von Anführungszeichen löschen.

Allgemeine Informationen zu SCPs finden Sie unter Service-Kontrollrichtlinien (SCPs).

Übersicht über die Elemente

In der folgenden Tabelle finden Sie eine Übersicht der Richtlinienelemente, die Sie in SCPs verwenden können. Einige Richtlinienelemente sind nur in SCPs verfügbar, die Aktionen ablehnen. Die Spalte Unterstützte Auswirkungen enthält die Art von Auswirkungen, die Sie mit jedem Richtlinienelement in SCPs verwenden können.

Element	Zweck	Unterstützte Auswirkungen
Version	Gibt die Regeln für die Sprachsyntax an, die für die Verarbeitung der	`Allow`, `Deny`

Element	Zweck	Unterstützte Auswirkungen
	Richtlinie verwendet wird.	
Statement	Dient als Container für Richtlinienelemente. Sie können mehrere Anweisungen in SCPs verwenden.	`Allow`, `Deny`
Anweisungs-ID (SID)	(Optional) Stellt einen Anzeigenamen für die Anweisung bereit.	`Allow`, `Deny`

Element	Zweck	Unterstützte Auswirkungen
Effect (Effekt)	Definiert, ob die SCP-Anweisung den Zugriff auf die IAM-Benutzer und -Rollen in einem Konto erlaubt oder verweigert.	`Allow`, `Deny`
Action (Aktion)	Gibt den AWS Service und die Aktionen an, die der SCP zulässt oder verweigert.	`Allow`, `Deny`

Element	Zweck	Unterstützte Auswirkungen
NotAction	Gibt AWS Dienste und Aktionen an, die vom SCP ausgenommen sind. Wird anstelle des Elements `Action` verwendet.	`Deny`
Ressource	Gibt die AWS Ressourcen an, für die der SCP gilt.	`Deny`
Bedingung	Gibt die Bedingungen dafür an, wann die Anweisung wirksam ist.	`Deny`

In den folgenden Abschnitten finden Sie weitere Informationen und Beispiele dazu, wie Richtlinienelemente in SCPs verwendet werden.

`Version`-Element

Jede SCP muss ein `Version`-Element mit dem Wert `"2012-10-17"` enthalten. Dieser Wert entspricht der aktuellen Version der IAM-Berechtigungsrichtlinien.

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

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Version im IAM-Benutzerhandbuch.

`Statement`-Element

Eine SCP besteht aus einem oder mehreren `Statement`-Elementen. Es kann nur ein `Statement`-Schlüsselwort in einer Richtlinie enthalten sein, doch der Wert kann ein JSON-Array von Anweisungen sein (in eckigen Klammern []).

Das folgende Beispiel zeigt eine einzelne Anweisung, die aus einzelnen `Effect`-, `Action`- und `Resource`-Elementen besteht.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

Das folgende Beispiel enthält zwei Anweisungen als Array-Liste innerhalb eines `Statement`-Elements. Die erste Anweisung lässt sämtliche Aktionen zu, während die zweite alle EC2-Aktionen ablehnt. Das Ergebnis ist, dass ein Administrator im Konto alle Berechtigungen außer denen von Amazon Elastic Compute Cloud (Amazon EC2) delegieren kann.

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
```

```
    ]
```

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Anweisung im IAM-Benutzerhandbuch.

Element der Anweisungs-ID (`Sid`)

Die `Sid` (Anweisungs-ID) ist eine optionale ID, die Sie für die Richtlinie angeben können. Sie können jeder Anweisung in einem Statement-Array einen `Sid`-Wert zuweisen. Die folgende Beispiel-SCP zeigt eine beispielhafte `Sid`-Anweisung.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Id im IAM-Benutzerhandbuch.

`Effect`-Element

Jede Anweisung muss ein `Effect`-Element enthalten. Der Wert kann entweder `Allow` oder `Deny` sein. Dieser Wert wirkt sich auf alle in derselben Anweisung aufgeführten Aktionen aus.

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Effect im IAM-Benutzerhandbuch.

`"Effect": "Allow"`

Das folgende Beispiel zeigt eine SCP mit einer Anweisung, die ein `Effect`-Element mit dem Wert `Allow` enthält, der Kontobenutzern erlaubt, Aktionen für den Amazon-S3-Service auszuführen. Dieses Beispiel ist in einer Organisation nützlich, die die Zulassungslistenstrategie verwendet (wo die `FullAWSAccess`-Standardrichtlinien alle getrennt sind, sodass Berechtigungen standardmäßig implizit verweigert werden). Das Ergebnis ist, dass die Anweisung die Amazon-S3-Berechtigungen für alle angehängten Konten erlaubt:

```
{
    "Statement": {
        "Effect": "Allow",
```

```
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

Trotz der Verwendung desselben `Allow`-Wertschlüsselworts der Anweisung als IAM-Berechtigungsrichtlinie werden in einer Service-Kontrollrichtlinie (SCP) nicht tatsächlich Benutzerberechtigungen für irgendeine Aktion erteilt. Stattdessen dienen SCPs als Filter, die die maximalen Berechtigungen für die IAM-Benutzer und IAM-Rollen in einer Organisation angeben. Auch wenn im vorherigen Beispiel für einen Benutzer im Konto die verwaltete `AdministratorAccess`-Richtlinie angehängt wäre, beschränkt die verwaltete SCP alle Benutzer im Konto auf Amazon-S3-Aktionen.

`"Effect": "Deny"`

In einer Anweisung, in der das `Effect`-Element den Wert `Deny` hat, können Sie auch den Zugriff auf bestimmte Ressourcen beschränken oder Bedingungen dafür definieren, wann die SCPs wirksam sind.

Nachfolgend sehen Sie ein Beispiel für die Verwendung eines Bedingungsschlüssel in einer Zugriffsverweigerungsanweisung.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Diese Anweisung in einer SCP dient als Leitlinie, um zu verhindern, dass betroffene Konten Amazon-EC2-Instances starten, wenn für die Amazon-EC2-Instance nicht `t2.micro` festgelegt ist (wobei die SCP dem Konto selbst oder dem Organisationsstamm oder der Organisationseinheit zugeordnet ist, der bzw. die das Konto enthält). Auch wenn dem Konto eine IAM-Richtlinie, die diese Aktion zulässt, zugeordnet ist, wird dies von der Leitlinie der SCP verhindert.

Elemente **`Action`** und **`NotAction`**

Jede Anweisung muss eines der folgenden Elemente enthalten:

- In Anweisungen zum Zulassen oder Ablehnen des Zugriffs ein `Action`-Element.
- Nur in Zugriffsverweigerungsanweisungen (wobei der Wert des `Effect`-Elements `Deny` lautet) ein `Action` oder `NotAction`-Element.

Der Wert für das `NotAction` Element `Action` or ist eine Liste (ein JSON-Array) von Zeichenfolgen, die AWS Dienste und Aktionen identifizieren, die durch die Anweisung zugelassen oder verweigert werden.

Jede Zeichenfolge besteht aus der Abkürzung für den Service (z. B. "s3", "ec2", "iam" oder "organizations"), in Kleinbuchstaben, gefolgt von einem Doppelpunkt und einer Aktion aus dem entsprechenden Service. Bei den Aktionen (bzw. Nicht-Aktionen) muss auf Groß- und Kleinschreibung geachtet werden. Daher müssen sie wie in der Dokumentation des jeweiligen Service dargestellt eingegeben werden. In der Regel werden sie alle so eingegeben, dass alle Wörter mit einem Großbuchstaben beginnen und der Rest in Kleinbuchstaben folgt. Zum Beispiel: `"s3:ListAllMyBuckets"`.

Sie können auch Platzhalterzeichen wie Sternchen (*) oder ein Fragezeichen (?) in einem SCP verwenden:

- Sie können auch ein Sternchen als Platzhalter verwenden, der mit mehreren Aktionen übereinstimmt, die Teile eines Namens gemeinsam haben. Der Wert `"s3:*"` bezeichnet alle Aktionen im Amazon-S3-Service. Der Wert `"ec2:Describe*"` entspricht nur den EC2-Aktionen, die mit "Describe" beginnen.
- Verwenden Sie das Fragezeichen (?) als Platzhalter für die Übereinstimmung mit einem einzelnen Zeichen.

> **Note**
>
> In einem SCP können die Platzhalter (*) und (?) in einem `Action`- oder `NotAction`-Element nur von sich selbst oder am Ende einer Zeichenfolge verwendet werden. Er darf nicht am Anfang oder in der Mitte der Zeichenfolge stehen. Daher ist `"servicename:action*"` gültig, aber `"servicename:*action"` und `"servicename:some*action"` sind in SCPs ungültig.

Eine Liste aller Dienste und der Aktionen, die sie sowohl in AWS Organizations SCPs als auch in IAM-Berechtigungsrichtlinien unterstützen, finden Sie im IAM-Benutzerhandbuch unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste.

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Aktion und IAM-JSON-Richtlinienelemente: NotAction im IAM-Benutzerhandbuch.

Beispiel für das **`Action`**-Element

Das folgende Beispiel zeigt eine SCP mit einer Anweisung, die Kontoadministratoren erlaubt, Berechtigungen für EC2-Instances zu delegieren, zu starten, zu stoppen und zu beenden. Dies ist ein Beispiel für eine Whitelist. Es ist hilfreich, wenn die `Allow *`-Standardrichtlinien nicht zugewiesen sind, sodass Berechtigungen implizit automatisch abgelehnt werden. Wenn die `Allow *`-Standardrichtlinie nach wie vor an den Root-Benutzer, die Organisationseinheit oder das Konto angehängt ist, an die die folgende Richtlinie angehängt ist, ist die Richtlinie wirkungslos.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

Das folgende Beispiel zeigt, wie Sie Services, die Sie nicht in zugewiesenen Konten verwenden möchten, in eine Sperrliste aufnehmen können. Es wird vorausgesetzt, dass die standardmäßigen `"Allow *"`-SCPs nach wie vor an alle Organisationseinheiten und an den Root angefügt sind. Dieses Beispielrichtlinie verhindert, dass die Kontoadministratoren in angefügten Konten Berechtigungen für die Services IAM, Amazon EC2 und Amazon RDS delegieren können. Aktionen von anderen Services können delegiert werden, solange keine Richtlinie angefügt ist, die diese abgelehnt.

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

```
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Beispiel für das **`NotAction`**-Element

Das folgende Beispiel zeigt, wie Sie ein `NotAction` Element verwenden können, um AWS Dienste von der Wirkung der Richtlinie auszuschließen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
         }
       }
     }
   ]
}
```

Mit dieser Aussage können die betroffenen Konten nur Aktionen in den angegebenen Fällen ausführen, es sei denn AWS-Region, sie verwenden IAM-Aktionen.

`Resource`-Element

In Anweisungen, in denen das `Effect`-Element den Wert `Allow` hat, können Sie nur "*" im `Resource`-Element einer SCP angeben. Sie können keine einzelnen Amazon Resource Names (ARNs) angeben.

Sie können auch Platzhalterzeichen wie Sternchen (*) oder ein Fragezeichen (?) im Ressourcenelement verwenden:

- Sie können auch ein Sternchen als Platzhalter verwenden, der mit mehreren Aktionen übereinstimmt, die Teile eines Namens gemeinsam haben.

- Verwenden Sie das Fragezeichen (?) als Platzhalter für die Übereinstimmung mit einem einzelnen Zeichen.

In Anweisungen, in denen das `Effect`-Element den Wert `Deny` hat, können Sie einzelne ARNs angeben, wie im folgenden Beispiel gezeigt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

Dieser SCP schränkt IAM-Benutzer und -Rollen in betroffenen Konten ein, Änderungen an einer gemeinsamen administrativen IAM-Rolle vorzunehmen, die in allen Konten in Ihrer Organisation erstellt wurde.

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Resource im IAM-Benutzerhandbuch.

`Condition`-Element

Sie können ein `Condition`-Element in Zugriffsverweigerungsanweisungen in einer SCP angeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

Diese SCP verweigert den Zugriff auf alle Operationen außerhalb der Regionen `eu-central-1` und `eu-west-1`, mit Ausnahme von Aktionen in den aufgeführten Services.

Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Nicht unterstützte Elemente

Die folgenden Elemente werden in SCPs nicht unterstützt:

- `Principal`
- `NotPrincipal`
- `NotResource`

Beispiele für Service-Kontrollrichtlinie

Die in diesem Thema beschriebenen Beispiele zu Service-Kontrollrichtlinien (SCPs) dienen lediglich zu Informationszwecken.

Hinweise zur Verwendung dieser Beispiele

Bevor Sie diese Beispiel-SCPs in Ihrer Organisation verwenden, gehen Sie wie folgt vor:

- Überprüfen Sie die SCPs sorgfältig und passen Sie sie an Ihre individuellen Anforderungen an.
- Testen Sie die SCPs in Ihrer Umgebung gründlich mit den von Ihnen verwendeten AWS-Services.

  Die Beispielrichtlinien in diesem Abschnitt veranschaulichen die Implementierung und Verwendung von SCPs. Sie sind nicht als offizielle AWS-Empfehlungen oder bewährte Methoden zu interpretieren, die genau wie gezeigt umgesetzt werden müssen. Es liegt in Ihrer Verantwortung, alle verweigerungsbasierten Richtlinien sorgfältig auf ihre Eignung zu testen, um die geschäftlichen Anforderungen Ihrer Umgebung zu erfüllen. Zugriffsverweigerungsbasierte Service-Kontrollrichtlinien können Ihre Nutzung von AWS-Services unbeabsichtigt einschränken oder blockieren, es sei denn, Sie fügen der Richtlinie die erforderlichen Ausnahmen hinzu. Ein Beispiel für eine solche Ausnahme finden Sie im ersten Beispiel, das globale Services von den Regeln ausnimmt, die den Zugriff auf unerwünschte AWS-Regionen blockieren.
- Denken Sie daran, dass ein SCP jeden Benutzer und jede Rolle betrifft, einschließlich des Root-Benutzers in jedem Konto, mit dem es verbunden ist.

Tip

Sie können die Daten, auf die zuletzt zugegriffen wurde, in IAM verwenden, um Ihre SCPs zu aktualisieren, um den Zugriff auf die AWS-Services zu beschränken, die Sie benötigen. Weitere Informationen finden Sie unter Anzeigen der Daten des letzten Zugriffs auf den Organizations-Service für Organizations im IAM-Benutzerhandbuch.

Jede der folgenden Richtlinien ist ein Beispiel einer Strategie für Sperrlistenrichtlinien. Sperrlistenrichtlinien müssen zusammen mit anderen Richtlinien zugewiesen werden, die die

genehmigten Aktionen in den betroffenen Konten zulassen. Zum Beispiel: Die Standardrichtlinie `FullAWSAccess` erlaubt die Verwendung aller Services in einem Konto. Diese Richtlinie ist standardmäßig mit dem Root-Benutzer, allen Organisationseinheiten (OUs) und allen Konten verbunden. Sie gewährt nicht eigentlich die Berechtigungen, keine Service-Kontrollrichtlinie tut dies. Stattdessen können Administratoren in diesem Konto den Zugriff auf diese Aktionen delegieren, indem sie im Konto AWS Identity and Access Management-(IAM)-Standardberechtigungsrichtlinien für Benutzer, Rollen oder Gruppen zuweisen. Jede dieser Sperrlistenrichtlinien setzt dann jede Richtlinie durch Blockieren des Zugriffs auf die angegebenen Services oder Aktionen außer Kraft.

Beispiele

- Allgemeine Beispiele
  - Verweigern Sie den Zugriff auf AWS basierend auf der angeforderten AWS-Region
  - Vermeiden Sie, dass IAM-Benutzer und -Rollen bestimmte Änderungen vornehmen
  - Verhindern, dass IAM-Benutzer und -Rollen bestimmte Änderungen vornehmen, mit Ausnahme für eine angegebene Administratorrolle
  - MFA zum Ausführen einer API-Aktion erforderlich
  - Blockieren des Service-Zugriffsdatums für den Stammbenutzer
  - Verhindern, dass Mitgliedskonten die Organisation verlassen
- Beispiel-SCPs für Amazon CloudWatch
  - Verhindern, dass Benutzer CloudWatch deaktivieren oder dessen Konfiguration verändern
- Beispiel-SCPs für AWS Config
  - Verhindern, dass Benutzer AWS Config deaktivieren oder dessen Regeln verändern
- Beispiel-SCPs für Amazon Elastic Compute Cloud (Amazon EC2)
  - Erfordern, dass Amazon-EC2-Instances einen bestimmten Typ verwenden
  - Verhindern Sie das Starten von EC2-Instances ohne IMDSv2
  - Verhindern Sie die Deaktivierung der standardmäßigen Amazon-EBS-Verschlüsselung
- Beispiel-SCPs für Amazon GuardDuty
  - Verhindern, dass Benutzer GuardDuty deaktivieren oder dessen Konfiguration verändern
- Beispiel-SCPs für AWS Resource Access Manager
  - Verhindern einer externen Freigabe
  - Zulassen, dass bestimmte Konten nur bestimmte Ressourcentypen freigeben
  - Vermeiden Sie die Freigabe für Organisationen oder Organisationseinheiten (OUs)

- Freigabe nur für bestimmte IAM-Benutzer und -Rollen zulassen
- Exemplarische SCPs für den Amazon-Route-53-Application-Recovery-Controller
  - Verhindern, dass Benutzer Routing-Steuerungsstatuswerte des Route-53-ARC aktualisieren
- Beispiel-SCPs für Amazon S3
  - Verhindern Sie unverschlüsselte Objekt-Uploads von Amazon S3
- Beispiel für SCPs zum Markieren von Ressourcen
  - Benötigen Sie ein Tag für angegebene erstellte Ressourcen
  - Verhindern, dass Tags geändert werden, außer von autorisierten Prinzipalen
- Beispiel für SCPs für Amazon Virtual Private Cloud (Amazon VPC)
  - Verhindern, dass Benutzer Amazon-VPC-Flow-Protokolle löschen
  - Verhindern, dass ein VPC, der nicht bereits Internetzugang hat, einen solchen Zugang erhält

Allgemeine Beispiele

Verweigern Sie den Zugriff auf AWS basierend auf der angeforderten AWS-Region

Diese SCP lehnt den Zugriff auf alle Operationen außerhalb der angegebenen Regionen ab. Ersetzen Sie `eu-central-1` und `eu-west-1` durch das AWS-Regionen, das Sie verwenden möchten. Sie sieht Ausnahmen für Operationen in genehmigten globalen Services vor. Dieses Beispiel zeigt auch, wie Anforderungen von einer der zwei angegebenen Administratorrollen ausgeschlossen werden.

> **Note**
>
> Um die SCP zur Regions-Verweigerung mit AWS Control Tower zu verwenden, siehe Verweigern Sie den Zugriff auf AWS basierend auf der angeforderten AWS-Region.

Diese Richtlinie verwendet den `Deny`-Effekt, um den Zugriff auf alle Anforderungen für Operationen abzulehnen, die sich nicht in einer der beiden genehmigten Regionen (`eu-central-1` und `eu-west-1`) befinden. Mithilfe des Elements NotAction können Sie Services auflisten, deren Operationen (oder individuelle Operationen) von dieser Einschränkung ausgenommen sind. Da globale Services Endpunkte besitzen, die physisch in der Region `us-east-1` gehostet werden, müssen sie auf diese Weise ausgenommen werden. Wenn eine SCP auf diese Weise strukturiert ist, werden Anforderungen für globale Services in der Region `us-east-1` zugelassen, wenn der angeforderte

Service im Element `NotAction` enthalten ist. Alle anderen Anforderungen für Services in der Region `us-east-1` werden durch diese Beispielrichtlinie abgelehnt.

> **Note**
>
> Dieses Beispiel enthält möglicherweise nicht alle aktuellen globalen AWS-Services oder -Vorgänge. Ersetzen Sie die Liste der Services und Operationen durch die globalen Services, die von den Konten in Ihrer Organisation verwendet werden.
>
> > **Tipp**
> >
> > Sie können die letzten Servicedaten, auf die in der IAM-Konsole zugegriffen wurde, anzeigen, um die von Ihrer Organisation verwendeten globalen Services zu ermitteln. Auf der Registerkarte Access Advisor (Zugriffsberater) auf der Detailseite für IAM-Benutzer, -Gruppen oder -Rollen werden die AWS-Services angezeigt, die von dieser Entität verwendet wurden, sortiert nach dem letzten Zugriff.

> **Überlegungen**
>
> - AWS KMS und AWS Certificate Manager unterstützen regionale Endpunkte. Wenn Sie sie jedoch mit einem globalen Service wie Amazon CloudFront verwenden möchten, müssen Sie sie im folgenden Beispiel für SCP in die globale Serviceausschlussliste aufnehmen. Ein globaler Service wie Amazon CloudFront erfordert normalerweise Zugriff auf AWS KMS und ACM in derselben Region, die für einen globalen Service die Region USA Ost (Nord-Virginia) (`us-east-1`) ist.
> - AWS STS ist standardmäßig ein globaler Service und muss in die globale Serviceausschlussliste aufgenommen werden. Sie können AWS STS jedoch aktivieren, um Regionsendpunkte anstelle eines einzelnen globalen Endpunkts zu verwenden. Wenn Sie dies tun, können Sie STS aus der globalen Dienstausnahmeliste im folgenden Beispiel SCP entfernen. Weitere Informationen finden Sie unter Verwalten von AWS STS im AWS-Region.

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

```
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
```

```
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Vermeiden Sie, dass IAM-Benutzer und -Rollen bestimmte Änderungen vornehmen

Mit diesem SCP können IAM-Benutzer und -Rollen Änderungen an der angegebenen IAM-Rolle vornehmen, die Sie in allen Konten in Ihrer Organisation erstellt haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
```

```
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Verhindern, dass IAM-Benutzer und -Rollen bestimmte Änderungen vornehmen, mit Ausnahme für eine angegebene Administratorrolle

Diese SCP baut auf dem vorherigen Beispiel auf und enthält eine Ausnahme für Administratoren. Dies verhindert, dass IAM-Benutzer und -Rollen in betroffenen Konten Änderungen an einer gemeinsamen administrativen IAM-Rolle vornehmen, die in allen Konten in Ihrer Organisation erstellt wurde, mit Ausnahme von Administratoren, die eine bestimmte Rolle verwenden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
```

```
      }
    }
  ]
}
```

MFA zum Ausführen einer API-Aktion erforderlich

Verwenden Sie eine SCP wie die folgende, um zu verlangen, dass die Multi-Faktor-Authentifizierung (MFA) aktiviert ist, bevor ein IAM-Benutzer oder eine IAM-Rolle eine Aktion ausführen kann. In diesem Beispiel wird eine Amazon-EC2-Instance angehalten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Blockieren des Service-Zugriffsdatums für den Stammbenutzer

Die folgende Richtlinie schränkt den gesamten Zugriff auf die angegebenen Aktionen für den Stammbenutzer in einem Mitgliedskonto ein. Wenn Sie verhindern möchten, dass Ihre Konten auf bestimmte Art und Weise Root-Anmeldeinformationen verwenden, fügen Sie dieser Richtlinie Ihre eigenen Aktionen hinzu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
```

```
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Verhindern, dass Mitgliedskonten die Organisation verlassen

Die folgende Richtlinie blockiert die Verwendung der `LeaveOrganization`-API-Operation, sodass Administratoren von Mitgliedskonten ihre Konten nicht aus der Organisation entfernen können.

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

Beispiel-SCPs für Amazon CloudWatch

Beispiele in dieser Kategorie

- Verhindern, dass Benutzer CloudWatch deaktivieren oder dessen Konfiguration verändern

Verhindern, dass Benutzer CloudWatch deaktivieren oder dessen Konfiguration verändern

Ein untergeordneter CloudWatch-Operator muss Dashboards und Alarme überwachen. Der Operator darf jedoch nicht Dashboards oder Alarme löschen können, die Benutzer auf höherer Ebene eingerichtet haben. Diese Service-Kontrollrichtlinie verhindert, dass Benutzer oder Rollen in einem betroffenen Konto einen der CloudWatch-Befehle ausführen, durch den Ihre Dashboards oder Alarme gelöscht oder verändert werden könnten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

Beispiel-SCPs für AWS Config

Beispiele in dieser Kategorie

- Verhindern, dass Benutzer AWS Config deaktivieren oder dessen Regeln verändern

Verhindern, dass Benutzer AWS Config deaktivieren oder dessen Regeln verändern

Diese Service-Kontrollrichtlinie verhindert, dass Benutzer oder Rollen in einem betroffenen Konto AWS Config-Operationen ausführen, durch die AWS Config deaktiviert bzw. dessen Regeln oder Auslöser verändert werden könnten.

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

```
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Beispiel-SCPs für Amazon Elastic Compute Cloud (Amazon EC2)

Beispiele in dieser Kategorie

- Erfordern, dass Amazon-EC2-Instances einen bestimmten Typ verwenden
- Verhindern Sie das Starten von EC2-Instances ohne IMDSv2
- Verhindern Sie die Deaktivierung der standardmäßigen Amazon-EBS-Verschlüsselung

Erfordern, dass Amazon-EC2-Instances einen bestimmten Typ verwenden

Mit dieser SCP wird das Starten aller Instances abgelehnt, die nicht den Instance-Typ `t2.micro` verwenden.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
```

```
}
```

Verhindern Sie das Starten von EC2-Instances ohne IMDSv2

Die folgende Richtlinie hindert alle Benutzer daran, EC2-Instances ohne IMDSv2 zu starten.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

Die folgende Richtlinie hindert alle Benutzer daran, EC2-Instances ohne IMDSv2 zu starten, erlaubt jedoch bestimmten IAM-Identitäten, Instance-Metadatenoptionen zu ändern.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
```

```
      }
    }
  }
]
```

Verhindern Sie die Deaktivierung der standardmäßigen Amazon-EBS-Verschlüsselung

Die folgende Richtlinie hindert alle Benutzer daran, die standardmäßige Amazon-EBS-Verschlüsselung zu deaktivieren.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Beispiel-SCPs für Amazon GuardDuty

Beispiele in dieser Kategorie

- Verhindern, dass Benutzer GuardDuty deaktivieren oder dessen Konfiguration verändern

Verhindern, dass Benutzer GuardDuty deaktivieren oder dessen Konfiguration verändern

Diese Service-Kontrollrichtlinie verhindert, dass Benutzer oder Rollen in einem betroffenen Konto GuardDuty deaktivieren oder die Konfiguration ändern, entweder direkt als Befehl oder über die Konsole. Dies ermöglicht effektiv schreibgeschützten Zugriff auf die Informationen und Ressourcen von GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
```

```
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel-SCPs für AWS Resource Access Manager

Beispiele in dieser Kategorie

- Verhindern einer externen Freigabe
- Zulassen, dass bestimmte Konten nur bestimmte Ressourcentypen freigeben
- Vermeiden Sie die Freigabe für Organisationen oder Organisationseinheiten (OUs)
- Freigabe nur für bestimmte IAM-Benutzer und -Rollen zulassen

Verhindern einer externen Freigabe

Das folgende Beispiel von SCP verhindert, dass Benutzer Ressourcenfreigaben erstellen, die die Freigabe für IAM-Benutzer und -Rollen ermöglichen, die nicht Teil der Organisation sind.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Zulassen, dass bestimmte Konten nur bestimmte Ressourcentypen freigeben

Das folgende SCP erlaubt Konten 111111111111 und 222222222222, Ressourcenfreigaben zu erstellen, die Präfixlisten freigeben, und Präfixlisten vorhandenen Ressourcenfreigaben zuzuordnen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
```

```
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Vermeiden Sie die Freigabe für Organisationen oder Organisationseinheiten (OUs)

Die folgende SCP verhindert, dass Benutzer Ressourcenfreigaben erstellen, die Ressourcen mit einerAWS-Organisation oder Organisationseinheiten teilen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Freigabe nur für bestimmte IAM-Benutzer und -Rollen zulassen

In der folgenden Beispiel-SCP können Benutzer Ressourcen nur für Organisation `o-12345abcdef`, Organisationseinheit `ou-98765fedcba` und Konto `111111111111` freigeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

Exemplarische SCPs für den Amazon-Route-53-Application-Recovery-Controller

Beispiele in dieser Kategorie

- Verhindern, dass Benutzer Routing-Steuerungsstatuswerte des Route-53-ARC aktualisieren

Verhindern, dass Benutzer Routing-Steuerungsstatuswerte des Route-53-ARC aktualisieren

Ein Route-53-ARC-Operator auf niedrigerer Ebene muss Dashboards überwachen und Route-53-ARC-Informationen anzeigen können. Im Gegensatz zu einem erfahrenen Operator darf der Operator jedoch nicht in der Lage sein, Routing-Steuerungen zu aktualisieren, um ein Failover der Anwendung auf eine andere AWS-Region durchzuführen. Diese Service-Kontrollrichtlinie verhindert, dass Benutzer oder Rollen in einem betroffenen Konto Route-53-ARC-Vorgänge ausführen, die Route-53-ARC-Routingsteuerungen aktualisieren.

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

```
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Beispiel-SCPs für Amazon S3

Beispiele in dieser Kategorie

- Verhindern Sie unverschlüsselte Objekt-Uploads von Amazon S3

Verhindern Sie unverschlüsselte Objekt-Uploads von Amazon S3

Die folgende Richtlinie hindert alle Benutzer daran, unverschlüsselte Objekte in S3-Buckets hochzuladen.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

Die folgende Richtlinie hindert alle Benutzer daran, unverschlüsselte Objekte in S3-Buckets hochzuladen und erzwingt außerdem einen bestimmten Verschlüsselungstyp (entweder AES256 oder aws:kms) für den Objekt-Upload in ihren Buckets.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

Beispiel für SCPs zum Markieren von Ressourcen

Beispiele in dieser Kategorie

- Benötigen Sie ein Tag für angegebene erstellte Ressourcen
- Verhindern, dass Tags geändert werden, außer von autorisierten Prinzipalen

Benötigen Sie ein Tag für angegebene erstellte Ressourcen

Die folgende SCP verhindert, dass IAM-Benutzer und -Rollen in den betroffenen Konten bestimmte Ressourcentypen erstellen, wenn die Anforderung die angegebenen Tags nicht enthält.

Important

Denken Sie daran, verweigerungsbasierte Richtlinien mit den Services zu testen, die Sie in Ihrer Umgebung verwenden. Das folgende Beispiel ist ein einfacher Block zum Erstellen unmarkierter Geheimnisse oder zum Ausführen von nicht markierten Amazon-EC2-Instances und enthält keine Ausnahmen.
Die folgende Beispielrichtlinie ist wie beschrieben nicht mit AWS CloudFormation kompatibel, da dieser Service ein Geheimnis erstellt und es dann als zwei separate Schritte kennzeichnet. Diese Beispielrichtlinie blockiert AWS CloudFormation effektiv daran, ein Geheimnis als Teil eines Stacks zu erstellen, da eine solche Aktion, wenn auch kurz, zu einem Geheimnis führen würde, das nicht wie erforderlich gekennzeichnet ist.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
```

```
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    }
  ]
}
```

Eine Liste aller Services und Aktionen, die diese sowohl in AWS Organizations-SCPs als auch in IAM-Berechtigungsrichtlinien unterstützen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS-Services im IAM-Benutzerhandbuch.

Verhindern, dass Tags geändert werden, außer von autorisierten Prinzipalen

Der folgende SCP zeigt, wie eine Richtlinie nur autorisierte Prinzipale erlauben kann, die Tags zu ändern, die Ihren Ressourcen zugeordnet sind. Dies ist ein wichtiger Bestandteil der attributbasierten Zugriffskontrolle (Attribute-based Access Control, ABAC) als Teil Ihrer AWS-Cloud-Sicherheitsstrategie. Die Richtlinie ermöglicht es einem Aufrufer, die Tags nur auf den Ressourcen zu ändern, bei denen das Autorisierungs-Tag (in diesem Beispiel `access-project`) genau mit dem gleichen Autorisierungs-Tag übereinstimmt, der an den Benutzer oder die Rolle angehängt ist, die die Anforderung stellt. Die Richtlinie verhindert auch, dass der autorisierte Benutzer den Wert

des Tags ändert, der für die Autorisierung verwendet wird. Der aufrufende Prinzipal muss über das Autorisierungs-Tag verfügen, um Änderungen überhaupt vornehmen zu können.

Diese Richtlinie blockiert nur nicht autorisierte Benutzer daran, Tags zu ändern. Ein autorisierter Benutzer, der nicht durch diese Richtlinie blockiert wird, muss dennoch über eine separate IAM-Richtlinie verfügen, die die `Allow`-Berechtigung für die entsprechenden Tagging-APIs explizit erteilt. Wenn Ihr Benutzer beispielsweise eine Administratorrichtlinie mit `Allow */*` hat (alle Services und alle Operationen zulassen), führt die Kombination dazu, dass der Administratorbenutzer nur die Tags ändern darf, deren Autorisierungs-Tag-Wert mit dem angehängten Autorisierungs-Tag-Wert übereinstimmt an den Auftraggeber des Benutzers. Dies liegt daran, dass die explizite `Deny` in dieser Richtlinie die explizite `Allow` in der Administratorrichtlinie überschreibt.

> **Important**
>
> Dies ist keine vollständige Richtlinienlösung und sollte nicht wie hier gezeigt verwendet werden. Dieses Beispiel soll nur einen Teil einer ABAC-Strategie veranschaulichen und muss für Produktionsumgebungen angepasst und getestet werden.
> Die vollständige Richtlinie mit einer detaillierten Analyse ihrer Funktionsweise finden Sie unter Sichern von Ressourcen-Tags, die für die Autorisierung verwendet werden, mithilfe einer Service-Kontrollrichtlinie in AWS Organizations
> Denken Sie daran, verweigerungsbasierte Richtlinien mit den Services zu testen, die Sie in Ihrer Umgebung verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
```

```
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Beispiel für SCPs für Amazon Virtual Private Cloud (Amazon VPC)

Beispiele in dieser Kategorie

- Verhindern, dass Benutzer Amazon-VPC-Flow-Protokolle löschen
- Verhindern, dass ein VPC, der nicht bereits Internetzugang hat, einen solchen Zugang erhält

Verhindern, dass Benutzer Amazon-VPC-Flow-Protokolle löschen

Diese SCP verhindert, dass Benutzer oder Rollen in einem betroffenen Konto Amazon-Elastic-Compute-Cloud-(Amazon-EC2)-Flow-Protokolle oder CloudWatch-Protokoll-Gruppen oder Protokoll-Streams löschen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Verhindern, dass ein VPC, der nicht bereits Internetzugang hat, einen solchen Zugang erhält

Diese Service-Kontrollrichtlinie verhindert, dass Benutzer oder Rollen in einem betroffenen Konto die Konfiguration Ihrer Virtual Private Clouds (VPCs) für Amazon EC2 so verändern, dass sie Zugang zum Internet erhalten. Vorhandener direkter Zugriff oder Zugriff, der über Ihre Netzwerkumgebung vor Ort läuft, wird nicht blockiert.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
    }
  ]
}
```

Verwalten von Organisationseinheiten (OUs)

Mithilfe von Organisationseinheiten können Sie Konten gruppieren und als eine Einheit verwalten. Dadurch wird die Verwaltung Ihrer Konten stark vereinfacht. Wenn Sie beispielsweise einer OU ein richtlinienbasiertes Steuerelement zuweisen, übernehmen alle Konten in der Organisationseinheit automatisch diese Richtlinie. Sie können mehrere Organisationseinheiten in einer Organisation und mehrere Organisationseinheiten in anderen Organisationseinheiten erstellen. Jede OU kann mehrere Konten enthalten, die Sie zwischen einzelnen OUs verschieben können. Die Namen von OUs müssen jedoch innerhalb einer übergeordneten OU oder eines Stamms eindeutig sein.

> **Note**
>
> Es gibt einen Stamm in der Organisation, den für Sie AWS Organizations erstellt, wenn Sie Ihre Organisation zum ersten Mal einrichten.

Themen

- Navigieren in der Hierarchie von Stammverzeichnis und Organisationseinheit
- Erstellen einer OU
- Umbenennen einer OU
- Bearbeiten von Tags, die einer Organisationseinheit zugeordnet sind
- Verschieben der Konten in eine OU oder zwischen Stamm und OUs
- Löschen von OUs

Sie können auch alle Organisationseinheiten in Ihrer Organisation überprüfen. Weitere Informationen finden Sie unter Anzeigen von OU-Details.

Navigieren in der Hierarchie von Stammverzeichnis und Organisationseinheit

Um beim Verschieben von Konten oder Anhängen von Richtlinien zu verschiedenen Organisationseinheiten oder zum Stamm zu navigieren, können Sie die standardmäßige „Baumansicht“ verwenden.

AWS Management Console

So navigieren Sie in der Organisation als 'Baum'

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der Seite AWS-Konten im oberen Bereich Organization den Schalter Hierarchie (anstelle von Liste) aus.
3. Die Struktur wird zunächst mit dem Stamm angezeigt und zeigt nur die erste Ebene der untergeordneten Organisationseinheiten und Konten an. Um die Struktur zu erweitern, sodass tiefere Level angezeigt werden, wählen Sie das Erweiterungs-Symbol ( ) neben einer übergeordneten Entität. Wählen Sie zur Verbesserung der Übersichtlichkeit und zum Ausblenden eines Zweigs der Struktur das Minimierungs-Symbol ( ) neben einer erweiterten übergeordneten Entität.
4. Wählen Sie den Namen einer Organisationseinheit oder eines Stamms aus, um deren Details anzuzeigen und bestimmte Vorgänge auszuführen. Alternativ können Sie das Optionsfeld neben dem Namen auswählen und bestimmte Operationen an dieser Entität im Menü Aktionen ausführen.

Sie können auch die Liste nur der Konten in Ihrer Organisation in tabellarischer Form anzeigen, ohne zuerst zu einer Organisationseinheit navigieren zu müssen, um sie zu finden. In dieser Ansicht können Sie keine Organisationseinheiten sehen oder die ihnen zugeordneten Richtlinien bearbeiten.

AWS Management Console

So zeigen Sie die Organisation als flache Liste von Konten ohne Hierarchie an

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Wählen Sie auf der AWS-Konten Seite oben im Abschnitt Organisation das Schaltersymbol AWS-Konten Nur anzeigen aus, um es zu aktivieren.
3. Die Liste der Konten wird ohne Hierarchie angezeigt.

Erstellen einer OU

Wenn Sie am Verwaltungskonto der Organisation angemeldet sind, können Sie im Stamm der Organisation eine OU erstellen. OUs können bis zu fünf Ebenen aufweisen. So erstellen Sie eine Organisationseinheit:

Important

Wenn diese Organisation mit verwaltet wird AWS Control Tower, erstellen Sie Ihre OUs mit der AWS Control Tower Konsole oder den APIs . Wenn Sie die Organisationseinheit in Organizations erstellen, ist diese Organisationseinheit nicht bei registriert AWS Control Tower. Weitere Informationen finden Sie unter Verweisen auf Ressourcen außerhalb von AWS Control Tower im AWS Control Tower -Benutzerhandbuch.

Mindestberechtigungen

Um eine Organisationseinheit innerhalb des Stammverzeichnisses Ihrer Organisation zu erstellen, benötigen Sie die folgenden Berechtigungen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:CreateOrganizationalUnit`

AWS Management Console

So erstellen Sie eine OU

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zur Seite AWS-Konten.

   Die Konsole zeigt die Stamm-OU und ihren Inhalt an. Wenn Sie zum ersten Mal auf einen Stamm zugreifen, werden in der Konsole alle AWS-Konten der obersten Ebene angezeigt. Wenn Sie zuvor bereits einige Organisationseinheiten erstellt und Konten in diese

verschoben haben, zeigt die Konsolenansicht nur die übergeordneten Organisationseinheiten und die noch nicht verschobenen Konten.

3. (Optional) Wenn Sie eine Organisationseinheit in einer vorhandenen Organisationseinheit erstellen möchten, navigieren Sie zur untergeordneten Organisationseinheit, indem Sie deren Namen auswählen (nicht das Kontrollkästchen aktivieren) oder indem Sie

   neben den Organisationseinheiten in der Strukturansicht auswählen, bis Sie die gewünschte Organisationseinheit sehen.
4. Wenn Sie die richtige übergeordnete Organisationseinheit in der Hierarchie ausgewählt haben, wählen Sie im Menü Aktionen unter Organisationseinheit die Option Neu erstellen
5. Geben Sie im Dialogfeld Organisationseinheit erstellen den Namen der OU ein, die Sie erstellen möchten.
6. (Optional) Fügen Sie ein oder mehrere Tags hinzu, indem Sie Tag hinzufügen auswählen und dann einen Schlüssel und einen optionalen Wert eingeben. Wenn Sie den Wert leer lassen, wird er auf eine leere Zeichenfolge gesetzt; er ist nicht `null`. Sie können einer Organisationseinheit bis zu 50 Tags anfügen.
7. Wählen Sie abschließend die Option Erstellen einer Organisationseinheit aus.

Ihre neue OU wird in der übergeordneten OU angezeigt. Nun können Sie Konten in diese Organisationseinheit verschieben oder ihr Richtlinien zuweisen.

AWS CLI & AWS SDKs

So erstellen Sie eine OU

Sie können einen der folgenden Befehle verwenden, um eine Organisationseinheit zu erstellen:

- AWS CLI: create-organizational-unit

  Um eine Organisationseinheit zu erstellen, müssen Sie zuerst die Identität des Stammes oder der Organisationseinheit ermitteln, die der neuen Organisationseinheit übergeordnet sein soll.

  Um die Identität des Stamms zu ermitteln, verwenden Sie den Befehl list-roots. Um die Identität einer OU zu finden, navigieren Sie mit list-children zu der gewünschten OU.

  Das folgende Beispiel zeigt, wie Sie die Identität des Stammes finden und dann die Identität einer Organisationseinheit unter dem Stamm finden. Der letzte Befehl zeigt, wie eine neue Organisationseinheit in dieser gefundenen Organisationseinheit erstellt wird.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- -AWS SDKs CreateOrganizationalUnit:

Umbenennen einer OU

Wenn Sie am Verwaltungskonto der Organisation angemeldet sind, können Sie eine OU umbenennen. Führen Sie dazu die folgenden Schritte aus.

Mindestberechtigungen

Um eine Organisationseinheit innerhalb eines Stamms in Ihrer AWS Organisation umzubenennen, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:UpdateOrganizationalUnit`

AWS Management Console

So benennen Sie eine OU um

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zur Organisationseinheit und führen Sie einen der folgenden Schritte aus:
   - Wählen Sie das Optionsfeld
     
     neben der OU aus, die Sie umbenennen möchten. Wählen Sie dann im Menü Aktionen unter Organisationseinheit die Option Umbenennen aus.
   - Wählen Sie den Namen der Organisationseinheit aus, um auf die Detailseite der Organisationseinheit zuzugreifen. Wählen Sie dann oben auf der Seite Umbenennen.
3. Geben Sie im Dialogfeld Organisationseinheit umbenennen einen neuen Namen ein und wählen Sie dann Änderungen speichern.

AWS CLI & AWS SDKs

So benennen Sie eine OU um

Sie können einen der folgenden Befehle verwenden, um eine Organisationseinheit umzubenennen:

- AWS CLI: update-organizational-unit

Im folgenden Beispiel wird gezeigt, wie eine Organisationseinheit umbenannt wird.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
}
```

- -AWS SDKs UpdateOrganizationalUnit:

Bearbeiten von Tags, die einer Organisationseinheit zugeordnet sind

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie die Tags hinzufügen oder entfernen, die einer OU zugeordnet sind. Führen Sie dazu die folgenden Schritte aus.

Mindestberechtigungen

Um die Tags zu bearbeiten, die einer Organisationseinheit innerhalb eines Stamms in Ihrer AWS Organisation zugeordnet sind, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:DescribeOrganizationalUnit` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

So bearbeiten Sie die Tags, die einer Organisationseinheit zugeordnet sind:

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie auf der Seite AWS-Konten zum Namen der Organisationseinheit und wählen Sie die OU aus, deren Tags Sie bearbeiten möchten.
3. Wählen Sie auf der Detailseite der Organisationseinheit die Registerkarte Tags und dann Tags verwalten aus.
4. Sie können eine dieser Aktionen auf dieser Registerkarte ausführen:
   - Bearbeiten Sie den Wert für ein beliebiges Tag, indem Sie einen neuen Wert über dem alten eingeben. Sie können den Tag-Schlüssel nicht ändern. Um einen Schlüssel zu ändern, müssen Sie das Tag mit dem alten Schlüssel löschen und ein Tag mit dem neuen Schlüssel hinzufügen.
   - Entfernen Sie ein vorhandenes Tag, indem Sie neben dem Tag, das Sie entfernen möchten, Entfernen auswählen.
   - Fügen Sie ein neues Tag-Schlüssel-Wert-Paar hinzu. Wählen Sie Tag hinzufügen aus und geben Sie dann den neuen Schlüsselnamen und den optionalen Wert in die bereitgestellten Felder ein. Wenn Sie das Feld Wert leer lassen, ist der Wert eine leere Zeichenfolge; er ist nicht `null`.
5. Wählen Sie Änderungen speichern, nachdem Sie alle gewünschten Ergänzungen, Entfernungen und Änderungen vorgenommen haben.

AWS CLI & AWS SDKs

So bearbeiten Sie die Tags, die einer Organisationseinheit zugeordnet sind:

Sie können einen der folgenden Befehle verwenden, um die einer OU zugeordneten Tags zu ändern:

- AWS CLI: tag-resource und untag-resource

  Im folgenden Beispiel wird ein Tag `"Department"="12345"` einer Organisationseinheit angefügt. Beachten Sie, dass bei `Key` und `Value` die Groß-/Kleinschreibung beachtet wird.

```
$ aws organizations tag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tags Key=Department,Value=12345
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

Im folgenden Beispiel wird das `Department`-Tag aus einer OU entfernt.

```
$ aws organizations untag-resource \
    --resource-id ou-a1b2-f6g7h222 \
    --tag-keys Department
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- -AWS SDKs TagResource :und UntagResource

Verschieben der Konten in eine OU oder zwischen Stamm und OUs

Wenn Sie am Verwaltungskonto der Organisation angemeldet sind, können Sie Konten innerhalb der Organisation verschieben, entweder vom Stamm zu einer OU, zwischen verschiedenen OUs oder von einer OU zurück zum Stamm. Wenn Sie ein Konto in einer OU ablegen, unterliegt dieses den Richtlinien der übergeordneten OU sowie den Richtlinien aller OUs in der Kette der übergeordneten OUs bis hin zum Stamm. Wenn sich ein Konto nicht in einer Organisationseinheit befindet, unterliegt dieses nur direkt den Richtlinien dem Stamm und den Richtlinien, die dem Konto direkt zugeordnet sind. Führen Sie die folgenden Schritte aus, um Konten zu verschieben.

Mindestberechtigungen

Um Konten an einen neuen Ort in der Hierarchie der Organisationseinheiten zu verschieben, benötigen Sie die folgenden Berechtigungen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:MoveAccount`

AWS Management Console

So verschieben Sie Konten in eine OU

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite AWS-Konten das Konto oder die Konten, die Sie verschieben möchten. Sie können in der OU-Hierarchie navigieren oder Nur AWS-Konten anzeigen aktivieren, um eine flache Liste von Konten ohne die OU-Struktur anzuzeigen. Wenn Sie viele Konten haben, müssen Sie möglicherweise unten in der Liste Weitere Konten in 'ou-name' laden auswählen, um alle Konten zu finden, die Sie verschieben möchten.
3. Aktivieren Sie das Kontrollkästchen
   ☑
   neben dem Namen jedes Kontos, das Sie verschieben möchten.
4. Wählen Sie im Menü Aktionen unter AWS-Konto die Option Verschieben aus.
5. Wählen Sie im Dialogfeld AWS-Kontoverschieben die Organisationseinheit oder den Stamm aus, in die Sie Konten verschieben möchten, und wählen Sie dann AWS-Kontoverschieben.

AWS CLI & AWS SDKs

So verschieben Sie ein Konto in eine OU

Sie können einen der folgenden Befehle verwenden, um ein Konto zu verschieben:

- AWS CLI: move-account

  Im folgenden Beispiel wird ein AWS-Konto vom Stamm in eine Organisationseinheit verschoben. Beachten Sie, dass Sie die IDs sowohl des Quell- als auch des Zielcontainers angeben müssen.

  ```
  $ aws organizations move-account \
      --account-id 111122223333 \
      --source-parent-id r-a1b2 \
      --destination-parent-id ou-a1b2-f6g7h111
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- -AWS SDKs MoveAccount:

Löschen von OUs

Wenn Sie am Verwaltungskonto der Organisation angemeldet sind, können Sie nicht mehr benötigte OUs löschen.

Dazu müssen Sie zunächst alle Konten aus der OU sowie aus allen untergeordneten OUs an eine andere Stelle verschieben und dann können Sie die untergeordneten OUs löschen.

Mindestberechtigungen

Zum Löschen einer Organisationseinheit benötigen Sie die folgenden Berechtigungen:

- `organizations:DescribeOrganization` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden
- `organizations:DeleteOrganizationalUnit`

AWS Management Console

So löschen Sie eine OU

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite AWS-Konten nach den OUs, die Sie löschen möchten und aktivieren Sie das Kontrollkästchen
   
   neben dem Namen der einzelnen OUs.
3. Wählen Sie Aktionen und dann unter Organisationseinheit die Option Löschen aus.
4. Um zu bestätigen, dass Sie die Organisationseinheiten löschen möchten, geben Sie den Namen der Organisationseinheit (wenn Sie nur eine Organisationseinheit löschen möchten) oder das Wort „Löschen“ (wenn Sie mehrere Organisationseinheiten ausgewählt haben) ein und wählen Sie dann Löschen.

   AWS Organizations löscht die OUs und entfernt sie aus der Liste.

AWS CLI & AWS SDKs

So löschen Sie eine OU

Sie können einen der folgenden Befehle verwenden, um eine Organisationseinheit zu löschen:

- AWS CLI: delete-organizational-unit

  Im folgenden Beispiel wird gezeigt, wie eine Organisationseinheit gelöscht wird.

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- -AWS SDKs DeleteOrganizationalUnit:

Markieren von AWS Organizations-Ressourcen

Ein Tag ist eine benutzerdefinierte Attributskennzeichnung, die Sie zu einer AWS-Ressource hinzufügen, damit sich Ressourcen einfacher identifizieren, organisieren und finden lassen. Jedes Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Tag-Schlüssel können bis zu 128 Zeichen lang sein und berücksichtigen die Groß-/Kleinschreibung.
- Einem Tag-Wert (z. B. `111122223333` oder `Production`). Tag-Werte können bis zu 256 Zeichen lang sein und wie bei Tag-Schlüsseln muss die Groß-/Kleinschreibung beachtet werden. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge.

Weitere Informationen darüber, welche Zeichen in einem Tag-Schlüssel oder -Wert zulässig sind, finden Sie im Tags-Parameter der Tag-API in der Ressource-Groups-Markierungs-API-Referenz.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Weitere Informationen finden Sie unter Bewährte Methoden zum Markieren von AWS Ressourcen.

> **Tip**
>
> Verwenden Sie Tag-Richtlinien, um die Implementierung von Tags in den Ressourcen in den Konten Ihrer Organisation zu standardisieren.

Derzeit unterstützt AWS Organizations die folgenden Tagging-Operationen, wenn Sie beim Verwaltungskonto angemeldet sind:

- Sie können den folgenden Organisationsressourcen Tags hinzufügen:
  - AWS-Konten
  - Organisationseinheiten
  - Der Stamm der Organisation
  - Richtlinien

Sie können Tags zu folgenden Zeiten hinzufügen:

- Wenn Sie die Ressource erstellen – Geben Sie die Tags entweder in der Organisationskonsole an oder verwenden Sie den `Tags`-Parameter mit einem der `Create`-API-Vorgänge. Dies gilt nicht für das Stammverzeichnis der Organisation.
- Nachdem Sie die Ressource erstellt haben – Verwenden Sie die Organizationskonsole oder rufen Sie die `TagResource`-Operation auf.

Sie können die Tags für jede der Taggable-Ressourcen in AWS Organizations anzeigen, indem Sie die Konsole verwenden oder die `ListTagsForResource`-Operation aufrufen.

Sie können Tags aus einer Ressource entfernen, indem Sie die zu entfernenden Schlüssel mithilfe der Konsole oder durch Aufrufen der `UntagResource`-Operation angeben.

Verwenden von Markierungen

Tags helfen Ihnen, Ihre Ressourcen zu organisieren, indem Sie sie nach Kategorien gruppieren können, die für Sie nützlich sind. Sie können beispielsweise ein „Abteilungs“-Tag zuweisen, das die besitzende Abteilung verfolgt. Sie können ein „Umgebungs“-Tag zuweisen, um zu verfolgen, ob eine bestimmte Ressource Teil Ihrer Alpha-, Beta-, Gamma- oder Produktionsumgebung ist.

Sie können Tags auch verwenden, um:

- Tagging-Standards für Ihre Ressourcen durchzusetzen.
- Den Zugriff auf Ihre Ressourcen zu kontrollieren.

Hinzufügen, Aktualisieren und Entfernen von Tags

Wenn Sie sich am Verwaltungskonto Ihrer Organisation anmelden, können Sie Tags zu den Ressourcen in Ihrer Organisation hinzufügen.

Hinzufügen von Tags zu einer Ressource beim Erstellen

Mindestberechtigungen

Um Tags zu einer Ressource hinzufügen zu können, wenn Sie sie erstellt haben, benötigen Sie folgende Berechtigungen:

- Berechtigung zum Erstellen einer Ressource des angegebenen Typs
- `organizations:TagResource`

- `organizations:ListTagsForResource` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

Sie können Tag-Schlüssel und -Werte hinzufügen, die den folgenden Ressourcen zugeordnet sind.

- AWS-Konto
  - Erstelltes Konto
  - Eingeladenes Konto
- Organisationseinheit (OU)
- Richtlinie
  - Richtlinie zur Abmeldung von KI-Services
  - Backup-Richtlinie
  - Service-Kontrollrichtlinie
  - Tag-Richtlinie

Der Organisationsstamm wird erstellt, wenn Sie die Organisation anfangs erstellen, sodass Sie ihr nur Tags als vorhandene Ressource hinzufügen können.

Hinzufügen oder Aktualisieren von Tags für eine vorhandene Ressource

Sie können auch neue Tags hinzufügen oder die Werte von Tags aktualisieren, die vorhandenen Ressourcen zugeordnet sind.

Mindestberechtigungen

Zum Hinzufügen oder Aktualisieren von Tags zu Ressourcen in Ihrer Organisation benötigen Sie folgende Berechtigungen:

- `organizations:TagResource`
- `organizations:ListTagsForResource` – nur erforderlich, wenn Sie die Organizations-Konsole verwenden

Zum Entfernen von Tags aus den Ressourcen in Ihrer Organisation benötigen Sie folgende Berechtigungen:

- `organizations:UntagResource`

AWS Management Console

So fügen Sie Tags für eine vorhandene -Ressource hinzu, aktualisieren oder entfernen sie

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Navigieren Sie zu dem Konto, dem Stammverzeichnis, der Organisationseinheit oder der Richtlinie, und klicken Sie auf den Namen, um die Detailseite zu öffnen.
3. Wählen Sie auf der Registerkarte Tags die Option Manage tags (Tags verwalten).
4. Sie können neue Tags hinzufügen, die Werte vorhandener Tags ändern oder Tags entfernen.

   Um ein Tag hinzuzufügen, wählen Sie Tag hinzufügen und geben dann einen Schlüssel und optional einen Wert für das Tag ein.

   Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).

   Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Verwenden Sie die Groß-/Kleinschreibung, die Sie zum Standard machen möchten. Sie müssen auch die Anforderungen der geltenden Tag-Richtlinien erfüllen.
5. Wiederholen Sie den vorherigen Schritt, bis Sie alle Tags hinzugefügt haben.
6. Wählen Sie Änderungen speichern aus.

AWS CLI & AWS SDKs

So fügen Sie Tags zu einer vorhandenen Ressource hinzu oder aktualisieren sie

Sie können einen der folgenden Befehle verwenden, um Tags zu den kennzeichenbaren Ressourcen in Ihrer Organisation hinzuzufügen:

- AWS CLI: tag-resource
- AWS -SDKs TagResource:

So löschen Sie Tags von einer Ressource in Ihrer Organisation

Sie können einen der folgenden Befehle verwenden, um Tags zu löschen:

- AWS CLI: untag-resource
- AWS -SDKs UntagResource:

Verwenden von AWS Organizations mit anderen AWS-Services

Sie können mit dem vertrauenswürdigen Zugriff einem von Ihnen angegebenen unterstützten AWS-Service, der als vertrauenswürdiger Service bezeichnet wird, ermöglichen, in Ihrem Namen Aufgaben für Ihre Organisation und deren Konten durchzuführen. Dies umfasst das Erteilen von Berechtigungen für den vertrauenswürdigen Service, hat aber keine Auswirkungen auf die Berechtigungen für Benutzer und Rollen. Wenn Sie den Zugriff aktivieren, kann der vertrauenswürdige Service in jedem Konto Ihrer Organisation immer dann, wenn erforderlich, eine IAM-Rolle erstellen, die als serviceverknüpfte Rolle bezeichnet wird. Der Rolle ist eine Berechtigungsrichtlinie zugeordnet, die es dem vertrauenswürdigen Service ermöglicht, die Aufgaben auszuführen, die in der Dokumentation des Services angegeben sind. Auf diese Weise können Sie Einstellungs- und Konfigurationsdetails angeben, die der vertrauenswürdigen Service in Ihrem Namen in den Konten Ihrer Organisation pflegen soll. Der vertrauenswürdige Service erstellt nur serviceverknüpfte Rollen, wenn er Verwaltungsaktionen für Konten ausführen muss, und nicht unbedingt in allen Konten der Organisation.

Important

Sofern die Option verfügbar ist, sollten Sie den vertrauenswürdigen Zugriff unbedingt aktivieren und deaktivieren, indem Sie ausschließlich die Konsole des vertrauenswürdigen Service, dessen AWS CLI oder entsprechende API-Vorgänge benutzen. Auf diese Weise kann der vertrauenswürdige Service jede erforderliche Initialisierung durchführen, wenn vertrauenswürdigen Zugriff aktiviert wird, z. B. das Erstellen aller erforderlichen Ressourcen und die erforderliche Bereinigung von Ressourcen beim Deaktivieren des vertrauenswürdigen Zugriffs.
Informationen zum Aktivieren oder Deaktivieren des vertrauenswürdigen Dienstzugriffs auf Ihre Organisation mithilfe des vertrauenswürdigen Dienstes finden Sie unter dem Weitere Informationen-Link unter der Spalte Unterstützt vertrauenswürdigen Zugriff unter AWS Dienste, die Sie mit verwenden können AWS Organizations.
Wenn Sie den Zugriff über die Organizationskonsole, CLI-Befehle oder API-Vorgänge deaktivieren, werden folgende Aktionen ausgeführt:

- Der Service kann keine serviceverknüpfte Rolle mehr in den Konten Ihrer Organisation erstellen. Dies bedeutet, dass der Service keine Vorgänge in Ihrem Namen für neue Konten in Ihrer Organisation ausführen kann. Der Service kann weiterhin Vorgänge in

älteren Konten ausführen, bis der Service seine Bereinigung von AWS Organizations fertigstellt.

- Der Service kann keine Aufgaben mehr in den Mitgliedskonten in der Organisation ausführen, es sei denn, diese Vorgänge sind explizit durch die IAM-Richtlinien zulässig, die Ihren Rollen zugeordnet sind. Dies schließt jede Datenaggregation von den Mitgliedskonten zum Verwaltungskonto oder gegebenenfalls zu einem delegierten Administratorkonto ein.
- Einige Services erkennen dies und bereinigen alle verbleibenden Daten oder Ressourcen im Zusammenhang mit der Integration, während andere Services nicht mehr auf die Organisation zugreifen, aber alle historischen Daten und Konfigurationen vorhanden lassen, um eine mögliche erneute Aktivierung der Integration zu unterstützen.

Stattdessen stellt die Verwendung der Konsole oder der Befehle des anderen Services zum Deaktivieren der Integration sicher, dass der andere Service alle Ressourcen bereinigen kann, die nur für die Integration erforderlich sind. Wie der Service seine Ressourcen in den Konten der Organisation bereinigt, hängt von diesem Service ab. Weitere Informationen finden Sie in der Dokumentation zu dem anderen AWS-Service.

Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs

Für den vertrauenswürdigen Zugriff sind Berechtigungen für zwei Services erforderlich: für AWS Organizations und für den vertrauenswürdigen Service. Zum Aktivieren des vertrauenswürdigen Zugriffs wählen Sie eines der folgenden Szenarien aus:

- Wenn Sie über Anmeldeinformationen mit Berechtigungen in AWS Organizations und den vertrauenswürdigen Service verfügen, aktivieren Sie den Zugriff mithilfe von Tools (Konsole oder AWS CLI), die über den vertrauenswürdigen Service bereitgestellt sind. Auf diese Weise kann der Service den vertrauenswürdigen Zugriff in Ihrem Namen in AWS Organizations aktivieren und alle Ressourcen erstellen, die der Service für die Durchführung seiner Aufgaben in Ihrer Organisation benötigt.

  Für diese Anmeldeinformationen sind mindestens die folgenden Berechtigungen erforderlich:

  - `organizations:EnableAWSServiceAccess`. Sie können auch den `organizations:ServicePrincipal`-Bedingungsschlüssel mit dieser Operation verwenden,

um Anfragen zu begrenzen, die diese Operationen an eine Liste genehmigter Service Prinzipal-Namen richten. Weitere Informationen finden Sie unter Bedingungsschlüssel.

- `organizations:ListAWSServiceAccessForOrganization` – Erforderlich bei Verwendung der AWS Organizations-Konsole
- Die Berechtigungen, die mindestens vom vertrauenswürdigen Service benötigt werden, hängen vom Service ab. Weitere Informationen finden Sie in der Dokumentation zum vertrauenswürdigen Service.

- Wenn eine Person über Anmeldeinformationen mit Berechtigungen in AWS Organizations verfügt, jemand anderes aber über Anmeldeinformationen mit Berechtigungen im vertrauenswürdigen Service, führen Sie diese Schritte in der folgenden Reihenfolge aus:

  1. Die Person, die über Anmeldeinformationen mit Berechtigungen in AWS Organizations verfügt, sollte die AWS Organizations-Konsole, die AWS CLI oder ein AWS-SDK nutzen, um den vertrauenswürdigen Zugriff für den vertrauenswürdigen Service zu aktivieren. Dadurch erhält der andere Service die Berechtigung, die erforderliche Konfiguration in der Organisation durchzuführen, wenn der folgende Schritt (Schritt 2) durchgeführt wird.

     Die AWS Organizations-Berechtigungen, die mindestens erforderlich sind, sind:

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – Nur erforderlich bei Verwendung der AWS Organizations-Konsole

     Informationen zu den spezifischen Schritte zum Aktivieren des vertrauenswürdigen Zugriffs in AWS Organizations finden Sie unter So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff.
  2. Die Person, die über Anmeldeinformationen mit Berechtigungen im vertrauenswürdigen Service verfügt, ermöglicht diesem Service das Arbeiten mit AWS Organizations. Dadurch wird der Service angewiesen, alle erforderlichen Initialisierungen durchzuführen. Dazu zählt beispielsweise das Erstellen von Ressourcen, die für die Ausführung des vertrauenswürdigen Services in Ihrer Organisation erforderlich sind. Weitere Informationen finden Sie in den servicespezifischen Anleitungen unter AWS Dienste, die Sie mit verwenden können AWS Organizations.

Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs

Wenn Sie nicht mehr möchten, dass der vertrauenswürdige Service in Ihrer Organisation oder deren Konten aktiv ist, wählen Sie eines der folgenden Szenarien aus.

> **Important**
>
> Das Deaktivieren des vertrauenswürdigen Servicezugriffs verhindert nicht, dass Benutzer und Rollen mit entsprechenden Berechtigungen diesen Service verwenden können. Wenn Sie den Zugriff für Benutzer und Rollen auf einen AWS-Service vollständig sperren möchten, können Sie die IAM-Berechtigungen entziehen, durch die der Zugriff möglich war, oder Sie könnenService-Kontrollrichtlinien (SCPs) in AWS Organizations nutzen.
> SCPs können nur auf Mitgliedskonten angewendet werden. SCPs gelten nicht für das Verwaltungskonto. Wir empfehlen Ihnen, keine Services im Verwaltungskonto auszuführen. Führen Sie sie stattdessen in Mitgliedskonten aus, in denen Sie die Sicherheit mithilfe von SCPs steuern können.

- Wenn Sie über Anmeldeinformationen mit Berechtigungen in AWS Organizations und den vertrauenswürdigen Service verfügen, deaktivieren Sie den Zugriff mithilfe von Tools (Konsole oder AWS CLI), die für den vertrauenswürdigen Service verfügbar sind. Der Service führt dann eine Bereinigung durch, indem er die nicht mehr benötigte Ressource entfernt und den vertrauenswürdigen Zugriff für den Service in Ihrem Namen in AWS Organizations deaktiviert.

  Für diese Anmeldeinformationen sind mindestens die folgenden Berechtigungen erforderlich:

  - `organizations:DisableAWSServiceAccess`. Sie können auch den `organizations:ServicePrincipal`-Bedingungsschlüssel mit dieser Operation verwenden, um Anfragen zu begrenzen, die diese Operationen an eine Liste genehmigter Service Prinzipal-Namen richten. Weitere Informationen finden Sie unter Bedingungsschlüssel.
  - `organizations:ListAWSServiceAccessForOrganization` – Erforderlich bei Verwendung der AWS Organizations-Konsole
  - Die Berechtigungen, die mindestens vom vertrauenswürdigen Service benötigt werden, hängen vom Service ab. Weitere Informationen finden Sie in der Dokumentation zum vertrauenswürdigen Service.

- Wenn die Anmeldeinformationen mit Berechtigungen in AWS Organizations nicht die Anmeldeinformationen mit Berechtigungen im vertrauenswürdigen Service sind, führen Sie diese Schritte in der folgenden Reihenfolge aus:

  1. Die Person mit Berechtigungen im vertrauenswürdigen Service deaktiviert zuerst den Zugriff über den Service. Dies weist den vertrauenswürdigen Service an, eine Bereinigung vorzunehmen, indem die für den vertrauenswürdigen Zugriff erforderliche Ressourcen entfernt werden. Weitere Informationen finden Sie in den servicespezifischen Anleitungen unter AWS Dienste, die Sie mit verwenden können AWS Organizations.
  2. Die Person, die über Berechtigungen in AWS Organizations verfügt, kann dann über die AWS Organizations-Konsole, AWS CLI oder ein AWS-SDK den Zugriff für den vertrauenswürdigen Service deaktivieren. Dadurch werden die Berechtigungen für den vertrauenswürdigen Service aus der Organisation und deren Konten entfernt.

     Die AWS Organizations-Berechtigungen, die mindestens erforderlich sind, sind:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` – Nur erforderlich bei Verwendung der AWS Organizations-Konsole

     Informationen zu den spezifischen Schritte zum Deaktivieren des vertrauenswürdigen Zugriffs in AWS Organizations finden Sie unter So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff.

So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff

Wenn Sie nur über Berechtigungen für AWS Organizations verfügen und einen vertrauenswürdigen Zugriff auf Ihre Organisation im Namen des Administrators anderer AWS-Services aktivieren oder deaktivieren möchten, führen Sie die folgenden Schritte durch.

> **Important**
>
> Sofern die Option verfügbar ist, sollten Sie den vertrauenswürdigen Zugriff unbedingt aktivieren und deaktivieren, indem Sie ausschließlich die Konsole des vertrauenswürdigen Service, dessen AWS CLI oder entsprechende API-Vorgänge benutzen. Auf diese Weise kann der vertrauenswürdige Service jede erforderliche Initialisierung durchführen, wenn vertrauenswürdigen Zugriff aktiviert wird, z. B. das Erstellen aller erforderlichen Ressourcen

und die erforderliche Bereinigung von Ressourcen beim Deaktivieren des vertrauenswürdigen Zugriffs.
Informationen zum Aktivieren oder Deaktivieren des vertrauenswürdigen Dienstzugriffs auf Ihre Organisation mithilfe des vertrauenswürdigen Dienstes finden Sie unter dem Weitere Informationen-Link unter der Spalte Unterstützt vertrauenswürdigen Zugriff unter AWS Dienste, die Sie mit verwenden können AWS Organizations.
Wenn Sie den Zugriff über die Organizationskonsole, CLI-Befehle oder API-Vorgänge deaktivieren, werden folgende Aktionen ausgeführt:

- Der Service kann keine serviceverknüpfte Rolle mehr in den Konten Ihrer Organisation erstellen. Dies bedeutet, dass der Service keine Vorgänge in Ihrem Namen für neue Konten in Ihrer Organisation ausführen kann. Der Service kann weiterhin Vorgänge in älteren Konten ausführen, bis der Service seine Bereinigung von AWS Organizations fertigstellt.
- Der Service kann keine Aufgaben mehr in den Mitgliedskonten in der Organisation ausführen, es sei denn, diese Vorgänge sind explizit durch die IAM-Richtlinien zulässig, die Ihren Rollen zugeordnet sind. Dies schließt jede Datenaggregation von den Mitgliedskonten zum Verwaltungskonto oder gegebenenfalls zu einem delegierten Administratorkonto ein.
- Einige Services erkennen dies und bereinigen alle verbleibenden Daten oder Ressourcen im Zusammenhang mit der Integration, während andere Services nicht mehr auf die Organisation zugreifen, aber alle historischen Daten und Konfigurationen vorhanden lassen, um eine mögliche erneute Aktivierung der Integration zu unterstützen.

Stattdessen stellt die Verwendung der Konsole oder der Befehle des anderen Services zum Deaktivieren der Integration sicher, dass der andere Service alle Ressourcen bereinigen kann, die nur für die Integration erforderlich sind. Wie der Service seine Ressourcen in den Konten der Organisation bereinigt, hängt von diesem Service ab. Weitere Informationen finden Sie in der Dokumentation zu dem anderen AWS-Service.

AWS Management Console

So aktivieren Sie vertrauenswürdigen Servicezugriff

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Suchen Sie auf der Seite Services nach der Zeile für den Service, den Sie aktivieren möchten und wählen Sie den Namen aus.
3. Wählen Sie Vertrauenswürdigen Zugriff aktivieren.
4. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
5. Wenn Sie den Zugriff aktivieren, informieren Sie den Administrator des anderen AWS-Services darüber, dass nun der andere Service für die Ausführung in AWS Organizations aktiviert werden kann.

So deaktivieren Sie einen vertrauenswürdigen Servicezugriff

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services nach der Zeile für den Service, den Sie deaktivieren möchten und wählen Sie den Namen aus.
3. Warten Sie, bis der Administrator des anderen Services Ihnen mitteilt, dass der Service deaktiviert und seine Ressourcen bereinigt wurden.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.

AWS CLI, AWS API

So aktivieren oder deaktivieren Sie einen vertrauenswürdigen Servicezugriff

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren oder deaktivieren:

- AWS CLI: AWS Organizations enable-aws-service-access
- AWS CLI: AWS Organizations disable-aws-service-access
- AWS-API: EnableAWSServiceAccess
- AWS-API: DisableAWSServiceAccess

AWS Organizations und serviceverknüpfte Rollen

AWS Organizations verwendet servicegebundene IAM-Rollen, um vertrauenswürdigen Services die Durchführung von Aufgaben in Ihrem Namen in den Mitgliedskonten Ihrer Organisation zu ermöglichen. Wenn Sie einen vertrauenswürdigen Service konfigurieren und ihn für die Integration in Ihre Organisation autorisieren, kann dieser Service verlangen, dass AWS Organizations in jedem seiner Mitgliedskonten eine servicegebundene Rolle erstellt. Der vertrauenswürdige Service tut dies asynchron – je nach Bedarf – und nicht unbedingt in allen Konten der Organisation gleichzeitig. Die servicegebundene Rolle verfügt über vordefinierte IAM-Berechtigungen, die es dem vertrauenswürdigen Service ermöglichen, nur bestimmte Aufgaben in diesem Konto auszuführen. Im Allgemeinen verwaltet AWS alle servicegebundenen Rollen. Dies bedeutet, dass Sie die Rollen oder die verknüpften Richtlinien in der Regel nicht ändern können.

Um all dies zu ermöglichen, stellt AWS Organizations das Mitgliedskonto mit einer servicegebundenen Rolle namens `AWSServiceRoleForOrganizations` bereit, sobald Sie ein Konto in einer Organisation erstellen oder eine Einladung annehmen, mit der Ihr bestehendes Konto einer Organisation beitritt. Nur der AWS Organizations-Service selbst kann diese Rolle annehmen. Die Rolle hat Berechtigungen, die AWS Organizations erlauben, servicegebundene Rollen für andere AWS-Services anzulegen. Diese servicegebundene Rolle ist in allen Organisationen vorhanden.

Wenn Ihr Unternehmen nur konsolidierte Fakturierungsfunktionen aktiviert hat, wird die servicegebundene Rolle namens `AWSServiceRoleForOrganizations` nie verwendet und kann gelöscht werden. Wir empfehlen diese Vorgehensweise jedoch nicht. Wenn Sie später alle Funktionen in Ihrer Organisation aktivieren möchten, ist die Rolle erforderlich und muss wiederhergestellt werden. Die folgenden Prüfungen finden statt, wenn Sie den Prozess starten, um alle Funktionen zu aktivieren:

- Für jedes Mitgliedskonto, das zum Beitritt zur Organisation eingeladen wurde – Der Kontoadministrator erhält eine Anforderung zur Zustimmung für die Aktivierung aller Funktionen. Um der Anforderung erfolgreich zustimmen zu können, muss der Administrator sowohl die Berechtigung `organizations:AcceptHandshake` als auch die Berechtigung `iam:CreateServiceLinkedRole` besitzen, wenn die serviceverknüpfte Rolle (`AWSServiceRoleForOrganizations`) nicht bereits vorhanden ist. Wenn die Rolle `AWSServiceRoleForOrganizations` bereits existiert, benötigt der Administrator nur die Berechtigung `organizations:AcceptHandshake`, um der Anfrage zuzustimmen. Wenn der Administrator der Anforderung zustimmt, erstellt AWS Organizations die servicegebundene Rolle, wenn sie noch nicht vorhanden ist.

- Für jedes Mitgliedskonto, das in der Organisation angelegt wurde – Der Kontoadministrator erhält die Anforderung, die servicegebundene Rolle neu zu erstellen. (Der Administrator des Mitgliedskontos erhält keine Aufforderung, alle Funktionen zu aktivieren, da der Administrator des Verwaltungskontos als Eigentümer der erstellten Mitgliedskonten betrachtet wird.) AWS Organizations erstellt die servicegebundene Rolle, wenn der Administrator des Mitgliedskontos der Anforderung zustimmt. Der Administrator muss sowohl die Berechtigung `organizations:AcceptHandshake` als auch die Berechtigung `iam:CreateServiceLinkedRole` besitzen, um den Handshake erfolgreich akzeptieren zu können.

Nachdem Sie alle Funktionen in Ihrer Organisation aktiviert haben, können Sie die servicegebundene Rolle `AWSServiceRoleForOrganizations` nicht mehr aus einem Konto löschen.

> **Important**
>
> AWS Organizations-Service-Kontrollrichtlinien wirken sich nie auf serviceverknüpfte Rollen aus. Diese Rollen sind von jeglichen Beschränkungen durch Service-Kontrollrichtlinien ausgenommen.

AWS Dienste, die Sie mit verwenden können AWS Organizations

Mit können AWS Organizations Sie Account-Management-Aktivitäten in großem Umfang durchführen, indem Sie mehrere Aktivitäten AWS-Konten in einer einzigen Organisation konsolidieren. Die Konsolidierung von Konten vereinfacht die Nutzung anderer AWS Dienste. Sie können die in AWS Organizations ausgewählten AWS Diensten verfügbaren Verwaltungsdienste für mehrere Konten nutzen, um Aufgaben für alle Konten auszuführen, die Mitglieder Ihrer Organisation sind.

In der folgenden Tabelle sind die AWS Dienste aufgeführt, die Sie zusammen verwenden können AWS Organizations, sowie die Vorteile, die sich aus der Nutzung der einzelnen Dienste auf organisationsweiter Ebene ergeben.

Vertrauenswürdiger Zugriff — Sie können einen kompatiblen AWS Dienst für die Ausführung von Vorgängen AWS-Konten in allen Bereichen Ihrer Organisation aktivieren. Weitere Informationen finden Sie unter Verwenden von AWS Organizations mit anderen AWS-Services.

Delegierter Administrator für AWS Dienste — Ein kompatibler AWS Dienst kann ein AWS Mitgliedskonto in der Organisation als Administrator für die Konten der Organisation in diesem Dienst registrieren. Weitere Informationen finden Sie unter Delegierter Administrator für AWS-Services, die mit Organizations zusammenarbeiten.

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Account Management Verwalten Sie die Details und Metadaten für alle Informationen AWS-Konten für Ihre Organisation.	Sie können die alternativen Kontaktinformationen für alle Konten in Ihrer Organisation erstellen, aktualisieren und löschen.	 Ja Weitere Informationen	 Ja Weitere Informationen	
AWS Dienst zur Anwendungsmigration (MGN)	So lassen sich große Migrationen für mehrere Konten	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Mit dem Application Migration Service können Unternehmen ohne Kompatibilitätsprobleme, Leistungsunterbrechungen oder lange Umstellungsfenster auf AWS eine große Anzahl von physischen, virtuellen oder Cloud-Servern zugreifen. lift-and-shift	bewältigen.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Artifact Laden Sie Berichte zur Einhaltung von AWS Sicherheitsvorschriften wie ISO- und PCI-Berichte herunter.	Sie können im Namen aller Konten in Ihrer Organisation Vereinbarungen zustimmen.	 Ja Weitere Informationen	 Ja Siehe AWS Artifact.	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Audit Manager Automatisieren Sie die kontinuierliche Sammlung von Beweisen, um Ihre Nutzung von Cloud-Services zu überprüfen.	Überprüfen Sie kontinuierlich Ihre AWS Nutzung für mehrere Konten in Ihrem Unternehmen, um die Bewertung von Risiken und der Einhaltung von Vorschriften zu vereinfachen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Backup Verwalten und überwachen Sie Backups über alle Konten in Ihrer Organisation hinweg.	Sie können Backup-Pläne für die gesamte Organisation oder für Gruppen von Konten in Ihren Organisationseinheiten (OUs) konfigurieren und verwalten. Sie können die Backups für alle Ihre Konten zentral	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	überwachen.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS CloudFormation Stacksets Ermöglicht Ihnen das Erstellen, Aktualisieren und Löschen von Stacks über mehrere Konten und Regionen in einer einzigen Operation.	Ein Benutzer im Verwaltungskonto oder ein delegiertes Administratorkonto kann ein Stack-Set mit serviceverwalteten Berechtigungen erstellen, der Stack-Instances für Konten in Ihrer Organisation bereitstellt.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS CloudTrail Aktivierung von Governance-, Compliance-, Betriebs- und Risikoprüfungen für Ihr Konto.	Ein Benutzer mit einem Verwaltungskonto oder einem Konto für den delegierten Administrator kann einen Organisationspfad oder Ereignisdatenspeicher erstellen, der alle Ereignisse für alle Konten in der Organisation	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	protokolliert.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Compute Optimizer Holen Sie sich Empfehlungen zur AWS Rechenoptimierung.	Sie können alle Ressourcen analysieren, die sich in den Konten Ihrer Organisation befinden, um Optimierungsempfehlungen zu erhalten. Weitere Informationen finden Sie unter Vom Compute Optimizer unterstützt	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	zte Konten im AWS Compute Optimizer-Benutzerhandbuch.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Config Zugriff, Prüfung und Bewertung der Konfigurationen Ihrer AWS -Ressourcen.	Sie können eine organisationsweite Ansicht Ihres Compliance-Status abrufen. Sie können AWS Config API-Operationen auch verwenden, um AWS Config Regeln und Konformitätspakete AWS-Konten in Ihrem	 Ja Weitere Informationen	 Ja Weitere Informationen: Konfigurationsregeln Conformance Packs Datenaggregation für mehrere Konten und Regionen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	gesamten Unternehmen zu verwalten. Sie können ein delegiertes Administratorkonto verwenden, um Ressourcenkonfigurations- und Compliance-Daten aus allen Mitgliedskonten einer Organisation in AWS Organizations zu			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	aggregieren. Weitere Informationen finden Sie unter Einen delegierten Administrator registrieren im AWS Config - Entwicklerhandbuch.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Control Tower Verwalten und richten Sie eine sichere, kompatible AWS -Umgebung mit mehreren Konten ein.	Sie können eine landing zone einrichten, eine Umgebung mit mehreren Konten für all Ihre AWS Ressourcen. Diese Umgebung umfasst eine Organisation und Organisationsentitäten. Sie können diese Umgebung verwenden, um	 Ja Weitere Informationen	 Nein	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Compliance-Vorschriften für alle Ihre AWS-Konten durchzusetzen. Weitere Informationen finden Sie unter Funktionsweise von AWS Control Tower und Verwalten von Konten über AWS Organizations im Benutzerhandbuch von AWS			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Control Tower .			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Cost Optimization Hub Sammeln Sie Kostenempfehlungen für alle AWS Optimierungsprodukte.	Sie können ganz einfach Empfehlungen zur AWS Kostenoptimierung für Ihre AWS Organizations Mitgliedskonten und AWS Regionen identifizieren, filtern und zusammenfassen. Weitere Informationen finden Sie unter Cost	 Ja Weitere Informationen	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Optimization Hub im Cost Optimization Hub-Benutzerhandbuch.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon Detective Generieren Sie Visualisierungen aus Ihren Protokolldaten, um die Ursache von Sicherheitsergebnissen oder verdächtigen Aktivitäten zu analysieren, zu untersuchen und schnell zu identifizieren.	Sie können Amazon Detective integrieren, AWS Organizations um sicherzustellen, dass Ihr Detective-Verhaltensdiagramm Einblick in die Aktivitäten aller Ihrer Unternehmenskonten bietet.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
DevOpsAmazon-Guru Analysieren Sie Betriebsdaten und Anwendungsmetriken und Ereignisse, um Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Benutzer werden benachrichtigt, wenn DevOps Guru ein betriebliches Problem oder Risiko feststellt.	Sie können es integrieren en AWS Organizations , um Erkenntnisse aus allen Konten in Ihrem gesamten Unternehmen zu verwalten. Sie delegieren einen Administrator, um Erkenntnisse aus allen Konten anzuzeigen, zu sortieren	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	und zu filtern, um den organisationsweiten Zustand aller überwachten Anwendungen zu erhalten.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Directory Service Richten Sie Verzeichnisse in der AWS Cloud ein und führen Sie sie aus oder verbinden Sie Ihre AWS Ressourcen mit einem vorhandenen lokalen Microsoft Active Directory.	Sie können es integrieren AWS Directory Service , AWS Organizations um eine nahtlose Verzeichnisfreigabe zwischen mehreren Konten und jeder VPC in einer Region zu ermöglichen.	 Ja Weitere Informationen	 Nein	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
Amazon EventBridge Überwachen Sie Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit.	Sie können die gemeinsame Nutzung aller EventBridge Amazon-Events, ehemals Amazon CloudWatch Events, für alle Konten in Ihrer Organisation aktivieren. Weitere Informationen finden Sie unter Senden und Empfangen	 Nein	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	von EventBridge Amazon-Ereignissen zwischen AWS-Konten im EventBridge Amazon-Benutzerhandbuch.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Firewall Manager Zentrale Konfiguration und Verwaltung von Firewall-Regeln für Webanwendungen für alle Konten und Anwendungen.	Sie können AWS WAF Regeln für alle Konten in Ihrer Organisation zentral konfigurieren und verwalten.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
Amazon GuardDuty GuardDuty ist ein Dienst zur kontinuierlichen Sicherheitsüberwachung, der Informationen aus einer Vielzahl von Datenquellen analysiert und verarbeitet. Er verwendet Bedrohungsdaten, ebenso wie Machine Learning, um unerwartete und potenziell nicht autorisierte bösartige Aktivitäten in Ihrer AWS -Umgebung zu identifizieren.	Sie können ein Mitgliedskonto festlegen, das GuardDuty für alle Konten in Ihrer Organisation angezeigt und verwaltet werden soll. Durch das Hinzufügen von Mitgliedskonten werden diese Konten automatisch in den	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	ausgewählten AWS-Region Konten aktiviert GuardDuty. Sie können auch die GuardDuty Aktivierung für neue Konten, die Ihrer Organisation hinzugefügt wurden, automatisieren. Weitere Informationen finden Sie unter GuardDuty			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Organizations im GuardDuty Amazon-Benutzerhandbuch.			
AWS Health Verschaffen Sie sich einen Überblick über Ereignisse, die sich auf die Leistung Ihrer Ressourcen oder auf Probleme mit der Verfügbarkeit von AWS Diensten auswirken könnten.	Sie können AWS Health Ereignisse kontenübergreifend in Ihrer Organisation zusammenfassen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Identity and Access Management Kontrollieren Sie den Zugriff auf AWS Ressourcen sicher.	Mithilfe der Daten zum letzten Servicezugriff in IAM können Sie die AWS -Aktivitäten in Ihrer Organisation besser verstehen. Sie können diese Daten zum Erstellen und Aktualisieren von Service-Kontrollri	 Nein	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	chtlinien (Service Control Policies, SCPs) verwenden, die den Zugriff auf die von den Konten Ihres Unternehmens verwendeten AWS -Services beschränken. Ein Beispiel finden Sie unter Verwenden von Daten zum Optimieren von			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Berechtigungen für eine Organisationseinheit im IAM-Benutzerhandbuch			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
IAM Access Analyzer Analysieren Sie ressourcenbasierte Richtlinien in Ihrer AWS Umgebung, um alle Richtlinien zu identifizieren, die einem Principal Zugriff gewähren, der sich außerhalb Ihrer Vertrauenszone befindet.	Sie können ein Mitgliedskonto als Administrator für IAM Access Analyzer festlegen. Weitere Informationen finden Sie unter Aktivieren von Access Analyzer im IAM-Benutzerhandbuch.	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon Inspector Scannen Sie Ihre AWS Workloads automatisch auf Sicherheitslücken, um Amazon EC2 EC2-Instances und Container-Images, die sich in Amazon ECR befinden, auf Softwareschwachstellen und unbeabsichtigte Netzwerkgefährdung zu erkennen.	Delegieren Sie einen Administrator, um Scans für Mitgliedskonten zu aktivieren oder zu deaktivieren, aggregierte Suchdaten aus der gesamten Organisation anzuzeigen und Unterdrückungsregeln zu erstellen und zu verwalten.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Weitere Informationen finden Sie unter Verwalten mehrerer Konten mit AWS Organizations im Amazon-Inspector-Benutzerhandbuch.			
AWS License Manager Optimierung der Migration von Softwarelizenzen in die Cloud.	Sie können Computing-Ressourcen in Ihrer gesamten Organisation kontoübergreifend entdecken.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon Macie Erkennt und klassifiziert Ihre geschäftskritischen Inhalte mithilfe von Machine Learning. Dies hilft Ihnen, Anforderungen in Bezug auf Datensicherheit und Datenschutz zu erfüllen. Die Lösung evaluiert kontinuierlich die Inhalte, die Sie in Amazon S3 speichern, und benachrichtigt Sie über potenzielle Probleme.	Sie können Amazon Macie für alle Konten in Ihrer Organisation konfigurieren. So erhalten Sie über ein dediziertes Macie-Administratorkonto eine konsolidierte Ansicht aller Daten in allen Amazon-S3-	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Konten. Sie können Macie so konfigurieren, dass Ressourcen in neuen Konten automatisch geschützt werden, wenn Ihre Organisation wächst. Sie erhalten Benachrichtigungen, die Ihnen die Korrektur falsch konfigurierter			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Richtlinien in S3-Buckets in der gesamten Organisation ermöglichen.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Marketplace Ein kuratierter digitaler Katalog, den Sie zum Suchen, Kaufen, Bereitstellen und Verwalten von Drittanbieter-Software verwenden können, die Sie zum Entwickeln von Lösungen und für geschäftliche Abläufe benötigen.	Sie können Lizenzen für Ihre AWS Marketplace Abonnements und Käufe für alle Konten in Ihrer Organisation gemeinsam nutzen.	 Ja Weitere Informationen	 Nein	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Marketplace Privater Marketplace Bietet Ihnen einen breiten Produktkatalog sowie eine detaillierte Steuerung dieser Produkte. AWS Marketplace	Ermöglicht es Ihnen, mehrere private Marketplace-Erlebnisse zu erstellen, die mit Ihrer gesamten Organisation, einer oder mehreren Organisationseinheiten oder einem oder mehreren Konten in Ihrer Organisation verknüpft sind, von	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	denen jedes seinen eigenen Satz zugelassener Produkte hat. Ihre AWS Administratoren können auch jedem privaten Marketplace-Erlebnis ein eigenes Branding mit dem Logo, der Botschaft und dem Farbschema Ihres Unternehmens oder			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Teams zuweisen.			
AWS -Network Manager Ermöglicht Ihnen die zentrale Verwaltung Ihres AWS Cloud WAN-Kernnetzwerks und Ihres AWS Transit Gateway Gateway-Netzwerks über AWS Konten, Regionen und lokale Standorte hinweg.	Sie können Ihre globalen Netzwerke mit Transit-Gateways und den damit verbundenen Ressourcen in mehreren AWS Konten innerhalb Ihrer Organisation zentral verwalten und überwachen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Resource Access Manager Teilen Sie bestimmte AWS Ressourcen, die Sie besitzen, mit anderen Konten.	Sie können Ressourcen innerhalb Ihrer Organisation freigeben, ohne zusätzliche Einladungen auszutauschen. Zu den Ressourcen, die Sie freigeben können, gehören Route-53-Resolver-Regeln, On-Demand-Kapazitä	 Ja Weitere Informationen	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	tsreservierungen und vieles mehr. Informationen zur gemeinsamen Nutzung von Kapazitätsreservierungen finden Sie im Amazon-EC2-Benutzerhandbuch für Linux-Instances oder im Amazon-EC2-Benutzerhandbuch für			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Windows-Instances. Eine Liste der gemeinsam nutzbaren Ressourcen finden Sie unter Gemeinsame Ressourcen im AWS RAM - Benutzerhandbuch.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Ressourcen Explorer Erkunden Sie Ihre Ressourcen mithilfe einer Suche, die sich wie eine Internet-Suchmaschine anfühlt.	Aktivieren Sie das Durchsuchen mehrerer Konten.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Security Hub Sehen Sie sich Ihren Sicherheitsstatus an AWS und überprüfen Sie Ihre Umgebung anhand von Industriestandards und Best Practices.	Sie können den Security Hub automatisch für alle Konten Ihrer Organisation aktivieren, einschließlich neuer Konten, wenn sie hinzugefügt werden. Dadurch wird die Abdeckung für Security-Hub-Überprüfungen	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	und -Erkenntnisse erhöht, was ein genaueres Bild Ihres gesamten Sicherheitszustands ermöglicht.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon-S3-Storage-Lens Erhalten Sie Einblicke in Ihre Amazon-S3-Speichernutzungs- und Aktivitätsmetriken mit umsetzbaren Empfehlungen zur Speicheroptimierung.	Konfigurieren Sie Amazon S3 Storage Lens, um Einblicke in Amazon-S3-Speichernutzungs- und Aktivitätstrends zu erhalten, und Empfehlungen für alle Mitgliedskonten in Ihrer Organisation zu erhalten.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon Security Lake Amazon Security Lake zentralisiert Sicherheitsdaten aus Cloud-, On-Premises- und benutzerdefinierten Quellen in einem Data Lake, der in Ihrem Konto gespeichert ist.	Erstellen Sie einen Data Lake, der Protokolle und Ereignisse in Ihren Konten erfasst.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS Service Catalog Erstellung und Verwaltung von Katalogen mit IT-Services, deren Verwendung in AWS von Ihnen genehmigt wurde.	Sie können leichter kontoübergreifend Portfolien freigeben und Produkte kopieren, ohne Portfolio-IDs freigeben zu müssen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
Service Quotas Anzeige und Verwaltung von Service-Kontingenten, auch als Einschränkungen bezeichnet, von einem zentralen Ort aus.	Sie können eine Kontingent-Anforderungsvorlage erstellen, um automatisch eine Kontingenterhöhung anzufordern, wenn Konten in Ihrer Organisation erstellt werden.	 Ja Weitere Informationen	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
AWS IAM Identity Center Bereitstellung von Single-Sign-On-Zugriff für alle Konten und Cloud-Anwendungen.	Benutzer können sich mit ihren Unternehmensanmeldedaten beim AWS Access Portal anmelden und über ihr zugewiesenes Verwaltungskonto oder ihre Mitgliedskonten auf Ressourcen zugreifen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Systems Manager Sorgen Sie für Transparenz und Kontrolle Ihrer AWS Ressourcen.	Mithilfe des Systems Manager Explorer können Sie Betriebsdaten AWS-Konten in Ihrem gesamten Unternehmen synchronisieren. Sie können Änderungsvorlagen, Genehmigungen und Berichte für alle Mitgliedskonten in Ihrer	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
	Organisation über ein delegiertes Administratorkonto verwalten, indem Sie den Änderungsmanager von Systems Manager verwenden.			

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Tag-Richtlinien Benutzen der Standardisierung von Tags in allen Ressourcen in den Konten Ihrer Organisation.	Sie können Tag-Richtlinien erstellen, um Tagging-Regeln für bestimmte Ressourcen und Ressourcentypen zu definieren, und diese Richtlinien an Organisationseinheiten und Konten anhängen, um diese Regeln durchzusetzen.	 Ja Weitere Informationen	 Nein	

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Trusted Advisor Trusted Advisor untersucht Ihre AWS Umgebung und gibt Empfehlungen, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen.	Trusted Advisor Führt Prüfungen für alle AWS-Konten in Ihrer Organisation durch.	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
AWS Well-Architected Tool Auf AWS Well-Architected Tool diese Weise können Sie den Status Ihrer Workloads dokumentieren und sie mit den neuesten bewährten AWS Architekturpraktiken vergleichen.	Ermöglicht es AWS WA Tool sowohl Kunden als auch Organizations, den Prozess der gemeinsamen Nutzung von AWS WA Tool Ressourcen mit anderen Mitgliedern ihrer Organisation zu vereinfachen.	 Ja Weitere Informationen	 Nein

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator
Amazon VPC IP Address Manager (IPAM) IPAM ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre AWS Workloads zu planen, zu verfolgen und zu überwachen.	Überwachen Sie die IP-Adressverwendung in Ihrer Organisation und teilen Sie IP-Adresspools zwischen den Mitgliedskonten.	 Ja Weitere Informationen	 Ja Weitere Informationen

AWS Dienst	Vorteile der Verwendung mit AWS Organizations	Unterstützt vertrauenswürdigen Zugriff	Unterstützt delegierten Administrator	
Amazon VPC Reachability Analyzer Reachability Analyzer ist ein Tool zur Konfigurationsanalyse, mit dem Sie Konnektivitätstests zwischen einer Quellressource und einer Zielressource in Ihren Virtual Private Clouds (VPCs) durchführen können.	Verfolgen Sie die Pfade zwischen Konten in Ihren Organisationen.	 Ja Weitere Informationen	 Ja Weitere Informationen	

AWS Account Management und AWS Organizations

AWS Account Management hilft Ihnen, die Kontoinformationen und Metadaten für alle AWS-Konten in Ihrer Organisation zu verwalten. Sie können die alternativen Kontaktinformationen für jedes Mitgliedskonto Ihrer Organisation festlegen, ändern oder löschen. Weitere Informationen finden Sie

unter Nutzen eines AWS Account Management in Ihrer Organisation im AWS Account Management-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Account Management mit AWS Organizations zu integrieren.

So aktivieren Sie den vertrauenswürdigen Zugriff mit Audit Management

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Audit Management erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Account Management, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Account Management, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Account Management als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

So deaktivieren Sie den vertrauenswürdigen Zugriff mit Audit Management

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit AWS Account Management deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Suchen Sie auf der Seite Services die Zeile für AWS Account Management und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Account Management mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Account Management als vertrauenswürdigen Service für Organizations zu deaktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

So aktivieren Sie ein delegiertes Administratorkonto für Audit Management

Wenn Sie ein Mitgliedskonto als delegierter Administrator für die Organisation festlegen, können Benutzer und Rollen des angegebenen Kontos die AWS-Konto-Metadaten für andere Mitgliedskonten in der Organisation verwalten. Wenn Sie ein delegiertes Administratorkonto nicht aktivieren, können diese Aufgaben nur vom Verwaltungskonto der Organisation ausgeführt werden. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung Ihrer Kontodetails zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für die Kontoverwaltung in der Organisation konfigurieren.

Weitere Informationen zur Konfiguration einer Delegierungsrichtlinie finden Sie unter Erstellen oder Aktualisieren einer ressourcenbasierten Delegierungsrichtlinie.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

AWS Application Migration Service (MGN) und AWS Organizations

AWS Application Migration Service vereinfacht und beschleunigt die Migration von Anwendungen zu AWS und senkt die Kosten dafür. Durch die Integration in Organizations können Sie große Migrationen für mehrere Konten in der globalen Ansicht verwalten. Weitere Informationen finden Sie unter Einrichten von AWS Organizations im MGN-Benutzerhandbuch.

Ziehen Sie die folgenden Informationen zurate, um AWS Application Migration Service in AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann MGN unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in der Organisation ausführen.

Diese Rolle können Sie nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen MGN und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForApplicationMigrationService`

Von MGN verwendete Service-Prinzipale

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von MGN verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Service-Prinzipale:

- `mgn.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit MGN

Wenn Sie den vertrauenswürdigen Zugriff mit MGN aktivieren, können Sie in der globalen Ansicht große Migrationen für mehrere Konten verwalten. Die globale Ansicht bietet Transparenz und die Möglichkeit, bestimmte Aktionen für Quellserver, Apps und Wellen in verschiedenen AWS-Konten auszuführen. Weitere Informationen finden Sie unter Einrichten der AWS-Organisationen im Benutzerhandbuch von AWS Application Migration Service.

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Den vertrauenswürdigen Zugriff können Sie entweder über die Konsole von AWS Application Migration Service oder die Konsole von AWS Organizations aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die Konsole oder die Tools von AWS Application Migration Service verwenden, um die Integration in Organizations zu aktivieren. Auf diese Weise kann AWS Application Migration Service erforderliche Konfigurationen ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den Tools von AWS Application Migration Service aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der Konsole oder der Tools von AWS Application Migration Service aktivieren, müssen Sie diese Schritte nicht ausführen.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services nach der Zeile für AWS Application Migration Service. Wählen Sie den Namen des Service und dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Application Migration Service mit, dass er diesen Service jetzt für die Zusammenarbeit mit AWS Organizations über die zugehörige Konsole aktivieren kann.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Application Migration Service als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit MGN

Nur ein Administrator im Verwaltungskonto von Organizations kann den vertrauenswürdigen Zugriff mit MGN deaktivieren.

Den vertrauenswürdigen Zugriff können Sie entweder mit dem AWS Application Migration Service oder den Tools von AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die Konsole oder die Tools von AWS Application Migration Service verwenden, um die Integration in Organizations zu deaktivieren. Auf diese Weise kann AWS Application Migration Service die erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den Tools von AWS Application Migration Service deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der Konsole oder der Tools von AWS Application Migration Service deaktivieren, müssen Sie diese Schritte nicht ausführen.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services nach der Zeile für AWS Application Migration Service und wählen Sie dann den Namen des Service aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Application Migration Service mit, dass er diesen Service jetzt über die zugehörige

Konsole oder mit den zugehörigen Tools für die Zusammenarbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Application Migration Service als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines Kontos für einen delegierten Administrator für MGN

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos Verwaltungsaktionen für MGN ausführen, die ansonsten nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von MGN zu trennen. Weitere Informationen finden Sie unter Einrichten von AWS Organizations im MGN-Benutzerhandbuch.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Verwaltungskonto von Organizations kann ein Mitgliedskonto als delegierten Administrator für MGN in der Organisation konfigurieren.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator`und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontodienst `mgn.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für MGN

Nur ein Administrator im Verwaltungskonto von Organizations kann einen delegierten Administrator für MGN entfernen. Den delegierten Administrator können Sie mithilfe des CLI- oder SDK-Vorgangs `DeregisterDelegatedAdministrator` von Organizations entfernen.

AWS Artifact und AWS Organizations

AWS Artifact ist ein Service, mit dem Sie AWS-Sicherheits-Compliance-Berichte herunterladen können, z. B. ISO- und PCI-Berichte. Durch die Verwendung von AWS Artifact kann ein Benutzer in einem Verwaltungskonto der Organisation automatisch Vereinbarungen für alle Mitgliedskonten in einer Organisation akzeptieren, auch wenn neue Berichte und Konten hinzugefügt werden. Benutzer von Mitgliedskonten können Vereinbarungen anzeigen und herunterladen. Weitere Informationen finden Sie unter Verwalten einer Vereinbarung für mehrere Konten in AWS Artifact im AWS Artifact-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Artifact mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS Artifact unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS Artifact und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

Obwohl Sie diese Rolle löschen oder ändern können, wenn Sie das Mitgliedskonto aus der Organisation entfernen, empfehlen wir es nicht.

Es wird davon abgeraten, die Rolle zu ändern, da dies zu Sicherheitsproblemen wie dem dienstübergreifenden verwirrten Stellvertreter führen kann. Weitere Informationen zum Schutz vor verwirrten Stellvertreter finden Sie unter Dienstübergreifende stellvertretende Prävention im AWS Artifact-Benutzerhandbuch.

- `AWSServiceRoleForArtifact`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS Artifact verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `artifact.amazonaws.com`

Den vertrauenswürdigen Zugriff mit AWS Artifact aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Artifact, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.

4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Artifact, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Artifact als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Artifact

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit AWS Artifact deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

AWS Artifact erfordert vertrauenswürdigen Zugriff mit AWS Organizations, um mit Organisationsvereinbarungen zu funktionieren. Wenn Sie vertrauenswürdigen Zugriff mithilfe von AWS Organizations deaktivieren, während Sie AWS Artifact für Organisationsvereinbarungen verwenden, funktioniert es nicht mehr, da es nicht mehr auf die Organisation zugreifen kann. Alle Organisationsvereinbarungen, die Sie in AWS Artifact akzeptieren, bleiben erhalten, jedoch ist der Zugriff über AWS Artifact nicht möglich. Die AWS Artifact-Rolle, die AWS Artifact erstellt, bleibt

erhalten. Wenn Sie den vertrauenswürdigen Zugriff dann wieder aktivieren, funktioniert AWS Artifact wie vorher, ohne dass der Service neu konfiguriert werden muss.

Ein eigenständiges Konto, das aus einer Organisation entfernt wurde, hat keinen Zugriff mehr auf Organisationsvereinbarungen.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Artifact und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Artifact mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Artifact als vertrauenswürdigen Service für Organizations zu deaktivieren.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal artifact.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für AWS Artifact

Weitere Informationen zum Aktivieren eines delegierten Administrators für AWS Artifact finden Sie unter AWS Artifact.

AWS Audit Manager und AWS Organizations

AWS Audit Manager hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Einhaltung von Branchenstandards zu vereinfachen. Audit Manager automatisiert die Sammlung von Beweisen, um die Bewertung zu erleichtern, ob Ihre Richtlinien, Verfahren und Aktivitäten effektiv funktionieren. Wenn es Zeit für eine Prüfung ist, hilft Audit Manager Ihnen, Stakeholder-Reviews Ihrer Steuerelemente zu verwalten und unterstützt Sie dabei, mit viel weniger manuellen Aufwand revisionsfähige Berichte zu erstellen.

Wenn Sie Audit Manager mit AWS Organizations integrieren, können Sie Beweise aus einer breiteren Quelle sammeln, indem Sie mehrere AWS-Konten aus Ihrer Organisation in Ihre Bewertungen einbeziehen.

Weitere Informationen finden Sie unter AWS-Organisationen aktivieren im Audit-Manager-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Audit Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Audit Manager unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Audit Manager und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

Weitere Informationen zur Verwendung dieser Rolle durch Audit Manager finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Audit Manager-Benutzerhandbuch.

- `AWSServiceRoleForAuditManager`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Audit Manager verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `auditmanager.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit Audit Manager

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Audit Manager erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für Ihre Organisation festlegen können.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Audit Manager-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Audit Manager-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Audit Manager jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Audit Manager bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Audit Manager-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Audit-Manager-Konsole

Anweisungen zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Einrichten im AWS Audit Manager-Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen delegierten Administrator mit der AWS Audit Manager-Konsole konfigurieren, aktiviert AWS Audit Manager automatisch den vertrauenswürdigen Zugriff für Sie.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Audit Manager als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

So deaktivieren Sie den vertrauenswürdigen Zugriff mit dem Audit Manager

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit AWS Audit Manager deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Audit Manager als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

So aktivieren Sie ein delegiertes Administratorkonto für Audit Manager

Wenn Sie ein Mitgliedskonto als delegierter Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Audit Manager ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung des Audit Manager zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto mit der folgenden Berechtigung kann ein Mitgliedskonto als delegierter Administrator für Audit Manager in der Organisation konfigurieren:
> `audit-manager:RegisterAccount`

Anweisungen zum Aktivieren eines delegierten Administratorkontos für Audit Manager finden Sie unter Einrichten im AWS Audit Manager-Benutzerhandbuch.

Wenn Sie einen delegierten Administrator mit der AWS Audit Manager-Konsole konfigurieren, aktiviert Audit Manager automatisch den vertrauenswürdigen Zugriff für Sie.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- AWS-SDK: Rufen Sie die Operation `RegisterAccount` auf und geben Sie `delegatedAdminAccount` als Parameter an, um das Administratorkonto zu delegieren.

AWS Backup und AWS Organizations

AWS Backup ist ein Service, mit dem Sie die AWS Backup-Aufgaben in Ihrer Organisation verwalten und überwachen können. Wenn Sie sich mit AWS Backup als Benutzer im Verwaltungskonto der Organisation anmelden, können Sie den organisationsweiten Backup-Schutz und die Überwachung aktivieren. Dies hilft Ihnen, Compliance zu erzielen, da mithilfe von Backup-Richtlinien AWS Backup-Pläne zentral auf Ressourcen für alle Konten in Ihrer Organisation angewendet werden. Wenn Sie AWS Backup und AWS Organizations zusammen verwenden, bringt Ihnen dies folgende Vorteile:

Schutz

Sie können den Backup-Richtlinientyp in Ihrer Organisation aktivieren und dann Backup-Richtlinien erstellen, die an den Organisationsstamm, an Organisationseinheiten oder Konten angefügt werden. Eine Backup-Richtlinie kombiniert einen AWS Backup-Plan mit den anderen erforderlichen Details, um den Plan automatisch auf Ihre Konten anzuwenden. Richtlinien, die direkt an ein Konto angefügt sind, werden mit geerbten Richtlinien aus dem Organisationsstamm und allen übergeordneten Organisationseinheiten zusammengeführt, um eine effektive Richtlinie zu erstellen, die für das Konto gilt. Die Richtlinie enthält die ID einer IAM-Rolle, die über Berechtigungen zur Ausführung von AWS Backup auf den Ressourcen in Ihren Konten verfügt. AWS Backup verwendet die IAM-Rolle, um das Backup gemäß dem Backupplan in der effektiven Richtlinie in Ihrem Namen durchzuführen.

Überwachung

Wenn Sie vertrauenswürdigen Zugriff für AWS Backupin Ihrer Organisation aktivieren, können Sie über die AWS Backup-Konsole Details zu den Backup-, Wiederherstellungs- und Kopieraufgaben in den Konten Ihrer Organisation anzeigen. Weitere Informationen finden Sie unter Überwachen Ihrer Backup-Aufträge im AWS Backup-Entwicklerhandbuch.

Weitere Informationen über AWS Backup finden Sie im AWS Backup-Entwicklerleitfaden.

Verwenden Sie die folgenden Informationen, um AWS Backup mit AWS Organizations zu integrieren.

Den vertrauenswürdigen Zugriff mit AWS Backup aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Backup-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Backup-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Backup jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Backup bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Backup-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

Informationen zum Aktivieren des vertrauenswürdigen Zugriffs mit AWS Backup finden Sie unter Aktivieren des Backups in mehreren AWS-Konten im AWS Backup-Entwicklerhandbuch.

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Backup

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

AWS Backup erfordert vertrauenswürdigen Zugriff mit AWS Organizations, um die Überwachung von Backup-, Wiederherstellungs- und Kopieraufgaben über die Konten Ihrer Organisation hinweg zu ermöglichen. Wenn Sie den vertrauenswürdigen Zugriff für AWS Backup deaktivieren, haben Sie nicht mehr die Möglichkeit, Aufgaben außerhalb des aktuellen Kontos anzuzeigen. Die AWS Backup-Rolle, die AWS Backup erstellt, bleibt erhalten. Wenn Sie den vertrauenswürdigen Zugriff später wieder aktivieren, funktioniert AWS Backup weiter wie vorher, ohne dass der Service neu konfiguriert werden muss.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Backup als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für AWS Backup

Weitere Informationen finden Sie im Entwicklerhandbuch zu AWS Backup unter Delegierter Administrator.

AWS CloudFormation StackSets und AWS Organizations

Mithilfe von AWS CloudFormation StackSets können Sie in einer einzigen Operation Stacks in mehreren AWS-Konten und AWS-Regionen erstellen, aktualisieren oder löschen. Durch die

StackSets-Integration mit AWS Organizations können Sie Stack-Sets mit serviceverwalteten Berechtigungen erstellen, indem Sie eine serviceverknüpfte Rolle verwenden, die in jedem Mitgliedskonto über die entsprechende Berechtigung verfügt. Auf diese Weise können Sie Stack-Instances für Mitgliedskonten in Ihrer Organisation bereitstellen. Sie müssen die erforderlichen AWS Identity and Access Management-Rollen nicht erstellen; StackSets erstellt die IAM-Rolle in jedem Mitgliedskonto in Ihrem Namen.

Sie können auch automatische Bereitstellungen für Konten aktivieren, die Ihrer Organisation in der Zukunft hinzugefügt werden. Wenn die automatische Bereitstellung aktiviert ist, werden Rollen und die Bereitstellung der zugehörigen Stackset-Instances automatisch zu allen Konten hinzugefügt, die dieser OU zukünftig hinzugefügt werden.

Wenn vertrauenswürdiger Zugriff zwischen StackSets und Organizations aktiviert ist, verfügt das Verwaltungskonto über Berechtigungen zum Erstellen und Verwalten von Stack-Sets für Ihre Organisation. Das Verwaltungskonto kann bis zu fünf Mitgliedskonten als delegierte Administratoren registrieren. Wenn vertrauenswürdiger Zugriff aktiviert ist, haben delegierte Administratoren auch Berechtigungen zum Erstellen und Verwalten von Stack-Sets für Ihre Organisation. StackSets mit vom Service verwalteten Berechtigungen werden im Verwaltungskonto erstellt, einschließlich StackSets, die von delegierten Administratoren erstellt werden.

> **Important**
>
> Delegierte Administratoren haben volle Berechtigungen für die Bereitstellung auf Konten Ihrer Organisation. Das Verwaltungskonto kann delegierte Administratorberechtigungen nicht auf die Bereitstellung auf bestimmten Organisationseinheiten oder die Durchführung bestimmter Operationen für Stack-Sets beschränken.

Weitere Informationen zum Integrieren von StackSets in Organizations finden Sie unter Arbeiten mit AWS CloudFormation StackSets im AWS CloudFormation-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS CloudFormation-StackSets mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS

CloudFormation-Stacksets unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS CloudFormation-Stacksets und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- Verwaltungskonto: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Um die serviceverknüpfte Rolle `AWSServiceRoleForCloudFormationStackSetsOrgMember` für die Mitgliedskonten in Ihrer Organisation zu erstellen, müssen Sie zunächst einen Stack-Satz im Managementkonto erstellen. Dies erstellt eine Stack-Satz-Instance, die dann die Rolle in den Mitgliedskonten erstellt.

- Mitgliedskonten: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Weitere Einzelheiten zum Erstellen von Stack-Sätzen finden Sie unter Arbeiten mit AWS-CloudFormation-StackSets im AWS CloudFormation-Benutzerhandbuch.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS CloudFormation-Stacksets verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- Verwaltungskonto: `stacksets.cloudformation.amazonaws.com`

  Sie können diese Rolle nur ändern oder löschen, wenn Sie den vertrauenswürdigen Zugriff zwischen StackSets und Organizations deaktiviert haben.
- Mitgliedskonten: `member.org.stacksets.cloudformation.amazonaws.com`

  Sie können diese Rolle nur dann aus einem Konto ändern oder löschen, wenn Sie zuerst den vertrauenswürdigen Zugriff zwischen StackSets und Organizations deaktivieren oder das Konto zuerst aus der Zielorganisation oder Organisationseinheit (OU) entfernen.

Aktivieren Sie den vertrauenswürdigen Zugriff mit AWS CloudFormation-Stack-Sets

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im Organizations-Verwaltungskonto verfügt über Berechtigungen zum Aktivieren des vertrauenswürdigen Zugriffs mit einem anderen AWS-Service. Sie können den vertrauenswürdigen Zugriff entweder über die AWS CloudFormation-Konsole oder über die Organizations-Konsole aktivieren.

Sie können den vertrauenswürdigen Zugriff nur mit AWS CloudFormation-StackSets aktivieren.

Informationen zum Aktivieren des vertrauenswürdigen Zugriffs über die AWS CloudFormation-Stacksets-Konsole finden Sie unter Aktivieren von vertrauenswürdigem Zugriff mit AWS Organizations im AWS CloudFormation-Benutzerhandbuch.

Deaktivieren Sie den vertrauenswürdigen Zugriff mit AWS CloudFormation-Stack-Sets

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im Organizations-Verwaltungskonto verfügt über Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs mit einem anderen AWS-Service. Sie können den vertrauenswürdigen Zugriff nur über die Organizations-Konsole deaktivieren. Wenn Sie den vertrauenswürdigen Zugriff mit Organizations deaktivieren, während Sie StackSets verwenden, werden alle zuvor erstellten Stack-Instances beibehalten. Stack-Sets, die mit den Berechtigungen der serviceverknüpften Rolle bereitgestellt werden, können jedoch keine Bereitstellungen mehr für Konten ausführen, die von Organizations verwaltet werden.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS CloudFormation-Konsole oder über die Organizations-Konsole deaktivieren.

> **Important**
>
> Wenn Sie vertrauenswürdigen Zugriff programmgesteuert deaktivieren (z. B. mit AWS CLI oder mit einer API), beachten Sie, dass dadurch die Berechtigung entzogen wird. Es ist besser, den vertrauenswürdigen Zugriff mit der AWS CloudFormation-Konsole zu deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS CloudFormation-StackSets und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS CloudFormation-StackSets mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS CloudFormation-StackSets als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für AWS CloudFormation-Stacksets

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos Verwaltungsaktionen für AWS CloudFormation Stacksets ausführen, die ansonsten nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von AWS CloudFormation Stacksets zu trennen.

Anweisungen zum Festlegen eines Mitgliedskontos als delegierter Administrator von AWS CloudFormation Stacksets in der Organisation finden Sie unter Registrieren eines delegierten Administrators im AWS CloudFormation-Benutzerhandbuch.

AWS CloudTrail und AWS Organizations

AWS CloudTrail ist ein - AWS Service, der Ihnen hilft, Governance, Compliance sowie Betriebs- und Risikoprüfungen Ihres zu ermöglichen AWS-Konto. Mit kann AWS CloudTrailein Benutzer in einem Verwaltungskonto einen Organisations-Trail erstellen, der alle Ereignisse für alle AWS-Konten in dieser Organisation protokolliert. Organisations-Trails werden automatisch auf alle Mitgliedskonten in der Organisation angewendet. Mitgliedskonten können den Organisations-Trail sehen, diesen aber weder ändern noch löschen. Standardmäßig haben Mitgliedskonten keinen Zugriff auf die Protokolldateien für den Organisations-Trail im Amazon-S3-Bucket. So können Sie Ihre Ereignisprotokollstrategie einheitlich auf die Konten in Ihrer Organisation anwenden und durchsetzen.

Weitere Informationen finden Sie unter Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um die Integration AWS CloudTrail mit zu erleichtern AWS Organizations.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation CloudTrail ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen CloudTrail und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForCloudTrail`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von verwendeten serviceverknüpften Rollen CloudTrail gewähren Zugriff auf die folgenden Serviceprinzipale:

- `cloudtrail.amazonaws.com`

Den vertrauenswürdigen Zugriff mit CloudTrail aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Trail von der AWS CloudTrail Konsole aus erstellen, wird der vertrauenswürdige Zugriff automatisch für Sie konfiguriert (empfohlen). Sie können den vertrauenswürdigen Zugriff auch über die AWS Organizations Konsole aktivieren. Sie müssen sich mit Ihrem AWS Organizations Verwaltungskonto anmelden, um einen Organisations-Trail zu erstellen.

Wenn Sie einen Organisations-Trail mit der AWS CLI oder der AWS -API erstellen möchten, müssen Sie den vertrauenswürdigen Zugriff manuell konfigurieren. Weitere Informationen finden Sie unter Aktivieren von CloudTrail als vertrauenswürdigen Service in AWS Organizations im AWS CloudTrail -Benutzerhandbuch.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS CloudTrail Konsole oder Tools verwenden, um die Integration mit Organizations zu ermöglichen.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations- AWS CLI Befehl ausführen oder eine Organizations-API-Operation in einem der AWS SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS CloudTrail als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS API: AktivierenAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit CloudTrail

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

AWS CloudTrail erfordert vertrauenswürdigen Zugriff mit AWS Organizations , um mit Organisations-Trails und Ereignisdatenspeichern der Organisation zu arbeiten. Wenn Sie den vertrauenswürdigen Zugriff mit AWS Organizations deaktivieren, während Sie verwenden AWS CloudTrail, werden alle Organisations-Trails für Mitgliedskonten gelöscht, da nicht auf die Organisation zugreifen CloudTrail kann. Alle Verwaltungskonto-Organisations-Trails und Ereignisdatenspeicher der Organisation werden in Trails und Ereignisdatenspeicher auf Kontoebene konvertiert. Die für die Integration zwischen CloudTrail und erstellte `AWSServiceRoleForCloudTrail` Rolle AWS Organizations bleibt im Konto. Wenn Sie den vertrauenswürdigen Zugriff erneut aktivieren, CloudTrail ergreift keine Maßnahmen für vorhandene Trails und Ereignisdatenspeicher. Das Verwaltungskonto muss alle Trails und Ereignisdatenspeicher auf Kontoebene aktualisieren, um sie auf die Organisation anzuwenden.

Gehen Sie wie folgt vor, um einen Trail oder Ereignisdatenspeicher auf Kontoebene in einen Trail oder Ereignisdatenspeicher einer Organisation zu konvertieren:

- Aktualisieren Sie in der CloudTrail Konsole den Trail oder Ereignisdatenspeicher und wählen Sie die Option Für alle Konten in meiner Organisation aktivieren aus.
- Führen Sie in der die folgenden AWS CLISchritte aus:
  - Um einen Trail zu aktualisieren, führen Sie den update-trail Befehl aus und fügen Sie den `--is-organization-trail` Parameter ein.

- Um einen Ereignisdatenspeicher zu aktualisieren, führen Sie den update-event-data-store Befehl aus und fügen Sie den `--organization-enabled` Parameter ein.

Nur ein Administrator im AWS Organizations Verwaltungskonto kann den vertrauenswürdigen Zugriff mit deaktivieren AWS CloudTrail. Sie können den vertrauenswürdigen Zugriff nur mit den Organizations-Tools deaktivieren, indem Sie entweder die AWS Organizations Konsole verwenden, einen Organizations AWS -CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS SDKs aufrufen.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die - AWS Organizations Konsole, einen Organizations- AWS CLI Befehl ausführen oder eine Organizations-API-Operation in einem der AWS SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS CloudTrail und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von sind AWS Organizations, teilen Sie dem Administrator von mit, AWS CloudTrail dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit deaktivieren kann AWS Organizations.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu deaktivieren:

- AWS CLI: disable-aws-service-access

Sie können den folgenden Befehl ausführen, um AWS CloudTrail als vertrauenswürdigen Service für Organizations zu deaktivieren.

```
$ aws organizations disable-aws-service-access \
    --service-principal cloudtrail.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS API: DeaktivierenAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für CloudTrail

Wenn Sie CloudTrail mit Organizations verwenden, können Sie jedes Konto innerhalb der Organisation registrieren, um als CloudTrail delegierter Administrator zu fungieren und die Trails und Ereignisdatenspeicher der Organisation im Namen der Organisation zu verwalten. Ein delegierter Administrator ist ein Mitgliedskonto in einer Organisation, das dieselben administrativen Aufgaben in CloudTrail wie das Verwaltungskonto ausführen kann.

> **Mindestberechtigungen**
>
> Nur ein Administrator im Organizations-Verwaltungskonto kann einen delegierten Administrator für registrieren CloudTrail.

Sie können ein delegiertes Administratorkonto über die CloudTrail Konsole oder mithilfe der Organizations`RegisterDelegatedAdministrator`-CLI- oder SDK-Operation registrieren. Informationen zum Registrieren eines delegierten Administrators über die CloudTrail Konsole finden Sie unter Hinzufügen eines CloudTrail delegierten Administrators.

Deaktivieren eines delegierten Administrators für CloudTrail

Nur ein Administrator im Organizations-Verwaltungskonto kann einen delegierten Administrator für entfernen CloudTrail. Sie können den delegierten Administrator entweder über die CloudTrail Konsole oder mithilfe der Organizations`DeregisterDelegatedAdministrator`-CLI- oder SDK-Operation entfernen. Informationen zum Entfernen eines delegierten Administrators mithilfe der CloudTrail Konsole finden Sie unter Entfernen eines CloudTrail delegierten Administrators.

AWS Compute Optimizer und AWS Organizations

AWS Compute Optimizer ist ein Service, der die Konfigurations- und Auslastungsmetriken Ihrer AWS-Ressourcen analysiert. Ressourcenbeispiele umfassen Instances von Amazon Elastic Compute Cloud (Amazon EC2) und Auto-Scaling-Gruppen. Compute Optimizer berichtet, ob Ihre Ressourcen optimal sind und generiert Optimierungsempfehlungen, um die Kosten zu senken und die Leistung Ihrer Workloads zu verbessern. Weitere Informationen über Compute Optimizer finden Sie im AWS Compute Optimizer-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Compute Optimizer mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Compute Optimizer unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Compute Optimizer und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForComputeOptimizer`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Compute Optimizer verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `compute-optimizer.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Compute Optimizer

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Compute Optimizer-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Compute Optimizer-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Compute Optimizer jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Compute Optimizer bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Compute Optimizer-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Compute-Optimizer-Konsole

Sie müssen sich mit dem Verwaltungskonto Ihrer Organisation an der Compute-Optimizer-Konsole anmelden. Melden Sie sich im Namen Ihrer Organisation an, indem Sie die Anweisungen unter Anmelden für Ihr Konto im AWS Compute Optimizer-Benutzerhandbuch befolgen.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Compute Optimizer, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.

4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Compute Optimizer, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Compute Optimizer als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Compute Optimizer

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit AWS Compute Optimizer deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Compute Optimizer als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Compute Optimizer

Wenn Sie ein Mitgliedskonto als delegierter Administrator für die Organisation festlegen, können Benutzer und Rollen des angegebenen Kontos die AWS-Konto-Metadaten für andere Mitgliedskonten in der Organisation verwalten. Wenn Sie ein delegiertes Administratorkonto nicht aktivieren, können diese Aufgaben nur vom Verwaltungskonto der Organisation ausgeführt werden. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung Ihrer Kontodetails zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Compute Optimizer in der Organisation konfigurieren.

Anweisungen zum Aktivieren eines delegierten Administratorkontos für Compute Optimizer finden Sie unter https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html im AWS Compute Optimizer-Benutzerhandbuch.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administratorkontos für Compute Optimizer

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für Compute Optimizer konfigurieren.

Informationen zum Deaktivieren des delegierten Compute Optimizer-Admin-Kontos mithilfe der Compute Optimizer Optimizer-Konsole finden Sie unter https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html im AWS Compute Optimizer-Benutzerhandbuch.

Informationen zum Entfernen eines delegierten Administrators mithilfe der AWS AWS CLI finden Sie unter deregister-delegated-administrator in der AWS AWS CLI-Befehlsreferenz.

AWS Config und AWS Organizations

Mithilfe der Datenaggregation für mehrere Konten und Regionen in AWS Config können Sie AWS Config-Daten aus mehreren Konten und AWS-Regionen in ein einziges Konto aggregieren. Die Datenaggregation für mehrere Konten und Regionen ist für IT-Administratoren hilfreich, die die Compliance mehrerer AWS-Konten im Unternehmen überwachen. Ein Aggregator ist ein Ressourcentyp in AWS Config, der AWS Config-Daten aus mehreren Quellkonten und -regionen sammelt. Erstellen Sie einen Aggregator in der Region, in der Sie die aggregierten AWS Config-Daten ansehen möchten. Beim Erstellen eines Aggregators können Sie wählen, ob Sie einzelne Konto-IDs oder Ihre Organisation hinzufügen möchten. Weitere Informationen über AWS Config finden Sie im AWS Config-Entwicklerleitfaden.

Sie können auch AWS Config-APIs zum Verwalten von AWS Config-Regeln für alle AWS-Konten in Ihrer Organisation verwenden. Weitere Informationen finden Sie unter Aktivieren von AWS Config-Regeln für alle Konten in Ihrer Organisation im AWS Config-Entwicklerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Config mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird im Konto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS Config unterstützte Vorgänge innerhalb der Konten in Ihrer Organisation ausführen.

- `AWSServiceRoleForConfig`

Diese Rolle wird erstellt, wenn Sie AWS Config in Ihrer Organisation aktivieren, indem Sie einen Aggregator für mehrere Konten erstellen. AWS Config fordert Sie auf, eine Rolle auszuwählen oder zu erstellen und den Namen anzugeben. Es gibt keinen automatisch generierten Namen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS Config und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

Den vertrauenswürdigen Zugriff mit AWS Config aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Config-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Config-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Config jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Config bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Config-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS Config-Konsole

Zum Aktivieren eines vertrauenswürdigen Zugriffs auf AWS Organizations mit AWS Config erstellen Sie einen Multi-Konten-Aggregator und fügen die Organisation hinzu. Weitere Informationen zur

Konfiguration eines Multi-Konten-Aggregators finden Sie unter Einrichten eines Aggregators mithilfe der Konsole im AWS Config-Entwicklerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Config, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Config, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Config als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Config

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Config als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

AWS Cost Optimization Hub und AWS Organizations

AWS Cost Optimization Hub ist eine Funktion für AWS Billing and Cost Management, mit der Sie Empfehlungen zur Kostenoptimierung für Ihre AWS Konten und AWS Regionen konsolidieren und priorisieren können, sodass Sie das Beste aus Ihren AWS Ausgaben herausholen können. Wenn Sie Cost Optimization Hub mit verwenden, können AWS Organizations Sie auf einfache Weise Empfehlungen zur AWS Kostenoptimierung für alle Mitgliedskonten und AWS Regionen Ihrer Organizations identifizieren, filtern und zusammenfassen.

Weitere Informationen finden Sie im AWS Cost Management Benutzerhandbuch unter Cost Optimization Hub.

Verwenden Sie die folgenden Informationen zur Unterstützung bei der Integration AWS Cost Optimization Hub mit AWS Organizations.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Diese Rolle ermöglicht es Cost Optimization Hub, unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation durchzuführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Cost Optimization Hub und Organizations deaktivieren oder wenn Sie das Mitgliedskonto aus der Organisation entfernen.

Weitere Informationen finden Sie im AWS Cost Management Benutzerhandbuch unter Dienstbezogene Rollenberechtigungen für Cost Optimization Hub.

- `AWSServiceRoleForCostOptimizationHub`

Von Cost Optimization Hub verwendete Serviceprinzipale

Cost Optimization Hub verwendet den `cost-optimization-hub.bcm.amazonaws.com` Service Principal.

Aktivierung eines vertrauenswürdigen Zugriffs mit Cost Optimization Hub

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie sich für die Verwendung des Verwaltungskontos Ihrer Organisation entscheiden und alle Mitgliedskonten innerhalb der Organisation einbeziehen, wird der vertrauenswürdige Zugriff für Cost Optimization Hub automatisch in Ihrem Organisationskonto aktiviert.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations Konsole verwenden, einen AWS CLI Befehl ausführen oder eine API-Operation in einem der AWS SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Cost Optimization Hub, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie der Administrator von Only sind AWS Organizations, teilen Sie dem Administrator mit, AWS Cost Optimization Hub dass er diesen Dienst jetzt über die Konsole aktivieren kann, mit AWS Organizations der er arbeiten kann.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Dienstzugriff zu aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um ihn AWS Cost Optimization Hub als vertrauenswürdigen Dienst bei Organizations zu aktivieren.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS API: Aktivieren AWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff auf Cost Optimization Hub deaktivieren, nachdem Sie sich angemeldet haben, verweigert Cost Optimization Hub den Zugriff auf Empfehlungen für die Mitgliedskonten Ihrer Organisation. Darüber hinaus sind die Mitgliedskonten innerhalb der Organisation nicht für Cost Optimization Hub angemeldet. Weitere Informationen finden Sie unter Cost Optimization Hub und vertrauenswürdiger Zugriff für Organizations im AWS Cost Management Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie den AWS CLI Befehl Organizations ausführen oder einen API-Vorgang für Organizations in einem der AWS SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Dienstzugriff zu deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um ihn AWS Cost Optimization Hub als vertrauenswürdigen Dienst bei Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS API: Deaktivieren AWSServiceAccess

AWS Control Tower und AWS Organizations

AWS Control Tower bietet eine einfache Möglichkeit zum Einrichten und Steuern einer AWS-Umgebung mit mehreren Konten, wobei die vorgeschriebenen bewährten Methoden befolgt werden. Die Orchestrierung von AWS Control Tower erweitert die Features von AWS Organizations. AWS

Control Towerwendet präventive und detektivische Kontrollen (sogenannte Leitplanken) an, damit Ihre Organisationen und Konten nicht von den bewährten Methoden abweichen.

Die Orchestrierung von AWS Control Tower erweitert die Features von AWS Organizations.

Weitere Informationen finden Sie im Benutzerhandbuch von AWS Control Tower.

Verwenden Sie die folgenden Informationen, um AWS Control Tower mit AWS Organizations zu integrieren.

Für die Integration benötigte Rollen

Die Rolle `AWSControlTowerExecution` muss in allen angemeldeten Konten vorhanden sein. Damit kann AWS Control Tower einzelne Konten verwalten und Informationen über sie an Ihr Audit- und Ihr Log-Archive-Konto melden.

Weitere Informationen über die von AWS Control Tower verwendeten Rollen finden Sie unter Wie AWS Control Tower-Konten mithilfe von Rollen erstellt und verwaltet und Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Control Tower.

Von AWS Control Tower verwendete Service-Prinzipale

AWS Control Tower verwendet den Service-Prinzipal `controltower.amazonaws.com`.

Den vertrauenswürdigen Zugriff mit AWS Control Tower aktivieren

AWS Control Tower nutzt den vertrauenswürdigen Zugriff, um Abweichungen bei präventiven Kontrollen zu erkennen und Änderungen an Konten und Organisationseinheiten zu verfolgen, die Abweichungen verursachen.

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Um den vertrauenswürdigen Zugriff über die Organizations-Konsole zu aktivieren, wählen Sie **`Enable access`** neben AWS Control Tower.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Control Tower als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Control Tower

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

> **Important**
>
> Wenn Sie den vertrauenswürdigen Zugriff von AWS Control Tower deaktivieren, driftet Ihre AWS Control Tower Landing Zone ab. Die einzige Möglichkeit, das Problem zu beheben, besteht darin, die Reparatur der AWS Control Tower Landing Zone zu verwenden. Durch die erneute Aktivierung des vertrauenswürdigen Zugriffs in Organizations wird das Problem nicht behoben. Weitere Informationen zum Drift finden Sie im AWS Control Tower-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Control Tower als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Amazon Detective und AWS Organizations

Amazon Detective verwendet Ihre Protokolldaten, um Visualisierungen zu generieren, mit denen Sie die Ursache von Sicherheitsbefunden oder verdächtigen Aktivitäten analysieren, untersuchen und identifizieren können.

Mit AWS Organizations können Sie sicherstellen, dass Ihr Detective-Verhaltensdiagramm Einblick in die Aktivitäten für alle Ihre Organisationskonten bietet.

Wenn Sie Detective vertrauenswürdigen Zugriff gewähren, kann der Detective-Dienst automatisch auf Änderungen der Organisationsmitgliedschaft reagieren. Der delegierte Administrator kann jedes Organisationskonto als Mitgliedskonto im Verhaltensdiagramm aktivieren. Detective kann neue Organisationskonten auch automatisch als Mitgliedskonten aktivieren. Organisationskonten können sich nicht vom Verhaltensdiagramm trennen.

Weitere Informationen finden Sie unter Verwenden von Amazon Detective in Ihrer Organisation im Amazon-Detective-Administratorhandbuch.

Verwenden Sie die folgenden Informationen, um Amazon Detective mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Detective unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForDetective`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Detective verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `detective.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit Detective

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

> **Note**
>
> Wenn Sie einen delegierten Administrator für Amazon Detective festlegen, aktiviert Detective automatisch den vertrauenswürdigen Zugriff für Detective in Ihrer Organisation. Detective erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff über die AWS Organizations-Konsole aktivieren.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon Detective, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von Amazon Detective, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

So deaktivieren Sie den vertrauenswürdigen Zugriff mit Detective

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit Amazon Detective deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff über die AWS Organizations-Konsole deaktivieren.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon Detective und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.

4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von Amazon Detective mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

Aktivieren eines delegierten Administratorkontos für Detective

Das delegierte Administratorkonto für Detective ist das Administratorkonto für ein Detective-Verhaltensdiagramm. Der delegierte Administrator bestimmt, welche Organisationskonten als Mitgliedskonten in diesem Verhaltensdiagramm aktiviert und deaktiviert werden sollen. Der delegierte Administrator kann Detective so konfigurieren, dass neue Organisationskonten automatisch als Mitgliedskonten aktiviert werden, wenn sie der Organisation hinzugefügt werden. Informationen darüber, wie ein delegierter Administrator Organisationskonten verwaltet, finden Sie unterVerwalten von Organisationskonten als Mitgliedskonten im Amazon-Detective-Administratorhandbuch.

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für Detective konfigurieren.

Sie können ein delegiertes Administratorkonto über die Detective-Konsole oder API oder mithilfe der Organizations-CLI- oder SDK-Operation angeben.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Detective in der Organisation konfigurieren.

Informationen zum Konfigurieren eines delegierten Administrators mithilfe der Detective-Console oder API finden Sie unter Festlegen eines Detective-Administratorkontos für eine Organisation im Amazon-Detective-Administratorhandbuch.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für Detective

Sie können ein delegiertes Administratorkonto entweder über die Detective-Konsole oder API oder mithilfe der Organizations-`DeregisterDelegatedAdministrator`CLI- oder SDK-Operation entfernen. Weitere Informationen zum Entfernen eines delegierten Administrators mithilfe der Detective-Console oder API, oder der Organizations-API finden Sie unter Festlegen eines Detective-Administratorkontos für eine Organisation im Amazon-Detective-Administratorhandbuch.

Amazon DevOps Guru und AWS Organizations

Amazon DevOps Guru analysiert Betriebsdaten und Anwendungsmetriken und Ereignisse, um Verhaltensweisen zu identifizieren, die von normalen Betriebsmustern abweichen. Benutzer werden benachrichtigt, wenn DevOps Guru ein operatives Problem oder Risiko erkennt.

Die Verwendung von DevOps Guru ermöglicht Multi-Konto-Unterstützung mit AWS Organizations, damit Sie ein Mitgliedskonto festlegen können, um Erkenntnisse in Ihrer gesamten Organisation zu verwalten. Dieser delegierte Administrator kann dann Erkenntnisse aus allen Konten in Ihrer Organisation anzeigen, sortieren und filtern, um eine ganzheitliche Sicht auf den Zustand aller überwachten Anwendungen in Ihrer Organisation zu entwickeln, ohne dass zusätzliche Anpassungen erforderlich sind.

Weitere Informationen finden Sie unter Überwachen Sie Konten in Ihrer gesamten Organisation im Benutzerhandbuch Amazon DevOps Guru.

Verwenden Sie die folgenden Informationen, um Amazon DevOps Guru mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann DevOps Guru unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen DevOps Guru und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForDevOpsGuru`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von DevOps Guru verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `devops-guru.amazonaws.com`

Weitere Informationen finden Sie unter Einrichten von serviceverlinkten Rollen für DevOps Guru im Amazon-DevOps-Guru-Benutzerhandbuch.

So aktivieren Sie den vertrauenswürdigen Zugriff mit DevOps Guru

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

> **Note**
>
> Wenn Sie einen delegierten Administrator für Amazon DevOps Guru festlegen, aktiviert DevOps Guru automatisch den vertrauenswürdigen Zugriff für DevOps Guru in Ihrer Organisation.
> DevOps Guru erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die Amazon-DevOps-Guru-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann Amazon DevOps Guru jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von Amazon DevOps Guru bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Organizations-Konsole oder über die DevOps-Guru-Konsole aktivieren.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon DevOps Guru, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von Amazon DevOps Guru, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

DevOps Guru console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff mit der DevOps Guru-Konsole

1. Melden Sie sich im Verwaltungskonto als Administrator an und öffnen Sie die DevOps Guru-Konsole:Amazon-DevOps-Guru-Konsole
2. Wählen Sie Vertrauenswürdigen Zugriff aktivieren.

So deaktivieren Sie den vertrauenswürdigen Zugriff mit DevOps Guru

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit Amazon DevOps Guru deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff über die AWS Organizations-Konsole deaktivieren.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon DevOps Guru und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von Amazon DevOps Guru mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

Aktivieren eines delegierten Administratorkontos für DevOps Guru

Das delegierte Administratorkonto für DevOps Guru kann die Erkenntnisdaten aller Mitgliedskonten einsehen, die von der Organisation an DevOps Guru übertragen werden. Informationen darüber, wie ein delegierter Administrator Organisationskonten verwaltet, finden Sie unterÜberwachen von Konten in der gesamten Organisation im Amazon-DevOps-Guru-Benutzerhandbuch.

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für DevOps Guru konfigurieren.

Sie können ein delegiertes Administratorkonto über die DevOps-Guru-Konsole oder mithilfe der Organizations-`RegisterDelegatedAdministrator`CLI- oder SDK-Operation angeben.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für DevOps Guru in der Organisation konfigurieren.

DevOps Guru console

So konfigurieren Sie einen delegierten Administrator in der DevOps-Guru-Konsole

1. Melden Sie sich im Verwaltungskonto als Administrator an und öffnen Sie die DevOps Guru-Konsole:Amazon-DevOps-Guru-Konsole
2. Wählen Sie Register delegated administrator (Delegierten Administrator registrieren). Sie können entweder ein Verwaltungskonto oder ein Mitgliedskonto als delegierter Administrator auswählen.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für DevOps Guru

Sie können ein delegiertes Administratorkonto entweder über die DevOps-Guru-Konsole oder mithilfe der Organizations-`DeregisterDelegatedAdministrator`CLI- oder SDK-Operation entfernen. Informationen zum Entfernen eines delegierten Administrators mit der DevOps-Guru-Konsole,

finden Sie unter Überwachen von Konten in der gesamten Organisation im Amazon-DevOps-Guru-Benutzerhandbuch.

AWS Directory Service und AWS Organizations

AWS Directory Service für Microsoft Active Directory, oder AWS Managed Microsoft AD, ermöglicht Ihnen, Microsoft Active Directory (AD) als verwalteten Service auszuführen. AWS Directory Service vereinfacht die Einrichtung und Ausführung von Verzeichnissen in der AWS Cloud sowie die Verbindung der AWS-Ressourcen mit einem bestehenden lokalen Microsoft Active Directory. AWS Managed Microsoft AD ist außerdem eng in AWS Organizations integriert, um eine nahtlose Verzeichnisfreigabe über mehrere AWS-Konten hinweg und in jeder beliebigen VPC in einer Region zu ermöglichen. Weitere Informationen finden Sie im Administrationshandbuch zu AWS Directory Service.

Verwenden Sie die folgenden Informationen, um AWS Directory Service mit AWS Organizations zu integrieren.

Den vertrauenswürdigen Zugriff mit AWS Directory Service aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Directory Service-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Directory Service-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Directory Service jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Directory Service bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Directory Service-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS Directory Service-Konsole

Informationen zum Freigeben eines Verzeichnisses, das automatisch den vertrauenswürdigen Zugriff ermöglicht, finden Sie unter Freigeben Ihres Verzeichnisses im AWS Directory Service-Administrationshandbuch. Schrittweise Anleitungen finden Sie unter Tutorial: Freigeben Ihres AWS-verwalteten Microsoft-AD-Verzeichnisses.

Sie können den vertrauenswürdigen Zugriff über die AWS Organizations-Konsole aktivieren.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Directory Service, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Directory Service, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Directory Service

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie vertrauenswürdigen Zugriff mithilfe von AWS Organizations deaktivieren, während Sie AWS Directory Service verwenden, werden alle zuvor freigegebenen Verzeichnisse weiterhin normal ausgeführt. Sie können jedoch keine neuen Verzeichnisse mehr innerhalb der Organisation freigeben, bis Sie den vertrauenswürdigen Zugriff wieder aktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff über die AWS Organizations-Konsole deaktivieren.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Directory Service und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Directory Service mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS Firewall Manager und AWS Organizations

AWS Firewall Manager ist ein Sicherheitsverwaltungsservice, mit dem Sie Firewall-Regeln und andere Schutzmaßnahmen für alle AWS-Konten und Anwendungen in Ihrem Unternehmen zentral konfigurieren und verwalten. Mit Firewall Manager können Sie AWS WAF-Regeln ausrollen, AWS Shield Advanced-Schutzmaßnahmen erstellen, Amazon-Virtual-Private-Cloud-(Amazon-VPC)-Sicherheitsgruppen konfigurieren und prüfen und AWS Network Firewall bereitstellen. Mit Firewall Manager müssen Sie Ihren Schutz nur einmal einrichten. Diese werden dann automatisch auf alle Konten und Ressourcen in Ihrer Organisation angewendet. Dies gilt auch für neu hinzugefügte Ressourcen und Konten. Weitere Informationen über AWS Firewall Manager finden Sie im AWS Firewall Manager-Entwicklerleitfaden.

Verwenden Sie die folgenden Informationen, um AWS Firewall Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Firewall Manager unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Firewall Manager und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForFMS`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Firewall Manager verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `fms.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Firewall Manager

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Firewall Manager-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Firewall Manager-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Firewall Manager jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Firewall Manager bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Firewall Manager-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

Sie müssen sich mit Ihrem AWS Organizations-Verwaltungskonto anmelden und ein Konto innerhalb der Organisation als AWS Firewall Manager-Administratorkonto konfigurieren. Weitere Informationen

finden Sie unter Festlegen des AWS Firewall Manager-Administratorkontos im AWS Firewall Manager-Entwicklerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Firewall Manager, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Firewall Manager, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Firewall Manager als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Firewall Manager

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Firewall Manager oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Firewall Manager-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Firewall Manager alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Firewall Manager bereitgestellten Tools deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Firewall Manager-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die Firewall-Manager-Konsole

Sie können das AWS Firewall Manager-Administratorkonto ändern oder widerrufen. Befolgen Sie hierzu die Anweisungen unter Zuweisen eines anderen Kontos als das AWS Firewall Manager-Administratorkonto im AWS Firewall Manager-Entwicklerhandbuch.

Wenn Sie das Administratorkonto auflösen, müssen Sie sich beim AWS Organizations-Verwaltungskonto anmelden und ein neues Administratorkonto für AWS Firewall Manager einrichten.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Firewall Manager und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Firewall Manager mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Firewall Manager als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Firewall Manager

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Firewall Manager ausführen, die

andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung des Firewall Manager zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Firewall Manager in der Organisation konfigurieren.

Anweisungen zum Festlegen eines Mitgliedskontos als Firewall-Manager-Administrator für die Organisation finden Sie unter Festlegen des AWS Firewall Manager-Administratorkontos im AWS Firewall Manager-Entwicklerhandbuch.

Amazon GuardDuty und AWS Organizations

Amazon GuardDuty ist ein kontinuierlicher Sicherheitsüberwachungsservice, der eine Vielzahl von Datenquellen analysiert und verarbeitet, indem er Bedrohungsdaten-Feeds und Machine Learning verwendet, um unerwartete und potenziell nicht autorisierte und böswillige Aktivitäten in Ihrer AWS-Umgebung zu identifizieren. Beispiele dafür sind Berechtigungseskalationen, die Verwendung kompromittierter Anmeldeinformationen, die Kommunikation mit schädlichen IP-Adressen, URLs und Domänen oder das Vorhandensein von Malware auf Instances von Amazon Elastic Compute Cloud und in Container-Workloads.

Sie können die Verwaltung von GuardDuty vereinfachen, indem Sie Organizations verwenden, um GuardDuty für alle Konten in Ihrer Organisation zu verwalten.

Weitere Informationen finden Sie unter Verwalten von GuardDuty-Konten mit AWS Organizations im Amazon-GuardDuty-Benutzerhandbuch

Verwenden Sie die folgenden Informationen, um Amazon GuardDuty mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgenden serviceverknüpften Rollen werden automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit diesen Rollen kann GuardDuty unterstützte Vorgänge innerhalb der Konten in Ihrer Organisation ausführen. Rollen können Sie

nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen GuardDuty und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- Die serviceverknüpfte Rolle `AWSServiceRoleForAmazonGuardDuty` wird automatisch in Konten erstellt, bei denen GuardDuty mit Organizations integriert ist. Weitere Informationen finden Sie unter Verwalten von GuardDuty-Konten mit Organizations im Benutzerhandbuch von Amazon GuardDuty.
- Die serviceverknüpfte Rolle `AmazonGuardDutyMalwareProtectionServiceRolePolicy` wird automatisch in Konten erstellt, bei denen der Malware-Schutz von GuardDuty aktiviert ist. Weitere Informationen finden Sie unter Berechtigungen von serviceverknüpften Rollen für den Malware-Schutz von GuardDuty im Benutzerhandbuch von Amazon GuardDuty.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

- `guardduty.amazonaws.com`, verwendet von der serviceverknüpften Rolle `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, verwendet von der serviceverknüpften Rolle `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Den vertrauenswürdigen Zugriff mit GuardDuty aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur mit Amazon GuardDuty aktivieren.

Amazon GuardDuty erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als GuardDuty-Administrator für Ihre Organisation festlegen können. Wenn Sie einen delegierten Administrator mit der GuardDuty-Konsole konfigurieren, aktiviert GuardDuty automatisch den vertrauenswürdigen Zugriff für Sie.

Wenn Sie jedoch ein delegiertes Administratorkonto mit AWS CLI oder einem der AWS-SDKs konfigurieren möchten, müssen Sie die Operation EnableAWSServiceAccess explizit aufrufen und den Serviceprinzipal als Parameter angeben. Rufen Sie die Seite EnableOrganizationAdminAccount auf, um das GuardDuty-Administratorkonto zu delegieren.

Deaktivieren Sie den vertrauenswürdigen Zugriff mit GuardDuty

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon GuardDuty als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für GuardDuty

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für GuardDuty ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von GuardDuty zu trennen.

Mindestberechtigungen

Informationen zu den Berechtigungen, die erforderlich sind, um ein Mitgliedskonto als delegierten Administrator zu bestimmen, finden Sie unter Erforderliche Berechtigungen zur Benennung eines delegierten Administrators im Amazon-GuardDuty-Benutzerhandbuch

So weisen Sie ein Mitgliedskonto als delegierten Administrator für GuardDuty an

Siehe Bestimmen eines delegierten Administrators und Hinzufügen von Mitgliedskonten (Konsole) und Bestimmen eines delegierten Administrators und Hinzufügen von Mitgliedskonten (API)

AWS Health und AWS Organizations

AWS Health bietet fortlaufenden Einblick in Ihre Ressourcenleistung und die Verfügbarkeit Ihrer AWS-Services und Konten. AWS Health liefert Ereignisse, wenn Ihre AWS-Ressourcen und Services von einem Problem betroffen sind oder von bevorstehenden Änderungen betroffen sind. Nachdem Sie die Organisationsansicht aktiviert haben, kann ein Benutzer im Verwaltungskonto der Organisation AWS Health Ereignisse für alle Konten in der Organisation zusammenfassen. In der Organisationsansicht werden nur AWS Health Ereignisse angezeigt, die nach der Aktivierung der Funktion geliefert wurden und behält sie 90 Tage lang bei.

Sie können die Organisationsansicht mithilfe der AWS Health-Konsole, der AWS Command Line Interface (AWS CLI) oder der AWS Health-API aktivieren.

Weitere Informationen finden Sie unter Aggregieren von AWS Health-Ereignissen im AWS Health-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Health mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS Health unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS Health und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForHealth_Organizations`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS Health verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `health.amazonaws.com`

Den vertrauenswürdigen Zugriff mit AWS Health aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie die Funktion „Organisationsansicht“ für AWS Health aktivieren, wird der vertrauenswürdige Zugriff auch automatisch für Sie aktiviert.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Health-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Health-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Health jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Health bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Health-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS Health-Konsole

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie AWS Health und eine der folgenden Optionen verwenden:

- Verwendung der AWS Health-Konsole. Weitere Informationen finden Sie unter Organisationsansicht (Konsole) im AWS Health-Benutzerhandbuch.
- Verwenden Sie die AWS CLI. Weitere Informationen finden Sie unter Organisationsansicht (CLI) im AWS Health-Benutzerhandbuch.
- Rufen Sie die EnableHealthServiceAccessForOrganization-API-Operation auf.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Health als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Health

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nachdem Sie die Organisationsansichtsfunktion deaktiviert haben, beendet AWS Health die Aggregation von Ereignissen für alle anderen Konten in Ihrer Organisation. Dadurch wird auch der vertrauenswürdige Zugriff für Sie automatisch deaktiviert.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Health oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Health-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Health alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Health bereitgestellten Tools deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Health-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die AWS Health-Konsole

Sie können den vertrauenswürdigen Zugriff über eine der folgenden Optionen deaktivieren:

- Verwendung der AWS Health-Konsole. Weitere Informationen finden Sie unter Organisationsansicht deaktivieren (Konsole) im AWS Health-Benutzerhandbuch.
- Verwenden Sie die AWS CLI. Weitere Informationen finden Sie unter Organisationsansicht deaktivieren (CLI) im AWS Health-Benutzerhandbuch.
- Rufen Sie die DisableHealthServiceAccessForOrganization-API-Operation auf.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Health als vertrauenswürdigen Service für Organizations zu deaktivieren.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal health.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für AWS Health

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos Verwaltungsaktionen für AWS Health ausführen, die ansonsten nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von AWS Health zu trennen.

So weisen Sie ein Mitgliedskonto als delegierten Administrator für AWS Health an

Siehe Registrieren eines delegierten Administrators für Ihre Organisationsansicht

So registrieren Sie einen delegierten Administrator für AWS Health

Siehe Entfernen eines delegierten Administrators von Ihrer Organisationsansicht

Amazon Inspector und AWS Organizations

Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der Amazon EC2 und Container-Workloads kontinuierlich auf Softwareschwachstellen und unbeabsichtigte Netzwerkfreigabe durchsucht.

Mit Amazon Inspector können Sie mehrere Konten verwalten, die über AWS Organizations verknüpft sind, indem Sie einfach ein Administratorkonto für Amazon Inspector delegieren. Der delegierte Administrator verwaltet Amazon Inspector für die Organisation und erhält spezielle Berechtigungen zur Ausführung von Aufgaben im Auftrag Ihrer Organisation wie:

- Aktivieren oder Deaktivieren von Scans nach Mitgliedskonten
- Anzeigen aggregierter Suchdaten aus der gesamten Organisation
- Unterdrückungsregeln erstellen und verwalten

Weitere Informationen finden Sie unter Verwalten mehrerer Konten mit AWS Organizations im Amazon-Inspector-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Amazon Inspector mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Amazon Inspector unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Amazon Inspector und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForAmazonInspector2`

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon Inspector im Benutzerhandbuch für Amazon Inspector.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Amazon Inspector verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `inspector2.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit Amazon Inspector

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Amazon Inspector erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

Wenn Sie einen delegierten Administrator für Amazon Inspector festlegen, aktiviert Amazon Inspector automatisch den vertrauenswürdigen Zugriff für Amazon Inspector in Ihrer Organisation.

Wenn Sie jedoch ein delegiertes Administratorkonto mit AWS-CLI oder einem der AWS-SDKs konfigurieren möchten, müssen Sie die Operation `EnableAWSServiceAccess` explizit aufrufen und den Serviceprinzipal als Parameter angeben. Dann kannst du `EnableDelegatedAdminAccount` anrufen, um das Inspector-Administratorkonto zu delegieren.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon Inspector als vertrauenswürdigen Service für Organizations zu aktivieren.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

> **Note**
>
> Wenn Sie das `EnableAWSServiceAccess`-API verwenden, müssen Sie auch `EnableDelegatedAdminAccount` anrufen, um das Inspector-Administratorkonto zu delegieren.

So deaktivieren Sie den vertrauenswürdigen Zugriff mit Amazon Inspector

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit Amazon Inspector deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon Inspector als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Amazon Inspector

Mit Amazon Inspector können Sie mehrere Konten in einer Organisation mit einem delegierten Administrator mit AWS Organizations-Service verwalten.

Das AWS Organizations-Verwaltungskonto bezeichnet ein Konto innerhalb der Organisation als delegiertes Administratorkonto für Amazon Inspector. Der delegierte Administrator verwaltet Amazon Inspector für die Organisation und erhält spezielle Berechtigungen zum Ausführen von Aufgaben im Auftrag Ihrer Organisation, z. B.: Aktivieren oder Deaktivieren von Scans für Mitgliedskonten, Anzeigen aggregierter Suchdaten aus der gesamten Organisation sowie Erstellen und Verwalten von Unterdrückungsregeln

Informationen darüber, wie ein delegierter Administrator Organisationskonten verwaltet, finden Sie unter Die Beziehung zwischen Administrator- und Mitgliedskonten verstehen im Amazon-Inspector-Benutzerhandbuch.

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für Amazon Inspector konfigurieren.

Sie können ein delegiertes Administratorkonto über die Amazon-Inspector-Konsole oder API oder mithilfe der Organizations-CLI- oder SDK-Operation angeben.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Amazon Inspector in der Organisation konfigurieren.

Informationen zum Konfigurieren eines delegierten Administrators über die Amazon-Inspector-Konsole finden Sie unter Schritt 1: Amazon Inspector aktivieren – Umgebung für mehrere Konten im Amazon-Inspector-Benutzerhandbuch.

> **Note**
>
> Sie müssen in jeder Region, in der Sie Amazon Inspector verwenden, `inspector2:enableDelegatedAdminAccount` anrufen.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für Amazon Inspector

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann ein delegiertes Administratorkonto aus der Organisation entfernen.

Sie können ein delegiertes Administratorkonto entweder über die Amazon-Inspector-Konsole oder API oder mithilfe der Organizations-`DeregisterDelegatedAdministrator`CLI- oder SDK-Operation entfernen. Informationen zum Entfernen eines delegierten Administrators über die Amazon-Inspector-Konsole finden Sie unter So entfernen Sie einen delegierten Administrator im Amazon-Inspector-Benutzerhandbuch.

AWS License Manager und AWS Organizations

AWS License Manager optimiert die Migration von Softwarelizenzen zur Cloud. Durch die Verwendung eigener Lizenzen (Bring Your Own License, BYOL) während der Entwicklung der Cloud-Infrastruktur auf AWS können Sie Kosten sparen. Damit ist die Wiederverwendung vorhandener Lizenzen zur Verwendung mit Cloud-Ressourcen gemeint. Mittels regelbasierter Kontrollen für die Nutzung von Lizenzen können Administratoren harte oder weiche Limits für neue und vorhandene Cloud-Bereitstellungen festlegen. Dies verhindert eine nicht konforme Servernutzung, bevor sie überhaupt erfolgt.

Weitere Informationen zu License Manager finden Sie im License-Manager-Benutzerhandbuch.

Die Verknüpfung von License Manager mit AWS Organizations ermöglicht Folgendes:

- Aktivieren der kontoübergreifenden Erkennung von Computing-Ressourcen in der gesamten Organisation
- Anzeigen und Verwalten kommerzieller Linux-Abonnements, die Sie besitzen und in AWS ausführen. Weitere Informationen finden Sie unter Linux-Abonnements in AWS License Manager.

Verwenden Sie die folgenden Informationen, um AWS License Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgenden serviceverknüpften Rollen werden automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit diesen Rollen kann License Manager unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können Rollen nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen License Manager und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Weitere Informationen finden Sie unter License Manager – Verwaltungskontorolle, License Manager – Mitgliedskontorolle und License Manager – Linux-Abonnementrolle.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von License Manager verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `license-manager.amazonaws.com`
- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

Den vertrauenswürdigen Zugriff mit License Manager aktivieren

Sie können den vertrauenswürdigen Zugriff nur mit AWS License Manager aktivieren.

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

So aktivieren Sie den vertrauenswürdigen Zugriff mit License Manager

Sie müssen sich mit Ihrem AWS Organizations-Verwaltungskonto bei der License-Manager-Konsole anmelden und es mit Ihrem License-Manager-Konto verknüpfen. Weitere Informationen finden Sie unter Einstellungen in AWS License Manager.

Deaktivieren des vertrauenswürdigen Zugriffs mit License Manager

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS License Manager als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-manager.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

  Verwenden Sie Folgendes, um den vertrauenswürdigen Zugriff für Linux-Abonnements zu deaktivieren:

  ```
  $  aws organizations disable-aws-service-access \
      --service-principal license-manager-linux-subscriptions.amazonaws.com
  ```

- AWS-API: DisableAWSServiceAccess

So aktivieren Sie ein delegiertes Administratorkonto für License Manager

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für License Manager ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden

können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung des Licence Manager zu trennen.

Um ein Mitgliedskonto als Administrator für License Manager zu delegieren, befolgen Sie die Schritte unter Registrieren eines delegierten Administrators im License-Manager-Benutzerhandbuch.

Amazon Macie und AWS Organizations

Amazon Macie ist ein vollständig verwalteter Service für Datensicherheit und Datenschutz, der Machine Learning und Musterabgleich verwendet, um Ihre sensiblen Daten in Amazon Simple Storage Service (Amazon S3) zu erkennen, zu überwachen und zu schützen. Macie automatisiert die Erkennung sensibler Daten, wie persönlich identifizierbare Informationen (PII) und geistiges Eigentum, um Ihnen ein besseres Verständnis für die Daten zu bieten, die Ihre Organisation in Amazon S3 speichert.

Weitere Informationen finden Sie unter Verwalten von Amazon-Macie-Konten mit AWS Organizations im Amazon-Macie-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Amazon Macie mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im delegierten Macie-Konto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Macie die unterstützten Vorgänge innerhalb der Konten in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen, wenn Sie den vertrauenswürdigen Zugriff zwischen Macie und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleRorAmazonMacie`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Macie verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `macie.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Macie

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die Amazon-Macie-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die Amazon-Macie-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann Amazon Macie jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von Amazon Macie bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der Amazon-Macie-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Macie-Konsole

Amazon Macie erfordert vertrauenswürdigen Zugriff auf AWS Organizations, um ein Mitgliedskonto als Macie-Administrator für Ihre Organisation zu bestimmen. Wenn Sie einen delegierten Administrator mit der Macie-Verwaltungskonsole konfigurieren, aktiviert Macie automatisch den vertrauenswürdigen Zugriff für Sie.

Weitere Informationen finden Sie unter Integration und Konfiguration einer Organisation in Amazon Macie im Amazon-Macie-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon Macie als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Macie

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Macie ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von Macie zu trennen.

Mindestberechtigungen

Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto mit den folgenden Berechtigungen kann ein Mitgliedskonto als delegierter Administrator für Macie in der Organisation konfigurieren:

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

So weisen Sie ein Mitgliedskonto als delegierten Administrator für Macie an

Amazon Macie erfordert vertrauenswürdigen Zugriff auf AWS Organizations, um ein Mitgliedskonto als Macie-Administrator für Ihre Organisation zu bestimmen. Wenn Sie einen delegierten Administrator mit der Macie-Verwaltungskonsole konfigurieren, aktiviert Macie automatisch den vertrauenswürdigen Zugriff für Sie.

Weitere Informationen finden Sie unter https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

AWS Marketplace und AWS Organizations

AWS Marketplace ist ein kuratierter digitaler Katalog, den Sie zum Suchen, Kaufen, Bereitstellen und Verwalten von Drittanbieter-Software verwenden können, die Sie zum Entwickeln von Lösungen und für geschäftliche Abläufe benötigen.

AWS Marketplace erstellt und verwaltet Lizenzen mithilfe von AWS License Manager für Ihre Einkäufe in AWS Marketplace. Wenn Sie Ihre Lizenzen mit anderen Konten in Ihrer Organisation teilen (Zugriff gewähren), erstellt und verwaltet AWS Marketplace neue Lizenzen für diese Konten.

Weitere Informationen finden Sie unter Serviceverknüpften Rollen für AWS Marketplace im AWS Marketplace-Käuferhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Marketplace mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS Marketplace unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS Marketplace und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS Marketplace verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `license-management.marketplace.amazonaws.com`

Den vertrauenswürdigen Zugriff mit AWS Marketplace aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Marketplace-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Marketplace-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Marketplace jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Marketplace bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Marketplace-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS Marketplace-Konsole

Siehe Erstellen einer serviceverknüpften Rolle für AWS Marketplace im AWS Marketplace-Käuferhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Marketplace, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Marketplace, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Marketplace als vertrauenswürdigen Service für Organizations zu aktivieren.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS Marketplace

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Marketplace als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

AWS Marketplace Private Marketplace und AWS Organizations

AWS Marketplace ist ein kuratierter digitaler Katalog, mit dem Sie Software, Daten und Services von Drittanbietern suchen, kaufen, bereitstellen und verwalten können, die Sie zum Entwickeln von Lösungen und für den Betrieb Ihres Unternehmens benötigen. Ein privater Marketplace bietet Ihnen eine breite Palette von Produkten, die in verfügbar sind AWS Marketplace, sowie eine differenzierte Kontrolle über diese Produkte.

AWS Marketplace Mit Private Marketplace können Sie mehrere private Marketplace-Erlebnisse erstellen, die Ihrer gesamten Organisation zugeordnet sind, eine oder mehrere OUs oder ein oder mehrere Konten in Ihrer Organisation, die jeweils einen eigenen Satz genehmigter Produkte aufweisen. Ihre AWS Administratoren können mit dem Logo, Messaging und Farbschema Ihres Unternehmens oder Teams auch Unternehmens-Branding auf jede private Marketplace-Erfahrung anwenden.

Weitere Informationen finden Sie unter Verwenden von Rollen zum Konfigurieren von Private Marketplace in AWS Marketplace im AWS Marketplace -Käuferhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Marketplace Private Marketplace in zu integrieren AWS Organizations.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff über die AWS Marketplace Private Marketplace-

Konsole aktivieren. Mit dieser Rolle kann Private Marketplace unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen. Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS Marketplace Private Marketplace und Organizations deaktivieren und die Zuordnung aller privaten Marketplace-Erlebnisse in Ihrer Organisation aufheben.

Wenn Sie den vertrauenswürdigen Zugriff direkt über die Organizations-Konsole, die CLI oder das SDK aktivieren, wird die serviceverknüpfte Rolle nicht automatisch erstellt.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Private Marketplace verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `private-marketplace.marketplace.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Private Marketplace

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Marketplace Private Marketplace-Konsole oder die AWS Organizations -Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Marketplace Private Marketplace-Konsole oder Tools verwenden, um die Integration mit Organizations zu ermöglichen. Auf diese Weise kann AWS Marketplace Private Marketplace jede erforderliche Konfiguration durchführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den Tools von AWS Marketplace Private Marketplace aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.

Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Marketplace Private Marketplace-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Private Marketplace-Konsole

Weitere Informationen finden Sie unter Erste Schritte mit Private Marketplace im AWS Marketplace - Käuferhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die - AWS Organizations Konsole, einen - AWS CLI Befehl ausführen oder eine API-Operation in einem der - AWS SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Marketplace Private Marketplace , wählen Sie den Namen des Services und dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von sind AWS Organizations, teilen Sie dem Administrator von AWS Marketplace Private Marketplace mit, dass er diesen Service jetzt über seine Konsole aktivieren kann, um mit zu arbeiten AWS Organizations.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu aktivieren:

- AWS CLI: enable-aws-service-access

Sie können den folgenden Befehl ausführen, um AWS Marketplace Private Marketplace als vertrauenswürdigen Service für Organizations zu aktivieren.

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

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS API: AktivierenAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Private Marketplace

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations- AWS CLI Befehl ausführen oder eine Organizations-API-Operation in einem der AWS SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Marketplace Private Marketplace als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS API: DeaktivierenAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Private Marketplace

Der Administrator des Verwaltungskontos kann administrative Private Marketplace-Berechtigungen an ein bestimmtes Mitgliedskonto delegieren, das als delegierter Administrator bezeichnet wird. Um ein Konto als delegierten Administrator für den privaten Marketplace zu registrieren, muss der Administrator des Verwaltungskontos sicherstellen, dass der vertrauenswürdige Zugriff und die serviceverknüpfte Rolle aktiviert sind, wählen Sie Neuen Administrator registrieren, geben Sie die 12-stellige AWS Kontonummer an und wählen Sie Senden.

Verwaltungskonten und delegierte Administratorkonten können administrative Aufgaben von Private Marketplace ausführen, z. B. das Erstellen von Erlebnissen, das Aktualisieren von Branding-Einstellungen, das Zuordnen oder Aufheben der Zuordnung von Zielgruppen, das Hinzufügen oder Entfernen von Produkten und das Genehmigen oder Ablehnen ausstehender Anfragen.

Informationen zum Konfigurieren eines delegierten Administrators mithilfe der Private Marketplace-Konsole finden Sie unter Erstellen und Verwalten eines privaten Marketplaces im AWS Marketplace - Käuferhandbuch.

Sie können einen delegierten Administrator auch mithilfe der Organizations`RegisterDelegatedAdministrator`-API konfigurieren. Weitere Informationen finden Sie unter RegisterDelegatedAdministrator in der Organizations-Befehlsreferenz.

Deaktivieren eines delegierten Administrators für Private Marketplace

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für Private Marketplace konfigurieren.

Sie können den delegierten Administrator entweder über die Private Marketplace-Konsole oder API oder über die Organizations`DeregisterDelegatedAdministrator`-CLI- oder SDK-Operation entfernen.

Informationen zum Deaktivieren des delegierten Private-Marketplace-Administratorkontos mithilfe der Private-Marketplace-Konsole finden Sie unter Erstellen und Verwalten eines privaten Marketplaces im -AWS Marketplace Käuferhandbuch.

AWS Network Manager und AWS Organizations

Mit Network Manager können Sie Ihr AWS-Cloud-WAN-Kernnetzwerk und Ihr AWS-Transit-Gateway-Netzwerk über AWS-Konten, Regionen und lokale Standorte verwalten. Mit Unterstützung für mehrere Konten können Sie ein einziges globales Netzwerk für jedes Ihrer AWS-Konten erstellen und

mithilfe der Network-Manager-Konsole Transit-Gateways von mehreren Konten im globalen Netzwerk registrieren.

Wenn der vertrauenswürdige Zugriff zwischen Network Manager und Organizations aktiviert ist, können die registrierten delegierten Administratoren und die Verwaltungskonten die in den Mitgliedskonten bereitgestellte serviceverknüpfte Rolle nutzen, um Ressourcen zu beschreiben, die mit Ihren globalen Netzwerken verbunden sind. In der Network-Manager-Konsole können die registrierten delegierten Administratoren und die Verwaltungskonten die benutzerdefinierten IAM-Rollen übernehmen, die in den Mitgliedskonten bereitgestellt werden: `CloudWatch-CrossAccountSharingRole` für die Überwachung und das Eventing von mehreren Konten und `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` für den Rollenwechselzugriff der Konsole zum Anzeigen und Verwalten von Ressourcen für mehrere Konten

> **Important**
>
> - Es wird nachdrücklich empfohlen, die Network-Manager-Konsole zum Verwalten von Einstellungen für mehrere Konten zu verwenden (vertrauenswürdigen Zugriff aktivieren/deaktivieren und delegierte Administratoren registrieren/abmelden). Durch die Verwaltung dieser Einstellungen von der Konsole aus werden alle erforderlichen serviceverknüpften Rollen und benutzerdefinierten IAM-Rollen automatisch auf den Mitgliedskonten bereitgestellt und verwaltet, die für den Zugriff auf mehrere Konten erforderlich sind.
> - Wenn Sie den vertrauenswürdigen Zugriff für Network Manager in der Network-Manager-Konsole aktivieren, aktiviert die Konsole auch den AWS CloudFormation-StackSets-Service. Network Manager verwendet StackSets, um benutzerdefinierte IAM-Rollen bereitzustellen, die für die Verwaltung von mehreren Konten erforderlich sind.

Weitere Informationen über die Integration von Network Manager in Organizations finden Sie unter Verwalten von mehreren Konten im Network Manager mit AWS Organizations im Amazon-VPC-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Network Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgenden serviceverknüpften Rollen werden automatisch in den gelisteten Organisationskonten erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit diesen Rollen kann Network

Manager unterstützte Vorgänge innerhalb der Konten in Ihrer Organisation ausführen. Wenn Sie den vertrauenswürdigen Zugriff deaktivieren, löscht Network Manager diese Rollen nicht aus Konten in Ihrer Organisation. Sie können sie manuell über die IAM-Konsole löschen.

Verwaltungskonto

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Mitgliedskonten

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Wenn Sie ein Mitgliedskonto als delegierten Administrator registrieren, wird automatisch die folgende zusätzliche Rolle im delegierten Administratorkonto erstellt:

- `AWSServiceRoleForCloudWatchCrossAccount`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpften Rollen im vorherigen Abschnitt können nur von den Service-Prinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind.

- Für die `AWSServiceRoleForNetworkManager service-linked`-Rolle hat `networkmanager.amazonaws.com` als einziger Service-Prinzipal Zugriff.
- Für die serviceverknüpfte `AWSServiceRoleForCloudFormationStackSetsOrgMember`-Rolle hat `member.org.stacksets.cloudformation.amazonaws.com` als einziger Service-Prinzipal Zugriff.
- Für die serviceverknüpfte `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`-Rolle hat `stacksets.cloudformation.amazonaws.com` als einziger Service-Prinzipal Zugriff.
- Für die serviceverknüpfte `AWSServiceRoleForCloudWatchCrossAccount`-Rolle hat `cloudwatch-crossaccount.amazonaws.com` als einziger Service-Prinzipal Zugriff.

Das Löschen dieser Rollen beeinträchtigt die Multi-Account-Funktionalität von Network Manager.

Aktivieren des vertrauenswürdigen Zugriffs mit Network Manager

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im Organizations-Verwaltungskonto verfügt über Berechtigungen zum Aktivieren des vertrauenswürdigen Zugriffs mit einem anderen AWS-Service. Verwenden Sie unbedingt die Network-Manager-Konsole, um den vertrauenswürdigen Zugriff zu aktivieren, damit Berechtigungsprobleme vermieden werden. Weitere Informationen finden Sie unter Verwalten mehrerer Konten in Network Manager mit AWS Organizations im Amazon-VPC-Benutzerhandbuch.

Deaktivieren des vertrauenswürdigen Zugriffs mit Network Manager

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im Organizations-Verwaltungskonto verfügt über Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs mit einem anderen AWS-Service.

> **Important**
>
> Es wird nachdrücklich empfohlen, die Network-Manager-Konsole zu verwenden, um den vertrauenswürdigen Zugriff zu deaktivieren. Wenn Sie den vertrauenswürdigen Zugriff auf andere Weise deaktivieren, z. B. mit AWS CLI, mit einer API oder mit der AWS CloudFormation-Konsole, werden bereitgestellte AWS CloudFormation StackSets und benutzerdefinierte IAM-Rollen möglicherweise nicht vollständig bereinigt. Um den vertrauenswürdigen Zugriff auf einen Service zu deaktivieren, melden Sie sich in der Network-Manager-Konsole an.

So aktivieren Sie ein delegiertes Administratorkonto für Network Manager

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Network Manager ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung des Network Manager zu trennen.

Anweisungen zum Festlegen eines Mitgliedskontos als delegierter Administrator von Network Manager in der Organisation finden Sie unter Registrieren eines delegierten Administrators im Amazon-VPC-Benutzerhandbuch.

AWS Resource Access Manager und AWS Organizations

AWS Resource Access Manager (AWS RAM) ermöglicht Ihnen die gemeinsame Nutzung angegebener AWS-Ressourcen, die Sie besitzen, zusammen mit anderen AWS-Konten. Es handelt sich um einen zentralen Service, der eine konsistente Erfahrung für die Freigabe verschiedener Arten von AWS-Ressourcen über mehrere Konten hinweg bereitstellt.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Resource Access Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS RAM unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS RAM und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForResourceAccessManager`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS RAM verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `ram.amazonaws.com`

Den vertrauenswürdigen Zugriff mit AWS RAM aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Resource Access Manager-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Resource Access Manager-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Resource Access Manager jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Resource Access Manager bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Resource Access Manager-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS RAM-Konsole oder CLI

Siehe Freigabe mit AWS Organizations aktivieren im AWS RAM-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Resource Access Manager, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Resource Access Manager, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Resource Access Manager als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS RAM

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Resource Access Manager oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Resource Access Manager-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Resource Access Manager alle erforderlichen Bereinigungen

durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Resource Access Manager bereitgestellten Tools deaktivieren können. Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Resource Access Manager-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die AWS Resource Access Manager-Konsole oder CLI

Siehe Freigabe mit AWS Organizations aktivieren im AWS RAM-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Resource Access Manager und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Resource Access Manager mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Resource Access Manager als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

AWS Ressourcen Explorer und AWS Organizations

AWS Ressourcen Explorer ist ein Dienst zur Suche und Entdeckung von Ressourcen. Mit Resource Explorer können Sie Ihre Ressourcen, wie Amazon Elastic Compute Cloud-Instances, Amazon Kinesis Data Streams oder Amazon DynamoDB-Tabellen mithilfe einer Internet-Suchmaschine erkunden. Sie können mithilfe von Ressourcen-Metadaten wie Namen, Tags und IDs nach Ihren Ressourcen suchen. Resource Explorer funktioniert über AWS-Regionen hinweg in Ihrem Konto, um Ihre regionsübergreifenden Workloads zu vereinfachen.

Wenn Sie Resource Explorer mit AWS Organizations integrieren, können Sie Beweise aus einer breiteren Quelle sammeln, indem Sie mehrere AWS-Konten aus Ihrer Organisation in Ihre Bewertungen einbeziehen.

Verwenden Sie die folgenden Informationen, um AWS Ressourcen Explorer mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Resource Explorer unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Resource Explorer und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

Weitere Informationen zur Verwendung dieser Rolle durch Resource Explorer finden Sie unter Verwenden von serviceverknüpften Rollen im AWS Ressourcen Explorer-Benutzerhandbuch.

- `AWSServiceRoleForResourceExplorer`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Resource Explorer verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Service-Prinzipale:

- `resource-explorer-2.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit AWS Ressourcen Explorer

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Resource Explorer erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für Ihre Organisation festlegen können.

Sie können den vertrauenswürdigen Zugriff entweder über die Resource-Explorer-Konsole oder über die Organizations-Konsole aktivieren. Wir empfehlen dringend, dass Sie nach Möglichkeit die Resource-Explorer-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Ressourcen Explorer jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Resource-Explorer-Konsole

Anweisungen zur Aktivierung des vertrauenswürdigen Zugriffs finden Sie unter Voraussetzungen für die Verwendung von Resource Explorer im AWS Ressourcen Explorer-Benutzerhandbuch.

> **Note**
>
> Wenn Sie einen delegierten Administrator mit der AWS Ressourcen Explorer-Konsole konfigurieren, aktiviert AWS Ressourcen Explorer automatisch den vertrauenswürdigen Zugriff für Sie.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Ressourcen Explorer als vertrauenswürdigen Service für Organizations zu aktivieren.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

So deaktivieren Sie den vertrauenswürdigen Zugriff mit Resource Explorer

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit AWS Ressourcen Explorer deaktivieren.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Ressourcen Explorer oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Ressourcen Explorer-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Ressourcen Explorer alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Ressourcen Explorer bereitgestellten Tools deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Ressourcen Explorer-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Ressourcen Explorer als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Resource Explorer

Verwenden Sie Ihr delegiertes Administratorkonto, um Ressourcenansichten für mehrere Konten zu erstellen und sie auf eine Organisationseinheit oder Ihre gesamte Organisation zu beschränken. Sie können durch AWS Resource Access Manager Ansichten mehrerer Konten mit jedem Konto in Ihrer Organisation teilen, indem Sie Ressourcenfreigaben erstellen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto mit der folgenden Berechtigung kann ein Mitgliedskonto als delegierter Administrator für Resource Explorer in der Organisation konfigurieren:
> `resource-explorer:RegisterAccount`

Anweisungen zum Aktivieren eines delegierten Administratorkontos für Resource Explorer finden Sie unter Einrichten im AWS Ressourcen Explorer-Benutzerhandbuch.

Wenn Sie einen delegierten Administrator mit der AWS Ressourcen Explorer-Konsole konfigurieren, aktiviert Resource Explorer automatisch den vertrauenswürdigen Zugriff für Sie.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator`und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontodienst `resource-explorer-2.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für Resource Explorer

Nur ein Administrator im Verwaltungskonto von Organizations oder im delegierten Administratorkonto von Resource Explorer kann einen delegierten Administrator für Resource Explorer entfernen. Sie können den vertrauenswürdigen Zugriff über den `DeregisterDelegatedAdministrator`-CLI- oder SDK-Vorgang von Organizations deaktivieren.

AWS Security Hub und AWS Organizations

AWS Security Hub bietet Ihnen einen umfassenden Überblick über Ihren Sicherheitsstatus in AWS und hilft Ihnen dabei, Ihre -Umgebung anhand von Sicherheitsstandards und bewährten Methoden der Branche zu überprüfen.

Security Hub sammelt Sicherheitsdaten aus Ihrem AWS-Konten, den von Ihnen verwendeten AWS Services und unterstützten Partnerprodukten von Drittanbietern. Sie hilft Ihnen dabei, Ihre Sicherheitstrends zu analysieren und Sicherheitsprobleme mit höchster Priorität zu identifizieren.

Wenn Sie sowohl Security Hub als auch AWS Organizations zusammen verwenden, können Sie Security Hub automatisch für alle Ihre Konten aktivieren, einschließlich neuer Konten, sobald sie hinzugefügt werden. Dadurch wird die Abdeckung für Security-Hub-Prüfungen und -Ergebnisse erhöht, wodurch ein umfassenderes und genaueres Bild Ihres gesamten Sicherheitsstatus erhalten wird.

Weitere Informationen zu Security Hub finden Sie im AWS Security Hub -Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um die Integration AWS Security Hub mit zu erleichtern AWS Organizations.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Security Hub unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Security Hub und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForSecurityHub`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Security Hub verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `securityhub.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Security Hub

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie einen delegierten Administrator für Security Hub festlegen, aktiviert Security Hub automatisch vertrauenswürdigen Zugriff für Security Hub in Ihrer Organisation.

So aktivieren Sie ein delegiertes Administratorkonto für den Security Hub

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Security Hub ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden

können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von Security Hub zu trennen.

Weitere Informationen finden Sie unter Festlegen eines Security-Hub-Administratorkontos im AWS Security Hub -Benutzerhandbuch.

So weisen Sie ein Mitgliedskonto als delegierten Administrator für Security Hub an

1. Melden Sie sich mit Ihrem Organizations-Verwaltungskonto an.
2. Führen Sie einen der folgenden Schritte aus:
   - Wenn für Ihr Verwaltungskonto Security Hub nicht aktiviert ist, wählen Sie in der Security-Hub-Konsole Zu Security Hub gehen.
   - Wenn für Ihr Verwaltungskonto Security Hub aktiviert ist, wählen Sie in der Security Hub-Konsole unter Allgemeine Einstellungen aus.
3. Geben Sie unter Delegierter Administrator die Konto-ID ein.

Amazon S3 Storage Lens und AWS Organizations

Indem Sie Amazon S3 Storage Lens vertrauenswürdigen Zugriff auf Ihre Organisation gewähren, ermöglichen Sie es, Metriken für alle AWS-Konten in Ihrer Organisation zu sammeln und zu aggregieren. S3 Storage Lens greift dazu auf die Liste der Konten zu, die zu Ihrer Organisation gehören, und sammelt und analysiert die Speicher- und Nutzungs- und Aktivitätsmetriken für alle von ihnen.

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon S3 Storage Lens im Amazon-S3-Storage-Lens-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Amazon S3 Storage Lens mit AWS Organizations zu integrieren.

Service-verknüpfte Rolle, die erstellt wird, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Konto des delegierten Administrators Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren und die Storage-Lens-Konfiguration auf Ihre Organisation angewendet wurde. Mit dieser Rolle kann Amazon S3 Storage Lens unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Amazon S3 Storage Lens und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForS3StorageLens`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Amazon S3 Storage Lens verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `storage-lens.s3.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Amazon S3 Storage Lens

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die Amazon-S3-Storage-Lens-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die Amazon-S3-Storage-Lens-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann Amazon S3 Storage Lens jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration mit den Tools von Amazon S3 Storage Lens nicht aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der Amazon-S3-Storage-Lens-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Amazon-S3-Konsole

Siehe So aktivieren Sie den vertrauenswürdigen Zugriff im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon S3 Storage Lens, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von Amazon S3 Storage Lens, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon S3 Storage Lens als vertrauenswürdigen Service für Organizations zu aktivieren.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Amazon S3 Storage Lens

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Amazon-S3-Storage-Lens-Tools deaktivieren.

Sie können den vertrauenswürdigen Zugriff über die Amazon-S3-Konsole, die AWS-CLI oder eines der AWS-SDKs deaktivieren.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die Amazon-S3-Konsole

Siehe So deaktivieren Sie den vertrauenswürdigen Zugriff im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Aktivieren eines delegierten Administratorkontos für Amazon S3 Storage Lens

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos administrative Aktionen für Amazon S3 Storage Lens ausführen, die andernfalls nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung von Amazon S3 Storage Lens zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto mit der folgenden Berechtigung kann ein Mitgliedskonto als delegierter Administrator für Amazon S3 Storage Lens in der Organisation konfigurieren:
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens unterstützt maximal 5 delegierte Administratorkonten in Ihrer Organisation.

So weisen Sie ein Mitgliedskonto als delegierter Administrator für Amazon S3 Storage Lens an

Sie können einen delegierten Administrator über die Amazon-S3-Konsole, die AWS-CLI oder eines der AWS-SDKs registrieren. Informationen zum Registrieren eines Mitgliedskontos als delegiertes Administratorkonto für Ihre Organisation mithilfe der Amazon-S3-Konsole finden Sie

unter So registrieren Sie einen delegierten Administrator im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Registrierung eines delegierten Administrators für Amazon S3 Storage Lens aufheben

Sie können einen delegierten Administrator über die Amazon-S3-Konsole, die AWS-CLI oder eines der AWS-SDKs deregistrieren. Informationen zum Abmelden eines delegierten Administrators mithilfe der Amazon-S3-Konsole finden Sie unter So deregistrieren Sie einen delegierten Administrator im Amazon-Simple-Storage-Service-Benutzerhandbuch.

Amazon Security Lake und AWS Organizations

Amazon Security Lake zentralisiert Sicherheitsdaten aus Cloud-, On-Premises- und benutzerdefinierten Quellen in einem Data Lake, der in Ihrem Konto gespeichert ist. Durch die Integration mit Organizations können Sie einen Data Lake erstellen, der Protokolle und Ereignisse in Ihren Konten erfasst. Weitere Informationen finden Sie unter Verwalten mehrerer Konten mit AWS Organizations im Amazon-Security-Lake-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Ihnen bei der Integration von Amazon Security Lake zu helfen AWS Organizations.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Diese Rolle ermöglicht es Amazon Security Lake, unterstützte Operationen innerhalb der Konten Ihrer Organisation in Ihrer Organisation durchzuführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Amazon Security Lake und Organizations deaktivieren oder wenn Sie das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForSecurityLake`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind.

Die von Amazon Security Lake verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Service Principals:

- `securitylake.amazonaws.com`

Vertrauenswürdigen Zugriff mit Amazon Security Lake aktivieren

Wenn Sie mit Security Lake den vertrauenswürdigen Zugriff aktivieren, kann Security Lake automatisch auf Änderungen der Organisationsmitgliedschaft reagieren. Der delegierte Administrator kann die Erfassung von AWS Protokollen von unterstützten Diensten in jedem Unternehmenskonto aktivieren. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Amazon Security Lake im Amazon Security Lake-Benutzerhandbuch.

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations Konsole verwenden, einen AWS CLI Befehl ausführen oder eine API-Operation in einem der AWS SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon Security Lake, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie der Administrator von Only sind AWS Organizations, teilen Sie dem Administrator von Amazon Security Lake mit, dass er diesen Service jetzt über die Konsole aktivieren kann, mit der er arbeiten kann AWS Organizations.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon Security Lake als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS API: Aktivieren AWSServiceAccess

Deaktivierung des vertrauenswürdigen Zugriffs mit Amazon Security Lake

Nur ein Administrator im Verwaltungskonto der Organizations kann den vertrauenswürdigen Zugriff mit Amazon Security Lake deaktivieren.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations Konsole verwenden, einen AWS CLI Organizations-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations -Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Amazon Security Lake und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.

4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie der Administrator von Only sind AWS Organizations, teilen Sie dem Administrator von Amazon Security Lake mit, dass er diesen Service jetzt mithilfe der Konsole oder der Tools deaktivieren kann, damit er nicht mehr funktioniert AWS Organizations.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Sie können die folgenden AWS CLI Befehle oder API-Operationen verwenden, um den vertrauenswürdigen Servicezugriff zu deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Amazon Security Lake als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS API: Deaktivieren AWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Amazon Security Lake

Der delegierte Administrator von Amazon Security Lake fügt weitere Konten in der Organisation als Mitgliedskonten hinzu. Der delegierte Administrator kann Amazon Security Lake aktivieren und Amazon Security Lake-Einstellungen für die Mitgliedskonten konfigurieren. Der delegierte Administrator kann unternehmensweit in allen AWS Regionen, in denen Amazon Security Lake aktiviert ist, Protokolle sammeln (unabhängig davon, welchen regionalen Endpunkt Sie gerade verwenden).

Sie können den delegierten Administrator auch so einrichten, dass er automatisch neue Konten in der Organisation als Mitglieder hinzufügt. Der delegierte Administrator von Amazon Security Lake hat Zugriff auf die Protokolle und Ereignisse in den zugehörigen Mitgliedskonten. Dementsprechend können Sie Amazon Security Lake so einrichten, dass Daten erfasst werden, die zugehörigen

Mitgliedskonten gehören. Sie können Abonnenten auch die Erlaubnis erteilen, Daten zu nutzen, die zugehörigen Mitgliedskonten gehören.

Weitere Informationen finden Sie unter Verwalten mehrerer Konten mit AWS Organizations im Amazon-Security-Lake-Benutzerhandbuch.

> **Mindestberechtigungen**
>
> Nur ein Administrator im Verwaltungskonto der Organizations kann ein Mitgliedskonto als delegierter Administrator für Amazon Security Lake in der Organisation konfigurieren

Sie können ein delegiertes Administratorkonto mithilfe der Amazon Security Lake-Konsole, der Amazon Security `CreateDatalakeDelegatedAdmin` Lake-API-Aktion oder des `create-datalake-delegated-admin` CLI-Befehls angeben. Alternativ hierzu können Sie auch die Organizations-`RegisterDelegatedAdministrator`-CLI- oder SDK-Operation verwenden. Anweisungen zur Aktivierung eines delegierten Administratorkontos für Amazon Security Lake finden Sie unter Benennen des delegierten Security Lake-Administrators und Hinzufügen von Mitgliedskonten im Amazon Security Lake-Benutzerhandbuch.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mithilfe der AWS CLI oder eines der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie den `RegisterDelegatedAdministrator` Betrieb Organizations und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontodienstprinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für Amazon Security Lake

Nur ein Administrator im Verwaltungskonto der Organizations oder im delegierten Administratorkonto von Amazon Security Lake kann ein delegiertes Administratorkonto aus der Organisation entfernen.

Sie können das delegierte Administratorkonto mithilfe der Amazon Security `DeleteDatalakeDelegatedAdmin` Lake-API-Aktion, des `delete-datalake-delegated-admin` CLI-Befehls oder mithilfe des CLI- oder SDK-Vorgangs Organizations `DeregisterDelegatedAdministrator` entfernen. Informationen zum Entfernen eines delegierten Administrators mithilfe von Amazon Security Lake finden Sie unter Entfernen des delegierten Amazon Security Lake-Administrators im Amazon Security Lake-Benutzerhandbuch.

AWS Service Catalog und AWS Organizations

Mit Service Catalog können Sie Kataloge von IT-Services erstellen und verwalten, die für die Verwendung auf AWS genehmigt sind.

Die Integration von Service Catalog mit AWS Organizations vereinfacht die Freigabe von Portfolios und das Kopieren von Produkten innerhalb einer Organisation. Servicekatalog-Administratoren können beim Freigeben eines Portfolios auf eine vorhandene Organisation in AWS Organizations verweisen. Außerdem können sie das Portfolio für jede vertrauenswürdige Organisationseinheit (OE) in der Struktur der Organisation teilen. Dies beseitigt die Notwendigkeit, Portfolio-IDs freigeben zu müssen. Außerdem muss das empfangende Konto die Portfolio-ID beim Importieren des Portfolios nicht mehr manuell referenzieren. Portfolios, die über diesen Mechanismus freigegeben werden, werden in dem gemeinsam genutzten Konto in der Ansicht Imported Portfolio (Importierte Portfolios) des Administrators im Service Catalog aufgeführt.

Weitere Informationen zu Service Catalog finden Sie im Service-Catalog-Administratorhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Service Catalog mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

AWS Service Catalog erstellt im Rahmen der Aktivierung des vertrauenswürdigen Zugriffs keine serviceverknüpften Rollen.

Serviceprinzipale zum Erteilen von Berechtigungen

Um den vertrauenswürdigen Zugriff zu aktivieren, müssen Sie den folgenden Serviceprinzipal angeben:

- `servicecatalog.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Service Catalog

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Service Catalog-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Service Catalog-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Service Catalog jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Service Catalog bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Service Catalog-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff mit der Service-Catalog-CLI oder dem AWS-SDK

Rufen Sie einen der folgenden Befehle oder Operationen auf:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- AWS-SDKs: AWSServiceCatalog::EnableAWSOrganizationsAccess

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).

2. Suchen Sie auf der Seite Services die Zeile für AWS Service Catalog, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Service Catalog, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Service Catalog als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Service Catalog

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie den vertrauenswürdigen Zugriff mithilfe von AWS Organizations deaktivieren, während Sie Service Catalog verwenden, werden Ihre aktuellen Freigaben nicht gelöscht Sie können jedoch keine neuen Freigaben für Ihre gesamte Organisation erstellen. Aktuelle Freigaben werden nicht mit der Struktur Ihrer Organisation synchronisiert, wenn sie nach dem Aufruf dieser Aktion geändert wird.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Service Catalog oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Service Catalog-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Service Catalog alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Service Catalog bereitgestellten Tools deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Service Catalog-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff mit der Service-Catalog-CLI oder dem AWS-SDK

Rufen Sie einen der folgenden Befehle oder Operationen auf:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- AWS-SDKs: DisableAWSOrganizationsAccess

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Service Catalog und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.

5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Service Catalog mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Service Catalog als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Service Quotas und AWS Organizations

Service Quotas ist ein AWS-Service, mit dem Sie Ihre Kontingente von einem zentralen Ort aus anzeigen und verwalten können. Kontingente, die auch als Einschränkungen bezeichnet werden, sind der Höchstwert für Ihre Ressourcen, Aktionen und Elemente in Ihrem AWS-Konto.

Wenn Service Quotas AWS Organizations zugeordnet ist, können Sie eine Kontingent-Anforderungsvorlage erstellen, um automatisch Kontingenterhöhungen anzufordern, wenn Konten erstellt werden.

Weitere Informationen zu Service Quotas finden Sie im Service-Quotas-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Service Quotas mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Service Quotas unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Service Quotas und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForServiceQuotas`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Service Quotas verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `servicequotas.amazonaws.com`

Aktivieren eines vertrauenswürdigen Zugriffs mit Service Quotas

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur mit Service Quotas aktivieren.

Sie können den vertrauenswürdigen Zugriff mit der Service-Quotas-Konsole, AWS CLI oder das SDK aktivieren

- So aktivieren Sie den vertrauenswürdigen Zugriff mit der Service-Quotas-Konsole

  Melden Sie sich mit Ihrem AWS Organizations-Verwaltungskonto an und konfigurieren Sie dann die Vorlage auf der Service-Quotas-Konsole. Weitere Informationen finden Sie unter Using the Service Quota Template im Service Quotas User Guide.
- So aktivieren Sie den vertrauenswürdigen Zugriff mit der Service-Quotas-AWS CLI oder SDK

  Rufen Sie den folgenden Befehl oder die Operation auf:

- AWS CLI: aws service-quotas associate-service-quota-template
- AWS-SDKs: AssociateServiceQuotaTemplate

AWS IAM Identity Center und AWS Organizations

AWS IAM Identity Center bietet Single-Sign-On-Zugriff für Ihre gesamten AWS-Konten- und Cloud-Anwendungen. Es verbindet sich über AWS Directory Service mit Microsoft Active Directory, um Benutzern in diesem Verzeichnis die Möglichkeit zu geben, sich bei einem personalisierten AWS-Zugriffsportal mit ihren vorhandenen Active-Directory-Benutzernamen und -Passwörtern anzumelden. Über das AWS-Zugriffsportal haben die Benutzer Zugriff auf AWS-Konten- und Cloud-Anwendungen, für die sie über Berechtigungen verfügen.

Weitere Informationen zu IAM Identity Center finden Sie im Benutzerhandbuch von AWS IAM Identity Center.

Verwenden Sie die folgenden Informationen, um AWS IAM Identity Center mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann IAM Identity Center unterstützte Vorgänge innerhalb der Konten in Ihrer Organisation ausführen.

Diese Rolle können Sie nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen IAM Identity Center und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForSSO`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von IAM Identity Center verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Service-Prinzipale:

- `sso.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit IAM Identity Center

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS IAM Identity Center-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS IAM Identity Center-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS IAM Identity Center jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS IAM Identity Center bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS IAM Identity Center-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

IAM Identity Center erfordert einen vertrauenswürdigen Zugriff mit AWS Organizations, um richtig zu funktionieren. Der vertrauenswürdige Zugriff wird bei der Einrichtung von IAM Identity Center aktiviert. Weitere Informationen finden Sie unter Erste Schritte - Schritt 1: Aktivieren von AWS IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS IAM Identity Center, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.

3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS IAM Identity Center, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS IAM Identity Center als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit IAM Identity Center

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

IAM Identity Center erfordert für den Betrieb einen vertrauenswürdigen Zugriff mit AWS Organizations. Wenn Sie während der Verwendung von IAM Identity Center den vertrauenswürdigen Zugriff mit AWS Organizations deaktivieren, ist das Center nicht mehr funktionsfähig, da es keinen Zugriff auf die Organisation hat. Benutzer können nicht mithilfe von IAM Identity Center auf Konten zugreifen. Alle von IAM Identity Center erstellten Rollen bleiben erhalten, dessen Service kann aber nicht auf sie zugreifen. Die serviceverknüpften Rollen von IAM Identity Center bleiben erhalten. Wenn Sie den vertrauenswürdigen Zugriff wieder aktivieren, funktioniert IAM Identity Center wie vorher, ohne dass der Service neu konfiguriert werden muss.

Wenn Sie ein Konto aus Ihrer Organisation entfernen, bereinigt IAM Identity Center automatisch alle Metadaten und Ressourcen, wie z. B. die serviceverknüpfte Rolle. Ein eigenständiges Konto, das aus einer Organisation entfernt wurde, funktioniert nicht mehr mit IAM Identity Center.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS IAM Identity Center und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.
5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS IAM Identity Center mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS IAM Identity Center als vertrauenswürdigen Service für Organizations zu deaktivieren.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal sso.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren von Konten für delegierte Administratoren für IAM Identity Center

Wenn Sie ein Mitgliedskonto als delegierten Administrator bzw. als delegierte Administratorin für die Organisation festlegen, können Benutzer und Rollen dieses Kontos Verwaltungsaktionen für IAM Identity Center ausführen, die ansonsten nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dadurch können Sie die Verwaltung der Organisation leichter von der Verwaltung von IAM Identity Center trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für IAM Identity Center in der Organisation konfigurieren.

Anweisungen zum Aktivieren von Konten für delegierte Administratoren für IAM Identity Center finden Sie unter Delegierte Administration im Benutzerhandbuch von AWS IAM Identity Center.

AWS Systems Manager und AWS Organizations

AWS Systems Manager ist eine Sammlung von Funktionen, die für Transparenz und Kontrolle über Ihre AWS-Ressourcen sorgen. Die folgenden Systems-Manager-Funktionen funktionieren mit Organizations in allen AWS-Konten Ihres Unternehmens:

- Systems Manager Explorer ist ein anpassbares Betriebs-Dashboard, das Informationen über Ihre AWS-Ressourcen meldet. Mithilfe von Organizations und Systems Manager Explorer können Sie Betriebsdaten in allen AWS-Konten in Ihrer Organisation synchronisieren. Weitere Informationen finden Sie unter Systems Manager Explorer im AWS Systems Manager-Benutzerhandbuch.
- Systems Manager Change Manager ist ein unternehmensweites Change-Management-Framework zum Anfordern, Genehmigen, Implementieren und Melden von Betriebsänderungen an Ihrer Anwendungskonfiguration und Infrastruktur. Weitere Informationen finden Sie unter AWS Systems Manager Change Manager im AWS Systems Manager-Benutzerhandbuch.

- Systems Manager OpsCenter bietet einen zentralen Speicherort, an dem Techniker und IT-Experten operative Arbeitselemente anzeigen, untersuchen und lösen können (OpsItems), die im Zusammenhang mit AWS-Ressourcen stehen. Wenn Sie OpsCenter mit Organizations verwenden, unterstützt es die Arbeit mit OpsItems über ein Verwaltungskonto (entweder ein Organisationsverwaltungskonto oder ein delegiertes Systems-Manager-Administratorkonto) und ein anderes Konto während einer einzelnen Sitzung. Nach der Konfiguration können Benutzer die folgenden Arten von Aktionen ausführen:
  - Erstellen, anzeigen und aktualisieren Sie OpsItems in einem anderen Konto.
  - Zeigen Sie detaillierte Informationen zu AWS-Ressourcen an, die in OpsItems in einem anderen Konto angegeben sind.
  - Starten Sie Systems-Manager-Automation-Runbooks, um Probleme mit AWS-Ressourcen in einem anderen Konto zu beheben.

  Weitere Informationen finden Sie unter AWS Systems Manager-OpsCenter im AWS Systems Manager-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Systems Manager mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Systems Manager unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Systems Manager und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Systems Manager verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `ssm.amazonaws.com`

Aktivieren des vertrauenswürdigen Zugriffs mit Systems Manager

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations aktivieren.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Systems Manager, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Systems Manager, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

Sie können den folgenden Befehl ausführen, um AWS Systems Manager als vertrauenswürdigen Service für Organizations zu aktivieren.

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

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Systems Manager

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Systems Manager erfordert vertrauenswürdigen Zugriff mit AWS Organizations, um Betriebsdaten über AWS-Konten in Ihrem Unternehmen zu synchronisieren. Wenn Sie den vertrauenswürdigen Zugriff deaktivieren, können Betriebsdaten in Systems Manager nicht synchronisiert werden, und es wird ein Fehler gemeldet.

Sie können den vertrauenswürdigen Zugriff nur über die Tools von Organizations deaktivieren.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen Organizations-AWS CLI-Befehl ausführen oder eine Organizations-API-Operation in einem der AWS-SDKs aufrufen.

AWS Management Console

So deaktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Systems Manager und wählen Sie dann den Namen des Services aus.
3. Wählen Sie Vertrauenswürdigen Zugriff deaktivieren.
4. Geben Sie im Bestätigungsdialogfeld **`disable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff deaktivieren.

5. Wenn Sie nur der Administrator von AWS Organizations sind, teilen Sie dem Administrator von AWS Systems Manager mit, dass er diesen Service jetzt mit seiner Konsole oder seinen Tools für die Arbeit mit AWS Organizations deaktivieren kann.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Systems Manager als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Systems Manager

Wenn Sie ein Mitgliedskonto als delegierten Administrator für die Organisation festlegen, können Benutzer und Rollen dieses Kontos Verwaltungsaktionen für Systems Manager ausführen, die ansonsten nur von Benutzern oder Rollen im Verwaltungskonto der Organisation ausgeführt werden können. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung des Systems Manager zu trennen.

Wenn Sie den Change Manager in einer Organisation verwenden, verwenden Sie ein delegiertes Administratorkonto. Dies ist das AWS-Konto, das als Konto für die Verwaltung von Änderungsvorlagen, Änderungsanforderungen, Änderungsrunbooks und Genehmigungsworkflows im Änderungsmanager festgelegt wurde. Das delegierte Konto verwaltet Änderungsaktivitäten in Ihrer gesamten Organisation. Wenn Sie Ihre Organisation für die Verwendung mit dem Change Manager einrichten, geben Sie an, welche Ihrer Konten in dieser Rolle verwendet werden. Es muss nicht das Verwaltungskonto der Organisation sein. Das delegierte Administratorkonto ist nicht erforderlich, wenn Sie Change Manager nur mit einem einzigen Konto verwenden.

Informationen zum Festlegen eines Mitgliedskontos als delegierter Administrator finden Sie in den folgenden Themen im AWS Systems Manager-Benutzerhandbuch:

- Informationen zu Explorer und OpsCenter finden Sie unter Konfigurieren eines delegierten Administrators.
- Informationen zu Change Manager finden Sie unter Einrichten einer Organisation und eines delegierten Kontos für Change Manager.

Tag-Richtlinien und AWS Organizations

Tag-Richtlinien sind eine Richtlinienart in AWS Organizations, mit der Sie Tags für alle Ressourcen in den Konten Ihrer Organisation standardisieren können. Weitere Informationen zu Tag-Richtlinien finden Sie unter Tag-Richtlinien.

Verwenden Sie die folgenden Informationen, um Tag-Richtlinien mit AWS Organizations zu integrieren.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Organizations interagieren mit den Tags, die Ihren Ressourcen zugeordnet sind, mithilfe des folgenden Serviceprinzipals.

- `tagpolicies.tag.amazonaws.com`

Den vertrauenswürdigen Zugriff für Tag-Richtlinien

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder Tag-Richtlinien in der Organisation aktivieren oder die AWS Organizations-Konsole verwenden.

> **Important**
>
> Es wird dringend davon abgeraten, den vertrauenswürdigen Zugriff durch Aktivieren von Tag-Richtlinien zu aktivieren. Auf diese Weise können Organizations erforderliche Einrichtungs-Aufgaben ausführen.

Sie können den vertrauenswürdigen Zugriff für Tag-Richtlinien aktivieren, indem Sie den Tag-Richtlinientyp in der AWS Organizations-Konsole aktivieren. Weitere Informationen finden Sie unter Aktivieren eines Richtlinientyps.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für Tag-Richtlinien, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von Tag-Richtlinien, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Tag-Richtlinien als vertrauenswürdigen Service für Organizations zu aktivieren.

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

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit Tag-Richtlinien

Sie können den vertrauenswürdigen Zugriff für Tag-Richtlinien deaktivieren, indem Sie den Tag-Richtlinientyp in der AWS Organizations-Konsole deaktivieren. Weitere Informationen finden Sie unter Deaktivieren eines Richtlinientyps.

AWS Trusted Advisor und AWS Organizations

AWS Trusted Advisor überprüft Ihre AWS-Umgebung und gibt Empfehlungen für Möglichkeiten ab, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Bei Integration in Organisationen können Sie Trusted Advisor-Prüfergebnisse für alle Konten in Ihrer Organisation erhalten und Berichte herunterladen, um die Zusammenfassungen Ihrer Prüfungen und alle betroffenen Ressourcen anzuzeigen.

Weitere Informationen finden Sie unter Organisationsansicht für AWS Trusted Advisorim AWS Support-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Trusted Advisor mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Trusted Advisor unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Trusted Advisor und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForTrustedAdvisorReporting`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von Trusted Advisor verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `reporting.trustedadvisor.amazonaws.com`

Den vertrauenswürdigen Zugriff mit Trusted Advisor aktivieren

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff nur mit AWS Trusted Advisor aktivieren.

So aktivieren Sie den vertrauenswürdigen Zugriff über die Trusted Advisor-Konsole

Siehe Organisationsansicht aktivieren im AWS Support-Benutzerhandbuch.

Deaktivieren des vertrauenswürdigen Zugriffs mit Trusted Advisor

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nachdem Sie diese Funktion deaktiviert haben, beendet Trusted Advisor die Aufzeichnung von Überprüfungsinformationen für alle anderen Konten in Ihrer Organisation. Sie können vorhandene Berichte weder anzeigen noch herunterladen oder neue Berichte erstellen.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Trusted Advisor oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Trusted Advisor-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Trusted Advisor alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Trusted Advisor bereitgestellten Tools deaktivieren können.

Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Trusted Advisor-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die Trusted Advisor-Konsole

Siehe Organisationsansicht deaktivieren im AWS Support-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Trusted Advisor als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für Trusted Advisor

Wenn Sie ein Mitgliedskonto als delegierter Administrator für die Organisation festlegen, können Benutzer und Rollen des angegebenen Kontos die AWS-Konto-Metadaten für andere Mitgliedskonten in der Organisation verwalten. Wenn Sie ein delegiertes Administratorkonto nicht aktivieren, können diese Aufgaben nur vom Verwaltungskonto der Organisation ausgeführt werden. Dies hilft Ihnen, die Verwaltung der Organisation von der Verwaltung Ihrer Kontodetails zu trennen.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Trusted Advisor in der Organisation konfigurieren.

Anweisungen zum Aktivieren eines delegierten Administratorkontos für Trusted Advisor finden Sie unter Registrieren delegierter Administratoren im AWS Support-Benutzerhandbuch.

AWS CLI, AWS API

Wenn Sie ein delegiertes Administratorkonto mit der AWS CLI oder einem der AWS SDKs konfigurieren möchten, können Sie die folgenden Befehle verwenden:

- AWS CLI:

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

- AWS SDK: Rufen Sie die Organizations-Operation `RegisterDelegatedAdministrator` und die ID-Nummer des Mitgliedskontos auf und identifizieren Sie den Kontoservice-Prinzipal `account.amazonaws.com` als Parameter.

Deaktivieren eines delegierten Administrators für Trusted Advisor

Sie können ein delegiertes Administratorkonto entweder über die Trusted Advisor-Konsole oder mithilfe der Organizations-`DeregisterDelegatedAdministrator`-CLI- oder -SDK-Operation entfernen. Weitere Informationen zum Deaktivieren des delegierten Trusted Advisor-Admin-Kontos mit der Trusted Advisor-Konsole finden Sie unter Aufheben der Registrierung delegierter Administratoren im AWS Support-Benutzerhandbuch.

AWS Well-Architected Tool und AWS Organizations

AWS Well-Architected Tool hilft Ihnen, den Status Ihrer Workloads zu dokumentieren und vergleicht sie mit den neuesten bewährten Methoden für Architektur von AWS.

Das Verwenden von AWS Well-Architected Tool mit Organizations ermöglicht sowohl Kunden von AWS Well-Architected Tool und Organizations, den Freigabeprozess von AWS Well-Architected Tool-Ressourcen mit anderen Mitgliedern ihrer Organisation zu vereinfachen.

Weitere Informationen finden Sie unter Freigeben Ihrer AWS Well-Architected Tool-Ressourcen im AWS Well-Architected Tool-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um AWS Well-Architected Tool mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann AWS WA Tool unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen AWS WA Tool und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForWellArchitected`

Die Servicerollenrichtlinie lautet `AWSWellArchitectedOrganizationsServiceRolePolicy`

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von AWS WA Tool verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `wellarchitected.amazonaws.com`

Den vertrauenswürdigen Zugriff mit AWS WA Tool aktivieren

Ermöglicht die Aktualisierung von AWS WA Tool, um hierarchische Veränderungen in einer Organisation wiederzugeben.

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die AWS Well-Architected Tool-Konsole oder über die AWS Organizations-Konsole aktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Well-Architected Tool-Konsole oder Tools verwenden, um die Integration mit Organisationen zu ermöglichen. Auf diese Weise kann AWS Well-Architected Tool jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Well-Architected Tool bereitgestellten Tools aktivieren können. Weitere Informationen sind in diesem Hinweis zu finden.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Well-Architected Tool-Konsole oder der Tools aktivieren, müssen Sie diese Schritte nicht ausführen.

So aktivieren Sie den vertrauenswürdigen Zugriff über die AWS WA Tool-Konsole

Siehe Freigeben Ihrer AWS Well-Architected Tool-Ressourcen im AWS Well-Architected Tool-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für AWS Well-Architected Tool, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von AWS Well-Architected Tool, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Well-Architected Tool als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.
- AWS-API: EnableAWSServiceAccess

Deaktivieren des vertrauenswürdigen Zugriffs mit AWS WA Tool

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder mit den Tools AWS Well-Architected Tool oder AWS Organizations deaktivieren.

> **Important**
>
> Wir empfehlen dringend, dass Sie nach Möglichkeit die AWS Well-Architected Tool-Konsole oder Tools verwenden, um die Integration mit Organisationen zu deaktivieren. Auf diese Weise kann AWS Well-Architected Tool alle erforderlichen Bereinigungen durchführen, z. B. das Löschen von Ressourcen oder Zugriffsrollen, die vom Service nicht mehr benötigt werden. Fahren Sie mit diesen Schritten nur fort, wenn Sie die Integration nicht mit den von AWS Well-Architected Tool bereitgestellten Tools deaktivieren können.
> Wenn Sie den vertrauenswürdigen Zugriff mithilfe der AWS Well-Architected Tool-Konsole oder der Tools deaktivieren, müssen Sie diese Schritte nicht ausführen.

So deaktivieren Sie den vertrauenswürdigen Zugriff über die AWS WA Tool-Konsole

Siehe Freigeben Ihrer AWS Well-Architected Tool-Ressourcen im AWS Well-Architected Tool-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

  Sie können den folgenden Befehl ausführen, um AWS Well-Architected Tool als vertrauenswürdigen Service für Organizations zu deaktivieren.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Amazon VPC IP Address Manager (IPAM) und AWS Organizations

Amazon VPC IP-Adressenmanager (IPAM) ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre AWS-Workloads zu planen, zu verfolgen und zu überwachen.

Mit AWS Organizations können Sie die IP-Adressverwendung in Ihrer Organisation überwachen und IP-Adresspools zwischen den Mitgliedskonten teilen.

Weitere Informationen finden Sie unter Integrieren von IPAM mit AWS Organizations im Amazon-VPC-IPAM-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Amazon VPC IP Adress Manager (IPAM) mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende servicegebundene Rolle wird automatisch im Verwaltungskonto Ihrer Organisation und in jedem Mitgliedskonto erstellt, wenn Sie IPAM mit AWS Organizations integrieren, entweder mit der IPAM-Konsole oder mit IPAMs `EnableIpamOrganizationAdminAccount`-API.

- `AWSServiceRoleForIPAM`

Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für IPAM im Amazon-VPC-IPAM-Benutzerhandbuch.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die von IPAM verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `ipam.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit IPAM

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

> **Note**
>
> Wenn Sie einen delegierten Administrator für IPAM festlegen, aktiviert er automatisch den vertrauenswürdigen Zugriff für IPAM in Ihrer Organisation.
> IPAM erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

Sie können den vertrauenswürdigen Zugriff nur mit Tools von Amazon VPC IP Address Manager (IPAM) aktivieren.

Wenn Sie IPAM über die IPAM-Konsole oder die IPAM `EnableIpamOrganizationAdminAccount` API mit AWS Organizations integrieren, gewähren Sie automatisch vertrauenswürdigen

Zugriff auf IPAM. Wenn Sie vertrauenswürdigen Zugriff gewähren, wird die serviceverknüpfte Rolle `AWSServiceRoleForIPAM` im Verwaltungskonto und in allen Mitgliedskonten in der Organisation erstellt. IPAM verwendet die serviceverknüpfte Rolle, um CIDRs zu überwachen, die mit EC2-Netzwerkressourcen in Ihrem Unternehmen verbunden sind, und um Metriken im Zusammenhang mit IPAM in Amazon CloudWatch zu speichern. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für IPAM im Amazon-VPC-IPAM-Benutzerhandbuch.

Anweisungen zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Integrieren von IPAM mit AWS Organizations im Amazon-VPC-IPAM-Benutzerhandbuch.

> **Note**
>
> Sie können den vertrauenswürdigen Zugriff mit IPAM nicht über die AWS Organizations-Konsole oder mit der `EnableAWSServiceAccess`-API aktivieren.

So deaktivieren Sie den vertrauenswürdigen Zugriff mit IPAM

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Nur ein Administrator im AWS Organizations-Verwaltungskonto kann den vertrauenswürdigen Zugriff mit IPAM mit der AWS Organizations `disable-aws-service-access` API deaktivieren.

Weitere Informationen zum Deaktivieren von IPAM-Kontoberechtigungen und zum Löschen der serviceverknüpften Rolle finden Sie unter Serviceverknüpfte Rollen für IPAM im Amazon-VPC-IPAM-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff deaktivieren, indem Sie einen Organizations-AWS CLI-Befehl ausführen oder einen Organizations-API-Vorgang in einem der AWS-SDKs aufrufen.

AWS CLI, AWS API

So deaktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff deaktivieren:

- AWS CLI: disable-aws-service-access

Sie können den folgenden Befehl ausführen, um Amazon VPC IP Address Manager (IPAM) als vertrauenswürdigen Service für Organizations zu deaktivieren.

```
$ aws organizations disable-aws-service-access \
    --service-principal ipam.amazonaws.com
```

Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: DisableAWSServiceAccess

Aktivieren eines delegierten Administratorkontos für IPAM

Das delegierte Administratorkonto für IPAM ist verantwortlich für die Erstellung der IPAM- und IP-Adresspools, die Verwaltung und Überwachung der IP-Adressennutzung in der Organisation und die Freigabe von IP-Adresspools über Mitgliedskonten hinweg. Weitere Informationen finden Sie unter Integrieren von IPAM mit AWS Organizations im Amazon-VPC-IPAM-Benutzerhandbuch.

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für IPAM konfigurieren.

Sie können ein delegiertes Administratorkonto über die IPAM-Konsole oder über die `enable-ipam-organization-admin-account` API festlegen. Weitere Informationen finden Sie unter enable-ipam-organization-admin-account in der AWS AWS CLI Befehlsreferenz.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für IPAM in der Organisation konfigurieren.

Informationen zum Konfigurieren eines delegierten Administrators mithilfe der IPAM-Konsole finden Sie unter Integrieren von IPAM mit AWS Organizations im Amazon-VPC-IPAM-Benutzerhandbuch.

Deaktivieren eines delegierten Administrators für IPAM

Nur ein Administrator im Organisationsverwaltungskonto kann einen delegierten Administrator für IPAM konfigurieren.

Informationen zum Entfernen eines delegierten Administrators mithilfe der AWS AWS CLI finden Sie unter disable-ipam-organization-admin-account in der AWS AWS CLI-Befehlsreferenz.

Informationen zum Deaktivieren eines delegierten Administratorkontos mithilfe der IPAM-Konsole finden Sie unter Integrieren von IPAM mit AWS Organizations im Amazon-VPC-IPAM-Benutzerhandbuch.

Amazon VPC Reachability Analyzer und AWS Organizations

Reachability Analyzer ist ein Tool zur Konfigurationsanalyse, mit dem Sie Konnektivitätstests zwischen einer Quellressource und einer Zielressource in Ihren Virtual Private Clouds (VPCs) durchführen können.

Durch die Verwendung von AWS Organizations mit Reachability Analyzer können Sie Pfade zwischen Konten in Ihren Organisationen verfolgen.

Weitere Informationen finden Sie unter Kontoübergreifende Analysen für Reachability Analyzer im Reachability-Analyzer-Benutzerhandbuch.

Verwenden Sie die folgenden Informationen, um Reachability Analyzer mit AWS Organizations zu integrieren.

Service-verknüpfte Rollen, die erstellt werden, wenn Sie die Integration aktivieren

Die folgende serviceverknüpfte Rolle wird automatisch im Verwaltungskonto Ihrer Organisation erstellt, wenn Sie den vertrauenswürdigen Zugriff aktivieren. Mit dieser Rolle kann Reachability Analyzer unterstützte Vorgänge innerhalb der Konten Ihrer Organisation in Ihrer Organisation ausführen.

Sie können diese Rolle nur löschen oder ändern, wenn Sie den vertrauenswürdigen Zugriff zwischen Reachability Analyzer und Organizations deaktivieren oder das Mitgliedskonto aus der Organisation entfernen.

- `AWSServiceRoleForReachabilityAnalyzer`

Weitere Informationen finden Sie unter Kontoübergreifende Analysen für Reachability Analyzer im Reachability-Analyzer-Benutzerhandbuch.

Serviceprinzipale, die von den serviceverknüpften Rollen verwendet werden

Die serviceverknüpfte Rolle im vorherigen Abschnitt kann nur von den Serviceprinzipalen übernommen werden, die durch die für die Rolle definierten Vertrauensstellungen autorisiert sind. Die

von Reachability Analyzer verwendeten serviceverknüpften Rollen gewähren Zugriff auf die folgenden Serviceprinzipale:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

So aktivieren Sie den vertrauenswürdigen Zugriff mit Reachability Analyzer

Informationen zu den Berechtigungen, die zum Aktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Aktivieren des vertrauenswürdigen Zugriffs.

Wenn Sie einen delegierten Administrator für Reachability Analyzer festlegen, aktiviert er automatisch den vertrauenswürdigen Zugriff für Reachability Analyzer in Ihrer Organisation.

Reachability Analyzer erfordert vertrauenswürdigen Zugriff auf AWS Organizations, bevor Sie ein Mitgliedskonto als delegierten Administrator für diesen Service für Ihre Organisation festlegen können.

Important

- Sie können den vertrauenswürdigen Zugriff entweder über die Reachability-Analyzer-Konsole oder über die Organizations-Konsole aktivieren. Wir empfehlen dringend, dass Sie die Reachability-Analyzer-Konsole oder die `EnableMultiAccountAnalysisForAwsOrganization`-API verwenden, um die Integration mit Organizations zu ermöglichen. Auf diese Weise kann Reachability Analyzer jede erforderliche Konfiguration ausführen, z. B. die vom Service benötigten Ressourcen erstellen.
- Wenn Sie vertrauenswürdigen Zugriff gewähren, wird die serviceverknüpfte Rolle `AWSServiceRoleForReachabilityAnalyzer` im Verwaltungskonto und in allen Mitgliedskonten in der Organisation erstellt. Reachability Analyzer verwendet die serviceverknüpfte Rolle, um das Management zu ermöglichen, und den delegierten Administrator, um Konnektivitätsanalysen zwischen beliebigen Ressourcen in der Organisation durchzuführen. Reachability Analyzer ist in der Lage, Snapshots der Netzwerkelemente der Konten in einer Organisation zu erstellen, um Konnektivitätsanfragen zu beantworten.
- Weitere Informationen und Anweisungen zur Aktivierung des vertrauenswürdigen Zugriffs über Reachability Analyzer finden Sie unter Kontoübergreifende Analysen für Reachability Analyzer im Reachability-Analyzer-Benutzerhandbuch.

Sie können den vertrauenswürdigen Zugriff aktivieren, indem Sie entweder die AWS Organizations-Konsole verwenden, einen AWS CLI-Befehl ausführen oder einen API-Vorgang in einem der AWS-SDKs aufrufen.

AWS Management Console

So aktivieren Sie den vertrauenswürdigen Service-Zugriff über die Organizations-Konsole

1. Melden Sie sich an der AWS Organizations-Konsole an. Sie müssen sich im Verwaltungskonto der Organisation als IAM-Benutzer anmelden, eine IAM-Rolle annehmen oder als Root-Benutzer anmelden (nicht empfohlen).
2. Suchen Sie auf der Seite Services die Zeile für VPC Reachability Analyzer, wählen Sie den Namen des Services aus und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren aus.
3. Aktivieren Sie im Bestätigungsdialogfeld Option zum Aktivieren des vertrauenswürdigen Zugriffs anzeigen, geben Sie **`enable`** in das Feld ein und wählen Sie dann Vertrauenswürdigen Zugriff aktivieren.
4. Wenn Sie nur der Administrator von AWS Organizations sind, informieren Sie den Administrator von Reachability Analyzer, dass sie diesen Service jetzt über seine Konsole aktivieren können, um mit AWS Organizations zu arbeiten.

AWS CLI, AWS API

So aktivieren Sie den vertrauenswürdigen Servicezugriff mithilfe der Organizations-CLI/SDK

Mit den folgenden AWS CLI-Befehlen oder API-Operationen können Sie den vertrauenswürdigen Servicezugriff aktivieren:

- AWS CLI: enable-aws-service-access

  Sie können den folgenden Befehl ausführen, um Reachability Analyzer als vertrauenswürdigen Service für Organizations zu aktivieren.

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

  Dieser Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

- AWS-API: EnableAWSServiceAccess

So deaktivieren Sie den vertrauenswürdigen Zugriff mit Reachability Analyzer

Informationen zu den Berechtigungen zum Deaktivieren des vertrauenswürdigen Zugriffs finden Sie unter Erforderliche Berechtigungen für das Deaktivieren des vertrauenswürdigen Zugriffs.

Sie können den vertrauenswürdigen Zugriff entweder über die Reachability-Analyzer-Konsole (empfohlen) oder über die Organizations-Konsole deaktivieren. Informationen zum Deaktivieren des vertrauenswürdigen Zugriffs mithilfe der Reachability-Analyzer-Konsole finden Sie unter Kontoübergreifende Analysen für Reachability Analyzer im Reachability-Analyzer-Benutzerhandbuch.

So aktivieren Sie ein Konto für den delegierte Administrator für Reachability Analyzer

Das Konto für den delegierten Administrator ist in der Lage, Konnektivitätsanalysen für alle Ressourcen in der Organisation durchzuführen. Weitere Informationen finden Sie unter Integrieren von Reachability Analyzer mit AWS Organizations im Reachability-Analyzer-Benutzerhandbuch.

Nur ein Administrator im Organizations-Verwaltungskonto kann einen delegierten Administrator für Reachability Analyzer konfigurieren.

Sie können ein Konto für den delegierten Administrator über die Reachability-Analyzer-Konsole oder über die `RegisterDelegatedAdministrator`-API festlegen. Weitere Informationen finden Sie unter RegisterDelegatedAdministrator in der Organizations-Befehlsreferenz.

> **Mindestberechtigungen**
>
> Nur ein Benutzer oder eine Rolle im Organizations-Verwaltungskonto kann ein Mitgliedskonto als delegierter Administrator für Reachability Analyzer in der Organisation konfigurieren.

Informationen zur Konfiguration eines delegierten Administrators mithilfe der Reachability-Analyzer-Konsole finden Sie unter Integrieren von Reachability Analyzer mit AWS Organizations im Reachability-Analyzer-Benutzerhandbuch.

Deaktivieren eines delegierten Administrators für Reachability Analyzer

Nur ein Administrator im Organizations-Verwaltungskonto kann einen delegierten Administrator für Reachability Analyzer konfigurieren.

Sie können ein Konto für den delegierten Administrator entweder über die Reachability-Analyzer-Konsole oder API oder mithilfe der Organizations-`DeregisterDelegatedAdministrator`CLI- oder SDK-Operation entfernen.

Informationen zum Deaktivieren des Kontos für den delegierten Administrator von Reachability Analyzer mithilfe der Reachability-Analyzer-Konsole finden Sie unter Kontoübergreifende Analysen für Reachability Analyzer im Reachability-Analyzer-Benutzerhandbuch.

Delegierter Administrator für AWS-Services, die mit Organizations zusammenarbeiten

Wir empfehlen, das Verwaltungskonto von AWS Organizations und die zugehörigen Benutzer und Rollen nur für Aufgaben zu verwenden, die über dieses Konto ausgeführt werden müssen. Außerdem sollten Sie die AWS-Ressourcen in anderen Mitgliedskonten in der Organisation speichern und sie aus dem Verwaltungskonto heraushalten. Der Grund dafür ist, dass Sicherheitsfeatures wie die Service-Kontrollrichtlinien (SCPs) von Organizations die Benutzer oder Rollen im Verwaltungskonto nicht einschränken. Durch die Trennung der Ressourcen vom Verwaltungskonto können Sie außerdem die Kosten auf Ihren Rechnungen leichter nachvollziehen.

Viele AWS-Services, die in Organizations integriert sind, ermöglichen es Ihnen, die Nutzung des Verwaltungskontos zu reduzieren. Mithilfe dieser Services können Sie ein oder mehrere Mitgliedskonten als Administratoren registrieren, die alle im Service verwendeten Konten der Organisation verwalten können. Diese Konten werden als delegierte Administratoren für den betreffenden Service bezeichnet. Durch die Registrierung eines Mitgliedskontos als delegierten Administrator für einen AWS-Service gewähren Sie diesem Konto einige Administratorberechtigungen für den Service sowie reine Leseberechtigungen für Organizations.

Führen Sie folgende Schritte aus, bevor Sie ein Konto als delegierten Administrator für einen Service registrieren:

- Vergewissern Sie sich, dass der Service delegierte Administratoren unterstützt. Der Tabelle unter AWS Dienste, die Sie mit verwenden können AWS Organizations können Sie entnehmen, welche Services delegierte Administratoren unterstützen.
- Aktivieren Sie vertrauenswürdigen Zugriff für den betreffenden Service.

> **Note**
>
> Um zu erfahren, wie Sie einen delegierten Administrator für einen Service aktivieren, rufen Sie die Tabelle unter AWS Dienste, die Sie mit verwenden können AWS Organizations

auf und wählen Sie den Link Weitere Informationen in der Spalte Unterstützt delegierten Administrator für den jeweiligen Service aus.

An Konten für delegierte Administratoren erteilte Berechtigungen

Jedes servicespezifische Konto für einen delegierte Administrator verfügt über Berechtigungen, die vom betreffenden Service erteilt werden. Um mehr zu erfahren, rufen Sie die Tabelle unter AWS Dienste, die Sie mit verwenden können AWS Organizations auf und wählen Sie den Link Weitere Informationen in der Spalte Unterstützt delegierten Administrator für den jeweiligen Service aus.

Ein Konto für einen delegierten Administrator verfügt außerdem über die folgenden reinen Leseberechtigungen:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`

- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

Mit diesen Berechtigungen lassen sich die folgenden Konsolenelemente anzeigen, aber nicht ändern:

- Organisationsstruktur, alle Konten und Organisationseinheiten sowie Organisationsrichtlinien
- Mitgliedschaften
- Alle Konten und Organisationseinheiten
- Organisationsrichtlinien

Sicherheit in AWS Organizations

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Organizations, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- 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 erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Organizations zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Organizations zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere AWS Dienste nutzen können, mit denen Sie die Ressourcen Ihres Unternehmens überwachen und sichern können.

Themen

- AWS PrivateLink für AWS Organizations
- AWS Identity and Access Management und AWS Organizations
- Protokollieren und Überwachen in AWS Organizations
- Compliance-Validierung für AWS Organizations
- Ausfallsicherheit in AWS Organizations
- Sicherheit der Infrastruktur in AWS Organizations

AWS PrivateLink für AWS Organizations

Mit AWS PrivateLink for AWS Organizations können Sie von der Virtual Private Cloud (VPC) aus auf den AWS Organizations Service zugreifen, ohne das öffentliche Internet überqueren 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 zu VPCs finden Sie im Amazon-VPC-Benutzerhandbuch.

Um Ihre Amazon-VPC mit zu verbinden AWS Organizations, müssen Sie zunächst einen VPC-Schnittstellen-Endpunkt (Schnittstellen-Endpunkte) definieren. Schnittstellenendpunkte werden durch eine oder mehrere Elastic Network-Schnittstellen (ENIs) repräsentiert, denen private IP-Adressen aus Subnetzen in Ihrer VPC zugewiesen werden. Anfragen von Ihrer VPC an Endpunkte AWS Organizations über Schnittstellen verbleiben im Amazon-Netzwerk.

Allgemeine Informationen zu Schnittstellenendpunkten finden Sie unter Zugreifen auf einen AWS Service mithilfe eines Schnittstellen-VPC-Endpunkts im Amazon VPC-Benutzerhandbuch.

Themen

- Einschränkungen und Einschränkungen von für AWS PrivateLinkAWS Organizations
- Erstellung eines VPC-Endpunkts
- Erstellen einer VPC-Endpunktrichtlinie für AWS Organizations

Einschränkungen und Einschränkungen von für AWS PrivateLinkAWS Organizations

VPC-Einschränkungen gelten AWS PrivateLink für AWS Organizations. Weitere Informationen finden Sie unter Zugreifen auf einen AWS Service über eine Schnittstelle, VPC-Endpunkt und AWS PrivateLink Kontingente im Amazon VPC-Benutzerhandbuch. Darüber hinaus gelten die folgenden Einschränkungen:

- Nur in der Region verfügbar `us-east-1`
- Unterstützt Transport Layer Security (TLS) 1.1 nicht

Erstellung eines VPC-Endpunkts

Sie können einen AWS Organizations Endpunkt in Ihrer VPC mithilfe der Amazon VPC-Konsole, dem AWS Command Line Interface (AWS CLI) oder, erstellen. AWS CloudFormation

Informationen zum Erstellen und Konfigurieren eines Endpunkts mithilfe der Amazon VPC-Konsole oder der AWS CLI finden Sie unter Erstellen eines VPC-Endpunkts im Amazon VPC-Benutzerhandbuch. Informationen zum Erstellen und Konfigurieren eines Endpunkts mithilfe AWS CloudFormation von finden Sie in der Ressource AWS: :EC2: :VpcEndpoint im Benutzerhandbuch.AWS CloudFormation

Wenn Sie einen AWS Organizations Endpunkt erstellen, verwenden Sie Folgendes als Servicenamen:

```
com.amazonaws.us-east-1.organizations
```

Wenn Sie für den Zugriff FIPS 140-2-validierte kryptografische Module benötigen AWS, verwenden Sie den folgenden AWS Organizations FIPS-Dienstnamen:

```
com.amazonaws.us-east-1.organizations-fips
```

Erstellen einer VPC-Endpunktrichtlinie für AWS Organizations

Sie können Ihrem VPC-Endpunkt eine Endpunktrichtlinie hinzufügen, die den Zugriff auf Organizations steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für AWS Organizations -Aktionen

```
{
   "Statement":[
      {
```

```
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management und AWS Organizations

Für den Zugriff auf AWS Organizations sind Anmeldeinformationen erforderlich. Diese Anmeldeinformationen müssen Berechtigungen für den Zugriff auf AWS-Ressourcen haben, wie ein Bucket von Amazon Simple Storage Service (Amazon S3), eine Amazon-Elastic-Compute-Cloud (Amazon EC2)-Instance oder eine AWS Organizations-Organisationseinheit. In den folgenden Abschnitten wird beschrieben, wie Sie mit AWS Identity and Access Management (IAM) den Zugriff auf Ihre Organisation schützen und kontrollieren können, wer sie verwaltet.

Um festzulegen, wer welche Teile Ihrer Organisation verwalten kann, nutzt AWS Organizations dasselbe IAM-basierte Berechtigungsmodell wie andere AWS-Services. Als Administrator im Verwaltungskonto einer Organisation können Sie IAM-basierte Berechtigungen zum Ausführen von AWS Organizations-Aufgaben erteilen, indem Sie Benutzern, Gruppen und Rollen im Verwaltungskonto Richtlinien zuordnen. Diese Richtlinien geben die Aktionen an, die diese Prinzipale ausführen können. Sie hängen eine IAM-Berechtigungsrichtlinie an eine Gruppe an, der der Benutzer angehört, oder direkt an einen Benutzer oder eine Rolle. Als bewährte Methode empfehlen wir, die Richtlinien an Gruppen statt an Benutzer anzuhängen. Sie haben auch die Möglichkeit, anderen Benutzern vollständige Administratorberechtigungen zu gewähren.

Für die meisten Administratoroperationen für AWS Organizations müssen Sie Berechtigungen an Benutzer oder Gruppen im Verwaltungskonto anfügen. Wenn ein Benutzer in einem Mitgliedskonto Administratorvorgänge für Ihre Organisation ausführen muss, müssen Sie einer IAM-Rolle im Verwaltungskonto die AWS Organizations-Berechtigungen erteilen und dem Benutzer im Mitgliedskonto ermöglichen, die Rolle zu übernehmen. Allgemeine Informationen zu IAM-Berechtigungsrichtlinien finden Sie in der Übersicht über die IAM-Richtlinien im IAM-Benutzerhandbuch.

Themen

- Authentifizierung

- Zugriffskontrolle
- Verwaltung von Zugriffsberechtigungen für Ihre AWS-Organisation
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Organizations
- Attributbasierte Zugriffskontrolle mit Tags und AWS Organizations

Authentifizierung

Sie können mit einer der folgenden Identitäten auf AWS zugreifen:

- AWS-Konto-Stammbenutzer – Wenn Sie sich bei AWS registrieren, geben Sie eine E-Mail-Adresse und ein Passwort an, die mit Ihrem AWS-Konto verknüpft sind. Dies sind Ihre Root-Anmeldeinformationen. Sie bieten vollständigen Zugriff auf alle Ihre AWS-Ressourcen.

  > **Important**
  >
  > Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

- IAM-Benutzer – Ein IAM-Benutzer ist einfach eine Identität in Ihrem AWS-Konto, die über bestimmte benutzerdefinierte Berechtigungen verfügt (z. B. Berechtigungen zum Erstellen eines Dateisystems in Amazon Elastic File System). Sie können einen IAM-Benutzernamen und ein Passwort für die Anmeldung bei sicheren AWS-Webseiten verwenden. Dazu zählen beispielsweise die AWS Management Console, AWS-Diskussionsforen und das AWS-Supportcenter.

  Zusätzlich zu einem Benutzernamen und Passwort können Sie Zugriffsschlüssel für jeden Benutzer erstellen. Verwenden Sie diese Schlüssel, wenn Sie über AWSeines der verschiedenen SDKs oder über die (AWS Command Line Interface)AWS CLI programmgesteuert auf -Services zugreifen. Das SDK und die AWS CLI-Tools verwenden die Zugriffsschlüssel, um Ihre Anfrage verschlüsselt zu signieren. Wenn Sie die AWS-Tools nicht nutzen, müssen Sie die Anfrage selbst signieren. AWS Organizations unterstützt Signature Version 4, ein Protokoll für die Authentifizierung eingehender API-Anfragen. Weitere Informationen zum Authentifizieren von Anforderungen finden Sie unter Signieren von AWS -API-Anforderungen im IAM-Benutzerhandbuch.
- IAM-Rolle – Eine IAM-Rolle ist eine andere IAM-Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Sie ähnelt einem IAM-Benutzer, ist aber nicht mit einer

bestimmten Person verknüpft. Eine IAM-Rolle ermöglicht Ihnen, temporäre Zugriffsschlüssel zu erhalten, mit denen Sie auf die AWS-Services und -Ressourcen zugreifen können. IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzer-Zugriff – Statt einen IAM-Benutzer zu erstellen, können Sie bereits vorhandene Benutzeridentitäten von AWS Directory Service, dem Benutzerverzeichnis Ihres Unternehmens oder von einem Web-Identitätsanbieter verwenden. Diese werden als Verbundbenutzer bezeichnet. AWS weist einem Verbundbenutzer eine Rolle zu, wenn Zugriff über einen Identitätsanbieter angefordert wird. Weitere Informationen zu Verbundbenutzern finden Sie unter Verbundbenutzer und Rollen im IAM-Benutzerhandbuch.
- Kontenübergreifender Zugriff – Sie können eine IAM-Rolle in Ihrem Konto verwenden, um einem anderen AWS-Konto Berechtigungen für den Zugriff auf die Ressourcen Ihres Kontos zu erteilen. Ein Beispiel finden Sie unter Tutorial: Delegieren des Zugriffs in mithilfe AWS-Konten von IAM-Rollen im IAM-Benutzerhandbuch.
- Zugriff auf AWS-Services – Sie können eine IAM-Rolle in Ihrem Konto verwenden, um einem AWS-Service Berechtigungen für den Zugriff auf die Ressourcen Ihres Konto zu erteilen. Sie können beispielsweise eine Rolle erstellen, mit der Amazon Redshift in Ihrem Namen auf einen Amazon-S3-Bucket zugreifen und die im Bucket gespeicherten Daten in einen Amazon-Redshift-Cluster laden kann. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Anwendungen in Amazon EC2 – Anstatt Zugriffsschlüssel in der EC2-Instance zu speichern, die von den dort ausgeführten Anwendungen zum Senden von AWS-API-Anforderungen verwendet werden, können Sie eine IAM-Rolle nutzen, um temporäre Anmeldeinformationen für diese Anwendungen zu verwalten. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle zu einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2 Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen zur Authentifizierung Ihrer Anfragen verfügen, doch Sie können die AWS Organizations-Ressourcen nur mit entsprechenden Berechtigungen verwalten

oder darauf zugreifen. Sie müssen z. B. über Berechtigungen verfügen, um eine OU zu erstellen oder eine Service-Kontrollrichtlinie (SCP) an ein Konto anzuhängen.

In den folgenden Abschnitten wird die Verwaltung von Berechtigungen für AWS Organizations beschrieben.

- Verwaltung von Zugriffsberechtigungen für Ihre AWS-Organisation
- Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Organizations
- Attributbasierte Zugriffskontrolle mit Tags und AWS Organizations

Verwaltung von Zugriffsberechtigungen für Ihre AWS-Organisation

Alle AWS-Ressourcen, einschließlich der Root-Benutzer, der Organisationseinheiten, der Konten und der Richtlinien in einer Organisation, gehören einem AWS-Konto. Die Berechtigungen zum Erstellen einer Ressource oder zum Zugriff auf eine Ressource werden durch Berechtigungsrichtlinien gesteuert. In einer Organisation ist das Verwaltungskonto Eigentümer aller Ressourcen. Ein Kontoadministrator kann den Zugriff auf AWS-Ressourcen steuern, indem er Berechtigungsrichtlinien zu IAM-Identitäten (Benutzer, Gruppen und Rollen) zuweist.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorberechtigungen. Weitere Informationen finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Beim Erteilen von Berechtigungen entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen die Berechtigungen gelten und welche Aktionen an diesen Ressourcen gestattet werden sollen.

Standardmäßig haben IAM-Benutzer, -Gruppen und -Rollen keine Berechtigungen. Als Administrator im Verwaltungskonto einer Organisation können Sie administrative Aufgaben durchführen oder Administrationsberechtigungen an andere IAM-Benutzer oder -Rollen im Verwaltungskonto delegieren. Fügen Sie hier eine IAM-Berechtigungsrichtlinie an einen IAM-Benutzer, eine -Gruppe oder eine -Rolle an. Standardmäßig hat ein Benutzer keine Berechtigungen (implizite Verweigerung). Die Richtlinie überschreibt die implizite Verweigerung mit einer expliziten Zulassung. Diese legt fest, welche Aktionen der Benutzer für welche Ressourcen ausführen kann. Wenn einer Rolle die

Berechtigungen erteilt werden, können die Benutzer in anderen Konten der Organisation diese Rolle annehmen.

AWS Organizations-Ressourcen und -Operationen

In diesem Abschnitt wird die Zuordnung der AWS Organizations-Konzepte zu den entsprechenden IAM-Konzepten erläutert.

Ressourcen

In AWS Organizations können Sie den Zugriff auf die folgenden Ressourcen steuern:

- Der Root-Benutzer und die OUs, aus denen die hierarchische Struktur einer Organisation besteht
- Die Konten, die Mitglieder einer Organisation sind
- Die Richtlinien, die Sie an die Entitäten der Organisation anhängen
- Die Handshakes, die Sie zum Ändern des Status der Organisation verwenden

Jeder dieser Ressourcen ist ein eindeutiger Amazon-Ressourcenname (ARN) zugeordnet. Sie steuern den Zugriff auf eine Ressource, indem Sie dessen ARN im `Resource`-Element einer IAM-Berechtigung angeben. Eine vollständige Liste der ARN-Formate für Ressourcen, die in verwendet werdenAWS Organizations, finden Sie unter Von definierte Ressourcentypen AWS Organizations in der Service-Autorisierungs-Referenz.

Operationen

AWS stellt verschiedene Vorgänge zur Arbeit mit den Ressourcen in einer Organisation bereit. Diese ermöglichen Ihnen die Durchführung von Aktivitäten wie das Erstellen, Auflisten, Ändern, Zugreifen auf Inhalte und das Löschen von Ressourcen. Die Berechtigungen für die meisten Vorgänge können über das `Action`-Element einer IAM-Richtlinie gesteuert werden. Eine Liste der AWS Organizations Operationen, die als Berechtigungen in einer IAM-Richtlinie verwendet werden können, finden Sie unter Von AWS Organizations definierte Aktionen in der Service-Autorisierungs-Referenz.

Wenn Sie eine `Action` und eine `Resource` in einem einzigen Berechtigungsrichtlinien-`Statement` kombinieren, können Sie genau steuern, für welche Ressourcen die entsprechenden Aktionen genutzt werden können.

Bedingungsschlüssel

AWS bietet Bedingungsschlüssel, die Sie abfragen können, um über differenziertere Steuerungsmöglichkeiten über bestimmte Aktionen zu verfügen. Sie können auf diese

Bedingungsschlüssel im `Condition`-Element einer IAM-Richtlinie verweisen, um die zusätzlichen Voraussetzungen anzugeben, die erfüllt sein müssen, bevor die Anweisung als zutreffend gilt.

Die folgenden Bedingungsschlüssel sind besonders nützlich für AWS Organizations:

- `aws:PrincipalOrgID` – Vereinfacht die Angabe des `Principal`-Elements in einer ressourcenbasierten Richtlinie. Dieser globale Schlüssel stellt eine Alternative zum Auflisten aller Konto-IDs für alle AWS-Konten in einer Organisation dar. Anstatt alle Konten, die Mitglieder einer Organisation sind, aufzulisten, können Sie die Organisations-ID im `Condition`-Element angeben.

  > **Note**
  >
  > Diese globale Bedingung gilt auch für das Verwaltungskonto einer Organisation.

  Weitere Informationen finden Sie in der Beschreibung von `PrincipalOrgID` in AWS globalen Bedingungskontextschlüsseln im IAM-Benutzerhandbuch.
- `aws:PrincipalOrgPaths` – Verwenden Sie diesen Bedingungsschlüssel, um Mitglieder eines bestimmten Organisationsstammes, einer OU oder deren untergeordneten Elemente abzugleichen. Der `aws:PrincipalOrgPaths`-Bedingungsschlüssel gibt „wahr“ zurück, wenn sich der Prinzipal (Stammbenutzer, IAM-Benutzer oder -Rolle), der die Anforderung durchführt, im angegebenen Organisationspfad befindet. Ein Pfad ist eine Textdarstellung der Struktur einer AWS Organizations-Entität. Weitere Informationen zu Pfaden finden Sie unter Verstehen des AWS Organizations Entitätspfads im IAM-Benutzerhandbuch. Weitere Informationen zur Verwendung dieses Bedingungsschlüssels finden Sie unter aws:PrincipalOrgPaths im IAM-Benutzerhandbuch.

  Das folgende Bedingungselement beispielsweise stimmt für Mitglieder einer von zwei OUs in derselben Organisation überein.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "aws:PrincipalOrgPaths": [
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
        ]
    }
}
```

- `organizations:PolicyType` – Mit diesem Bedingungsschlüssel können Sie die richtlinienbezogenen Organizations-API-Vorgänge so einschränken, dass sie nur mit Organizations-Richtlinien des angegebenen Typs funktionieren. Sie können diesen Bedingungsschlüssel auf jede Richtlinienanweisung anwenden, die eine Aktion enthält, die mit Organizations-Richtlinien interagiert.

  Mit diesem Bedingungsschlüssel können Sie die folgenden Werte verwenden:

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

  Mit der folgenden Beispielrichtlinie kann der Benutzer beispielsweise jede Organizations-Operation ausführen. Wenn der Benutzer jedoch einen Vorgang ausführt, der ein Richtlinienargument verwendet, ist der Vorgang nur zulässig, wenn die angegebene Richtlinie eine Tagging-Richtlinie ist. Der Vorgang schlägt fehl, wenn der Benutzer einen anderen Richtlinientyp angibt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal` – Verfügbar als Bedingung, wenn Sie die Operationen AktivierenAWSServiceAccess oder DeaktivierenAWSServiceAccess verwenden, um den vertrauenswürdigen Zugriff mit anderen -AWSServices zu aktivieren oder zu deaktivieren. Sie können `organizations:ServicePrincipal` verwenden, um Anfragen zu begrenzen, die diese Operationen an eine Liste genehmigter Service Prinzipal-Namen richten.

Die folgende Richtlinie beispielsweise erlaubt dem Benutzer nur die Angabe von AWS Firewall Manager, wenn der vertrauenswürdige Zugang mit AWS Organizations aktiviert und deaktiviert wird:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Eine Liste aller AWS Organizations-spezifischen Bedingungsschlüssel, die als Berechtigungen in einer IAM-Richtlinie verwendet werden können, finden Sie unter Bedingungsschlüssel für AWS Organizations in der Service-Autorisierungs-Referenz.

Grundlegendes zum Eigentum an Ressourcen

Das AWS-Konto ist Eigentümer aller Ressourcen, die innerhalb des Kontos erstellt werden, unabhängig davon, wer sie erstellt. Genauer gesagt ist der Ressourcenbesitzer das AWS-Konto der Prinzipal-Entität (der Root-Benutzer, ein IAM-Benutzer oder eine IAM-Rolle), die die Ressourcenerstellungsanforderung authentifiziert. Für eine AWS-Organisation, die immer das Verwaltungskonto ist. Sie können keine Vorgänge aufrufen, die Organisationsressourcen aus anderen Mitgliedskonten erstellen oder auf diese zugreifen. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Stammkonto-Anmeldeinformationen für Ihr Verwaltungskonto verwenden, um eine OU zu erstellen, ist Ihr Verwaltungskonto der Eigentümer der Ressource. (In AWS Organizations ist die Ressource die OU).
- Wenn Sie einen IAM-Benutzer in Ihrem Verwaltungskonto erstellen und diesem Berechtigungen zum Erstellen von OUs erteilen, kann dieser Benutzer eine OU erstellen. Der Eigentümer der OU-Ressource ist jedoch das Verwaltungskonto, dem der Benutzer angehört.
- Wenn Sie in Ihrem Verwaltungskonto eine IAM-Rolle mit Berechtigungen zum Erstellen einer OU einrichten, kann jeder mit der Rolle eine OU erstellen. Der Eigentümer der OU-Ressource ist das Verwaltungskonto, zu dem die Rolle gehört (nicht der Benutzer mit der Rolle).

Verwalten des Zugriffs auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> Dieser Abschnitt behandelt die Verwendung von IAM um Zusammenhang mit AWS Organizations. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie im IAM User Guide. Informationen zur IAM-Richtliniensyntax und Beschreibungen finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

An eine IAM-Identität angefügte Richtlinien werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. An Ressourcen angefügte Berechtigungsrichtlinien werden als ressourcenbasierte Richtlinien bezeichnet. AWS Organizations unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Identitätsbasierte Berechtigungsrichtlinien (IAM-Richtlinien)
- Ressourcenbasierte Richtlinien

Identitätsbasierte Berechtigungsrichtlinien (IAM-Richtlinien)

Sie können Richtlinien IAM-Identitäten zuweisen, damit diese Identitäten Vorgänge für AWS-Ressourcen ausführen können. Sie können z. B. Folgendes tun:

- Eine Berechtigungsrichtlinie an einen Benutzer oder eine Gruppe in Ihrem Konto anfügen – Um eine Benutzerberechtigung zum Erstellen einer AWS Organizations-Ressource, z. B. eine Service-Kontrollrichtlinie (SCP) oder eine Organisationseinheit (OU), zu erteilen, können Sie einem Benutzer oder einer Gruppe, der der Benutzer angehört, eine Berechtigungsrichtlinie anhängen. Der Benutzer oder die Gruppe muss sich in der Organisation des Verwaltungskontos befinden.
- Eine Berechtigungsrichtlinie zu einer Rolle zuweisen (kontoübergreifende Berechtigungen erteilen) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Zugriffsberechtigungen zu erteilen. Der Administrator im Verwaltungskonto kann beispielsweise folgendermaßen eine Rolle erstellen, um einem Benutzer in einem Mitgliedskonto kontenübergreifende Berechtigungen zu erteilen:
  1. Der Verwaltungskontoadministrator erstellt eine IAM-Rolle und fügt dieser eine Berechtigungsrichtlinie an, die die Berechtigungen für die Ressourcen der Organisation erteilt.
  2. Der Verwaltungskontoadministrator fügt der Rolle eine Vertrauensrichtlinie hinzu. Diese definiert die Mitgliedskonto-ID des `Principal`, der die Rolle annehmen darf.
  3. Der Mitgliedskontoadministrator kann dann die Berechtigung zum Annehmen der Rolle an jegliche Benutzer im Mitgliedskonto delegieren. Dadurch können Benutzer im Mitgliedskonto Ressourcen im Verwaltungskkonto und in der Organisation erstellen oder auf diese zugreifen. Wenn Sie einem AWS-Service die Berechtigungen zum Annehmen der Rolle erteilen möchten, kann es sich bei dem Prinzipal in der Vertrauensrichtlinie auch um ein AWS-Service-Prinzipal handeln.

  Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Die folgenden Beispiele zeigen Richtlinien, die Benutzern das Ausführen der Aktion `CreateAccount` in Ihrer Organisation gestatten.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
```

```
   ]
}
```

Außerdem können Sie eine Teil-ARN im Element `Resource` der Richtlinie zur Angabe des Ressourcentyps einfügen.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

Darüber hinaus können Sie die Erstellung von Konten verweigern, die keine spezifischen Tags für das zu erstellende Konto enthalten.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter IAM-Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Einige Services (beispielsweise Amazon S3) unterstützen ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem Amazon-S3-Bucket eine ressourcenbasierte Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. AWS Organizations bietet keine Unterstützung für ressourcenbasierte Richtlinien.

Angeben der Richtlinienelemente: Aktionen, Bedingungen, Effekte und Ressourcen

Für jede AWS Organizations-Ressource definiert der Service eine Reihe von API-Operationen oder Aktionen, die mit dieser Ressource interagieren oder sie verändern können. Zur Erteilung von Berechtigungen für diese API-Operationen definiert AWS Organizations Aktionen, die Sie in einer Richtlinie angeben können. Für die OU-Ressource (Organisationseinheit) definiert AWS Organizations zum Beispiel die folgenden Aktionen:

- `AttachPolicy` und `DetachPolicy`
- `CreateOrganizationalUnit` und `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` und `DescribeOrganizationalUnit`

In einigen Fällen erfordert die Durchführung einer API-Operation Berechtigungen für mehr als eine Aktion und Ressource.

Die folgenden grundlegenden Elemente können Sie in einer IAM-Berechtigungsrichtlinie verwenden:

- Aktion – Mit diesem Schlüsselwort können Sie die Operationen (Aktionen) festlegen, die Sie zulassen oder verweigern möchten. Beispielsweise gestattet oder verweigert `organizations:CreateAccount` je nach Einstellung von `Effect` in den Benutzerberechtigungen die Durchführung der AWS Organizations-Operation `CreateAccount`. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Aktion im IAM-Benutzerhandbuch.
- Ressource – Mit diesem Schlüsselwort legen Sie den ARN (Amazon-Ressourcenname) der Ressource fest, für die die Richtlinienanweisung gilt. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Ressource im IAM-Benutzerhandbuch.
- Bedingung – Verwenden Sie dieses Schlüsselwort, um eine Bedingung anzugeben, die erfüllt werden muss, damit die Richtlinienanweisung gilt. `Condition` gibt in der Regel zusätzliche Umstände an, die erfüllt sein müssen, damit die Richtlinie zutrifft. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Effekt – Mit diesem Schlüsselwort geben Sie an, ob die Richtlinienanweisung die Aktion für die Ressource zulässt oder verweigert. Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten (bzw. zulassen), wird er automatisch verweigert. Sie können außerdem den Zugriff auf eine Ressource explizit verweigern. So können Sie gewährleisten, dass ein Benutzer die angegebene Aktion für die definierte Ressource nicht ausführen kann (selbst dann nicht, wenn er über eine andere Richtlinie Zugriff erhält). Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Auswirkung im IAM-Benutzerhandbuch.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). AWS Organizations unterstützt derzeit nur identitätsbasierte Richtlinien. Ressourcenbasierte Richtlinien werden nicht unterstützt.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien) für AWS Organizations

Als Administrator des Verwaltungskontos können Sie den Zugriff auf AWS-Ressourcen steuern, indem Sie Berechtigungsrichtlinien an AWS Identity and Access Management-(IAM)-Identitäten (z. B. Benutzer, Gruppen und Rollen) in der Organisation zuweisen. Beim Erteilen von Berechtigungen entscheiden Sie, wer die Berechtigungen erhält, für welche Ressourcen die Berechtigungen gelten und welche Aktionen an diesen Ressourcen gestattet werden sollen. Wenn einer Rolle die Berechtigungen erteilt werden, können die Benutzer in anderen Konten der Organisation diese Rolle annehmen.

Standardmäßig hat ein Benutzer keinerlei Berechtigungen. Alle Berechtigungen müssen durch eine Richtlinie explizit gewährt werden. Eine Berechtigung, die nicht explizit gewährt wird, wird stillschweigend verweigert. Wenn eine Berechtigung explizit verweigert wird, werden dadurch alle anderen Richtlinien überschrieben, die die Berechtigung möglicherweise zugelassen hätten. Mit anderen Worten, ein Benutzer verfügt nur über die Berechtigungen, die ihm explizit erteilt und nicht explizit verweigert wurden.

Zusätzlich zu den in diesem Thema beschriebenen grundlegenden Techniken können Sie den Zugriff auf Ihre Organisation steuern, indem Sie die Tags verwenden, die auf die Ressourcen in Ihrer Organisation angewendet werden: Organisationsstamm, Organisationseinheiten (OU), Konten und

Richtlinien. Weitere Informationen finden Sie unter Attributbasierte Zugriffskontrolle mit Tags und AWS Organizations.

Erteilen von vollständigen Administratorberechtigungen an einen Benutzer

Sie können eine IAM-Richtlinie erstellen, die einem IAM-Benutzer vollständige AWS Organizations-Administratorberechtigungen in Ihre Organisationen gewährt. Dies kann mithilfe des JSON-Richtlinieneditors in der IAM-Konsole erfolgen.

So verwenden Sie den JSON-Richtlinieneditor zum Erstellen einer Richtlinie

1. Melden Sie sich bei der AWS Management Console an, und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien).

   Wenn Sie zum ersten Mal Policies (Richtlinien) auswählen, erscheint die Seite Welcome to Managed Policies (Willkommen bei verwalteten Richtlinien). Wählen Sie Get Started.
3. Wählen Sie oben auf der Seite Create policy (Richtlinie erstellen) aus.
4. Wählen Sie im Bereich Policy editor (Richtlinien-Editor) die Option JSON aus.
5. Geben Sie folgendes JSON-Richtliniendokument ein:

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

6. Wählen Sie Weiter aus.

> **Note**
>
> Sie können jederzeit zwischen den Editoroptionen Visual und JSON wechseln. Wenn Sie jedoch Änderungen vornehmen oder im Visual-Editor Weiter wählen, strukturiert IAM Ihre Richtlinie möglicherweise um, um sie für den visuellen Editor zu optimieren. Weitere Informationen finden Sie unter Richtlinienrestrukturierung im IAM-Benutzerhandbuch.

7. Geben Sie auf der Seite Prüfen und erstellen unter Richtlinienname einen Namen und unter Beschreibung (optional) eine Beschreibung für die Richtlinie ein, die Sie erstellen. Überprüfen Sie Permissions defined in this policy (In dieser Richtlinie definierte Berechtigungen), um die Berechtigungen einzusehen, die von Ihrer Richtlinie gewährt werden.
8. Wählen Sie Create policy (Richtlinie erstellen) aus, um Ihre neue Richtlinie zu speichern.

Weitere Informationen zum Erstellen einer IAM-Richtlinie finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Gewähren von beschränktem Zugriff durch Aktionen

Wenn Sie einem Benutzer anstelle von vollständigen Berechtigungen eingeschränkte Berechtigungen erteilen möchten, können Sie im `Action`-Element der Richtlinie für IAM-Berechtigungen eine Richtlinie mit den einzelnen Berechtigungen erstellen. Wie im folgenden Beispiel dargestellt, können Sie mithilfe von Platzhaltern (*) der Organisation nur die Berechtigungen `Describe*` und `List*`, d. h. einen schreibgeschütztem Zugriff, erteilen.

> **Note**
>
> In einer Service-Kontrollrichtlinie (SCP) kann der Platzhalter (*) in einem `Action`-Element nur von sich selbst oder am Ende einer Zeichenfolge verwendet werden. Er darf nicht am Anfang oder in der Mitte der Zeichenfolge stehen. Daher ist `"servicename:action*"` gültig, aber `"servicename:*action"` und `"servicename:some*action"` sind in SCPs ungültig.

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

Eine Liste aller Berechtigungen, die in einer IAM-Richtlinie zugewiesen werden können, finden Sie unter Von AWS Organizations definierte Aktionen in der Service-Autorisierungs-Referenz.

Gewähren des Zugriffs auf bestimmte Ressourcen

Sie können den Zugriff auf bestimmte Aktionen und auf bestimmte Entitäten in der Organisation beschränken. In den `Resource`-Elementen aus den beiden Beispielen in den vorherigen Abschnitten werden Platzhalterzeichen (*) angegeben; diese stehen für alle Ressourcen, auf die die Aktion zugreifen darf. Sie können das Platzhalterzeichen "*" auch durch den ARN (Amazon Resource Name) der Entitäten ersetzen, auf die Sie den Zugriff ermöglichen möchten.

Beispiel: Gewähren von Berechtigungen für eine einzelne OU

Die erste Anweisung der folgenden Richtlinie gewährt einem IAM-Benutzer Lesezugriff auf die gesamte Organisation; die zweite Anweisung ermöglicht dem Benutzer lediglich die Ausführung von administrativen Aufgaben in AWS Organizations in einer bestimmten Organisationseinheit (OU). Dies gilt nicht für untergeordnete Organisationseinheiten. Dem Benutzer wird kein Zugriff auf die Buchhaltung gewährt. Beachten Sie, dass dies Ihnen keinen Administratorzugriff auf die AWS-Konten in der OU gewährt. Sie erhalten lediglich die Berechtigung zur Durchführung von AWS Organizations-Operationen auf den Konten innerhalb der angegebenen OU:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

Die IDs für die OU und die Organisation erhalten Sie über die AWS Organizations-Konsole oder durch Aufruf der `List*`-APIs. Der Benutzer oder die Gruppe, der Sie diese Richtlinie zuweisen,

kann beliebige Aktionen (`"organizations:*"`) für beliebige Entitäten direkt in der angegebenen Organisationseinheit ausführen. Die OU wird durch den ARN (Amazon Resource Name) angegeben.

Weitere Informationen zu den ARNs für verschiedene Ressourcen finden Sie unter Von definierte Ressourcentypen AWS Organizations in der Service-Autorisierungs-Referenz.

Erteilen der Fähigkeit zur Aktivierung des vertrauenswürdigen Zugriffs auf eingeschränkte Serviceprinzipale

Sie können das `Condition`-Element einer Richtlinienanweisung verwenden, um die Umstände weiter einzuschränken, für die die Richtlinienanweisung zutrifft.

Beispiel: Erteilen der Berechtigungen zur Aktivierung des vertrauenswürdigen Zugriffs auf einen bestimmten Service

Die folgende Anweisung zeigt, wie Sie die Fähigkeit zur Aktivierung des vertrauenswürdigen Zugriffs auf nur die von Ihnen angegebenen Services einschränken können. Wenn der Benutzer versucht, die API mit einem anderen Serviceprinzipal als dem für AWS IAM Identity Center aufzurufen, trifft diese Richtlinie nicht zu, und die Anforderung wird abgelehnt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
        }
    ]
}
```

Weitere Informationen zu den ARNs für verschiedene Ressourcen finden Sie unter Von definierte Ressourcentypen AWS Organizations in der Service-Autorisierungs-Referenz.

Attributbasierte Zugriffskontrolle mit Tags und AWS Organizations

Mit der attributbasierten Zugriffskontrollek önnen Sie vom Administrator verwaltete Attribute wie Tags, die an AWS-Ressourcen und AWS-Identitäten angefügt sind, verwenden, um den Zugriff auf diese Ressourcen zu steuern. Sie können beispielsweise angeben, dass ein Benutzer auf eine Ressource zugreifen kann, wenn sowohl der Benutzer als auch die Ressource denselben Wert für ein bestimmtes Tag haben.

Markierbare AWS Organizations-Ressourcen beinhalten AWS-Konten-Stamm-Organisationseinheiten (OUs) oder Richtlinien der Organisation. Wenn Sie Tags an Organizationsressourcen anfügen, können Sie diese Tags verwenden, um zu steuern, wer auf diese Ressourcen zugreifen kann. Dazu fügen Sie `Condition`-Elemente zu Ihren AWS Identity and Access Management-Berechtigungsrichtlinienanweisungen (IAM) hinzu, die prüfen, ob bestimmte Tag-Schlüssel und -Werte vorhanden sind, bevor die Aktion zugelassen wird. Auf diese Weise können Sie eine IAM-Richtlinie erstellen, die effektiv besagt: „Benutzer darf nur die OUs verwalten, die ein Tag mit einem Schlüssel `X` und einem Wert `Y` haben“ oder „Benutzern erlauben, nur die OUs zu verwalten, die mit einem Schlüssel `Z` gekennzeichnet sind“ der denselben Wert hat wie der angehängte Tag-Schlüssel `Z` des Benutzers.“

Sie können Ihre `Condition`-Tests auf verschiedenen Typen von Tag-Referenzen in einer IAM-Richtlinie aufbauen.

- Überprüfen der Tags, die den Ressourcen zugeordnet sind, die in der Anforderung angegeben sind
- Überprüfen der Tags, die dem IAM-Benutzer oder -Rolle angefügt sind, der die Anforderung stellt
- Überprüfen Sie die Tags, die als Parameter in der Anforderung enthalten sind

Weitere Informationen zur Verwendung von Tags für die Zugriffssteuerung in Richtlinien finden Sie unter Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Ressourcen-Tags. Die vollständige Syntax der IAM-Berechtigungsrichtlinien finden Sie in der IAM-JSON-Richtlinienreferenz

Überprüfen der Tags, die den Ressourcen zugeordnet sind, die in der Anforderung angegeben sind

Wenn Sie eine Anfrage mit AWS Management Console, AWS Command Line Interface (AWS CLI) oder einem der AWS-SDKs stellen, geben Sie an, auf welche Ressourcen Sie mit dieser Anfrage zugreifen möchten. Unabhängig davon, ob Sie versuchen, verfügbare Ressourcen eines bestimmten Typs aufzulisten, eine Ressource zu lesen oder eine Ressource zu schreiben, zu

ändern oder zu aktualisieren, geben Sie die Ressource als Parameter in der Anforderung an. Solche Anforderungen werden durch IAM-Berechtigungsrichtlinien gesteuert, die Sie Ihren Benutzern und Rollen zuordnen. In diesen Richtlinien können Sie die Tags vergleichen, die der angeforderten Ressource zugeordnet sind, und den Zugriff basierend auf den Schlüsseln und Werten dieser Tags zulassen oder verweigern.

Um ein Tag zu überprüfen, das an die Ressource angehängt ist, verweisen Sie auf das Tag in einem `Condition`-Element durch Voranstellen des Tag-Schlüsselnamens mit der folgenden Zeichenfolge: `aws:ResourceTag/`

Die folgende Beispielrichtlinie ermöglicht es dem Benutzer oder der Rolle beispielsweise, jede AWS Organizations-Operation auszuführen, es sei denn, diese Ressource hat ein Tag mit dem Schlüssel `department` und dem Wert `security`. Wenn dieser Schlüssel und Wert vorhanden ist, verweigert die Richtlinie die Operation `UntagResource` explizit.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

Weitere Informationen zur Verwendung dieses Elements finden Sie unter Steuern des Zugriffs auf Ressource und aws:ResourceTag im IAM-Benutzerhandbuch.

Überprüfen der Tags, die dem IAM-Benutzer oder -Rolle angefügt sind, der die Anforderung stellt

Steuern Sie, welche Aktionen die Person, von der die Anforderung stammt (der Prinzipal), durchführen darf, auf Grundlage der Tags, die dem IAM-Benutzer oder der Rolle der Person angefügt sind. Verwenden Sie dazu die `aws:PrincipalTag/`*`key-name`*, um anzugeben, welcher Tag und welcher Wert dem aufrufenden Benutzer oder der aufrufenden Rolle zugeordnet werden müssen.

Das folgende Beispiel zeigt, wie eine Aktion nur zugelassen wird, wenn das angegebene Tag (`cost-center`) denselben Wert sowohl für den die Operation aufrufenden Prinzipal als auch für die Ressource hat, auf die die Operation zugreift. In diesem Beispiel kann der aufrufende Benutzer eine Amazon-EC2-Instance nur starten und stoppen, wenn die Instance mit demselben `cost-center`-Wert wie der Benutzer gekennzeichnet ist.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Weitere Informationen zur Verwendung dieses Elements finden Sie unter Steuern des Zugriffs für IAM-Prinzipale und `aws:PrincipalTag` im IAM-Benutzerhandbuch.

Überprüfen Sie die Tags, die als Parameter in der Anforderung enthalten sind

Mehrere Operationen ermöglichen es Ihnen, Tags als Teil der Anforderung anzugeben. Wenn Sie beispielsweise eine Ressource erstellen, können Sie die Tags angeben, die der neuen Ressource zugeordnet sind. Sie können ein `Condition`-Element angeben, das `aws:TagKeys` verwendet, um den Vorgang zuzulassen oder zu verweigern, je nachdem, ob ein bestimmter Tag-Schlüssel oder eine Reihe von Schlüsseln in der Anforderung enthalten ist. Diesem Vergleichsoperator ist es egal, welchen Wert das Tag enthält. Es prüft nur, ob ein Tag mit dem angegebenen Schlüssel vorhanden ist.

Um den Tag-Schlüssel oder eine Liste von Schlüsseln zu überprüfen, geben Sie ein `Condition`-Element mit der folgenden Syntax an:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Sie können dem Vergleichsoperator `ForAllValues:` voranstellen, um sicherzustellen, dass alle Schlüssel in der Anforderung mit einem der in der Richtlinie angegebenen Schlüssel übereinstimmen müssen. Die folgende Beispielrichtlinie lässt beispielsweise jede Organisationsoperation nur zu, wenn alle drei der angegebenen Tag-Schlüssel in der Anforderung vorhanden sind.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

Alternativ können Sie `ForAnyValue:` verwenden, um einen Vergleichsoperator voranzustellen, um sicherzustellen, dass mindestens einer der Schlüssel in der Anforderung mit einem der in der Richtlinie angegebenen Schlüssel übereinstimmen muss. Die folgende Richtlinie lässt beispielsweise eine Organizations-Operation nur zu, wenn mindestens einer der angegebenen Tag-Schlüssel in der Anforderung vorhanden ist.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
```

```
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Mehrere Operationen ermöglichen es Ihnen, Tags in der Anforderung anzugeben. Wenn Sie beispielsweise eine Ressource erstellen, können Sie die Tags angeben, die der neuen Ressource zugeordnet sind. Sie können ein Tag-Schlüssel-Wert-Paar in der Richtlinie mit einem Schlüssel-Wert-Paar vergleichen, das in der Anforderung enthalten ist. Verweisen Sie dazu auf das Tag in einem `Condition`-Element, indem Sie dem Tag-Schlüsselnamen die folgende Zeichenfolge voranstellen: `aws:RequestTag/`*`key-name`* und dann den Tag-Wert angeben, der vorhanden sein muss.

Die folgende Beispielrichtlinie lehnt beispielsweise jede Anforderung des Benutzers oder der Rolle ab, ein AWS-Konto zu erstellen, wenn in der Anforderung entweder das `costcenter`-Tag fehlt oder dieses Tag mit einem anderen Wert als 1, 2, oder 3versehen wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
```

```
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Weitere Informationen zur Verwendung dieser Elemente finden Sie unter aws:TagKeys und aws:RequestTag im IAM-Benutzerhandbuch.

Protokollieren und Überwachen in AWS Organizations

Als bewährte Methode sollten Sie Ihre Organisation überwachen, um sicherzustellen, dass Änderungen protokolliert werden. Auf diese Weise können Sie sicherstellen, dass alle unerwarteten Änderungen untersucht werden und ungewollte Änderungen rückgängig gemacht werden können. AWS Organizations unterstützt zurzeit zwei AWS-Services, mit denen Sie Ihre Organisation und die Aktivitäten darin überwachen können.

Themen

- Protokollierung von AWS Organizations-API-Aufrufen mit AWS CloudTrail
- Amazon EventBridge

Protokollierung von AWS Organizations-API-Aufrufen mit AWS CloudTrail

AWS Organizations ist in AWS CloudTrail integriert, einen Service, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in AWS Organizations protokolliert. CloudTrail erfasst alle API-Aufrufe für AWS Organizations als Ereignisse, einschließlich Aufrufen von der AWS Organizations-Konsole und von Code-Aufrufen an die AWS Organizations-APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail-Ereignissen an einen Amazon S3-Bucket, einschließlich Ereignisse für AWS Organizations aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die an AWS Organizations gestellte Anfrage, die IP-Adresse, von der sie gestellt wurde, von wem und wann sie gestellt wurde und weitere Details ermitteln.

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

> **Important**
>
> Sie können alle CloudTrail-Informationen für AWS Organizations nur in der Region USA Ost (Nord-Virginia) anzeigen. Wenn Ihre AWS Organizations-Aktivitäten nicht in der CloudTrail-Konsole zu sehen sind, stellen Sie Ihre Konsole über das Menü in der rechten oberen Ecke auf USA Ost (Nord-Virginia) ein. Wenn Sie CloudTrail mit der AWS CLI oder SDK-Tools abfragen, richten Sie Ihre Abfrage an den Endpunkt USA Ost (Nord-Virginia).

AWS Organizations-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Konto für Sie aktiviert. Die in AWS Organizations auftretenden Aktivitäten werden als CloudTrail-Ereignis zusammen mit anderen AWS-Serviceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Organizations, erstellen Sie einen Trail. Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Wenn die CloudTrail-Protokollierung in Ihrem AWS-Konto-Konto aktiviert ist, werden API-Aufrufe von AWS Organizations-Aktionen zusammen mit anderen AWS-Servicedatensätzen in CloudTrail-Protokolldateien aufgezeichnet. Sie können andere AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail

Alle AWS Organizations-Aktionen werden von CloudTrail protokolliert und sind in der AWS Organizations-API-Referenz dokumentiert. Zum Beispiel werden durch Aufrufe von `CreateAccount` (einschließlich des `CreateAccountResult`-Ereignisses), `ListHandshakesForAccount`, `CreatePolicy` und `InviteAccountToOrganization` Einträge in den CloudTrail-Protokolldateien generiert.

Jeder Protokolleintrag enthält Informationen über den Ersteller der Anforderung. Der Benutzeridentität im Protokolleintrag können Sie folgende Informationen entnehmen:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des IAM-Benutzers gestellt wurde
- Ob die Anfrage mit temporären Sicherheitsanmeldeinformationen für eine IAM-Rolle oder einen Verbundbenutzer ausgeführt wurde
- Ob die Anforderung von einem anderen AWS-Service getätigt wurde.

Weitere Informationen finden Sie unter dem CloudTrail-userIdentity-Element.

Grundlagen zu AWS Organizations-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail-Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail-Protokolleinträge sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Beispielprotokolleinträge: CloseAccount

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen Beispiel-`CloseAccount`-Aufruf, der generiert wird, wenn die API aufgerufen wird und der Workflow zum Schließen des Kontos im Hintergrund mit der Verarbeitung beginnt.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
```

```
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen `CloseAccountResult`-Aufruf, nachdem der Hintergrund-Workflow zum Schließen des Kontos erfolgreich abgeschlossen wurde.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
```

```
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Beispielprotokolleinträge: CreateAccount

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen Beispiel-`CreateAccount`-Aufruf, der generiert wird, wenn die API aufgerufen wird und der Workflow zum Erstellen des Kontos im Hintergrund mit der Verarbeitung beginnt.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag für einen `CreateAccount`-Aufruf, nachdem der Hintergrundworkflow zum Erstellen des Kontos erfolgreich abgeschlossen wurde.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
```

```
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

Das folgende Beispiel zeigt einen CloudTrail-Protokolleintrag, der generiert wird, nachdem ein `CreateAccount`-Hintergrundworkflow das Konto nicht erstellen konnte.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
```

```
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Beispielprotokolleintrag: CreateOrganizationalUnit

Das folgende Beispiel zeigt den CloudTrail-Protokolleintrag des Beispielaufrufs `CreateOrganizationalUnit`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
```

```
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Beispielprotokolleintrag: InviteAccountToOrganization

Das folgende Beispiel zeigt den CloudTrail-Protokolleintrag des Beispielaufrufs `InviteAccountToOrganization`.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
```

```
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
```

```
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Beispielprotokolleintrag: AttachPolicy

Das folgende Beispiel zeigt den CloudTrail-Protokolleintrag des Beispielaufrufs `AttachPolicy`. Die Antwort gibt an, dass der Aufruf fehlgeschlagen ist, da der Typ der angeforderten Richtlinie nicht in dem Stammverzeichnis aktiviert ist, in dem der Anfügungsversuch ausgeführt wurde.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
```

```
}
```

Amazon EventBridge

AWS Organizations kann mit Amazon EventBridge, früher Amazon CloudWatch Events, zusammenarbeiten, um Ereignisse auszulösen, wenn vom Administrator festgelegte Aktionen in einer Organisation stattfinden. Zum Beispiel möchten die meisten Administratoren, aufgrund der Vertraulichkeit solcher Aktionen, gewarnt werden, sobald jemand ein neues Konto in der Organisation erstellt oder wenn der Administrator eines Mitgliedskontos versucht, die Organisation zu verlassen. Sie können EventBridge-Regeln konfigurieren, die auf diese Aktionen achten und die generierten Ereignisse dann an die vom Administrator festgelegten Ziele senden. Ziele können ein Amazon-SNS-Thema sein, das E-Mails oder SMS-Nachrichten an Abonnenten verwendet. Sie können auch eine AWS Lambda-Funktion erstellen, die Details der Aktion für die spätere Überprüfung protokolliert.

Ein Tutorial, das zeigt, wie Sie EventBridge aktivieren, um wichtige Aktivitäten in Ihrer Organisation zu überwachen, finden Sie unter Tutorial: Überwachen wichtiger Änderungen an Ihrer Organisation mit Amazon EventBridge.

Weitere Informationen zu Amazon EventBridge, einschließlich Konfiguration und Aktivierung, finden Sie im Benutzerhandbuch für Amazon EventBridge.

Compliance-Validierung für AWS Organizations

Informationen darüber, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services in Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

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

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.

- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

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

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden – Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit in AWS Organizations

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt.

Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Sicherheit der Infrastruktur in AWS Organizations

Als verwalteter Service ist AWS Organizations durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

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

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

AWS Organizations-Referenz

In den Themen in diesem Abschnitt finden Sie ausführliche Referenzinformationen für verschiedene Aspekte von AWS Organizations.

Themen

- Kontingente für AWS Organizations
- Von AWS verwaltete Richtlinien zur Nutzung mit AWS Organizations

Kontingente für AWS Organizations

In diesem Abschnitt werden Kontingente angegeben, die AWS Organizations beeinflussen.

Vorgaben für die Benennung

Im Folgenden finden Sie Richtlinien für Namen, in denen Sie Namen erstellen AWS Organizations, einschließlich Namen von Konten, Organisationseinheiten (OUs), Stammverzeichnissen und Richtlinien:

- Sie müssen aus Unicode-Zeichen bestehen
- Die maximale Zeichenfolgenlänge für Namen variiert je nach Objekt. Um das tatsächliche Limit für jeden anzuzeigen, lesen Sie die AWS Organizations -API-Referenz und suchen Sie den API-Vorgang, der das Objekt erstellt. Sehen Sie sich die Details für die `Name`-Parameter an. Beispiel: Account name (Kontoname) oder Name der Organisationseinheit.

Höchst- und Mindestwerte

Im Folgenden sind die standardmäßigen Höchstwerte für Entitäten in AWS Organizations aufgeführt.

> **Note**
>
> Sie können Erhöhungen für einige dieser Werte anfordern, indem Sie die Service-Quotas-Konsole verwenden.
> Organizations sind ein globaler Service, der physisch in der Region USA Ost (Nord-Virginia) gehostet wird (`us-east-1`) enthalten. Daher müssen Sie für `us-east-1` den Zugriff auf

Unternehmensquotas verwenden, wenn Sie die Service Quotas Console AWS CLI, das oder ein AWS SDK verwenden.

Anzahl AWS-Konten in einer Organisation	10 – Die standardmäßige maximale Anzahl zulässiger Konten in einer Organisation. Wenn Sie mehr benötigen, können Sie mit der Service-Quotas-Konsole eine Erhöhung anfordern. Eine an ein Konto gesendete Einladung wird auf dieses Kontingen t angerechnet. Die Anrechnung entfällt, wenn das eingeladene Konto ablehnt, das Verwaltungskonto die Einladung ablehnt oder die Einladung abgelaufen ist. Bei neu erstellten Konten und Organisationen kann es vorkommen, dass die Quota unter dem Standardwert von 10 Konten liegt.
Anzahl der Roots je Organisation	1
Anzahl der OUs je Organisation	1000
Anzahl der Richtlinien jedes Typs je Organisat ion	1000 pro Richtlinientyp
Maximale Größe eines Richtliniendokuments	Service-Kontrollrichtlinien: 5120 Zeichen Richtlinien zum Abmelden von KI-Services: 2500 Zeichen Backup-Richtlinien: 10000 Zeichen Tag-Richtlinien: 10000 Zeichen Hinweis: Wenn Sie die Richtlinie speichern AWS Management Console, werden zusätzliche Leerzeichen (wie Leerzeichen und Zeilenumbrüche) zwischen JSON-Elementen und außerhalb von Anführungszeichen entfernt und nicht gezählt. Wenn Sie die Richtlini e mithilfe eines SDK-Vorgangs oder des speichern AWS CLI, wird die

	Richtlinie genau so gespeichert, wie Sie sie angegeben haben, und es erfolgt keine automatische Entfernung von Zeichen.
Maximale Verschachtelungstiefe der Organisationseinheiten in einem Root	Fünf Organisationseinheitsstufen unter einem Root.
Maximale Anzahl der Einladungsversuche, die Sie in einem Zeitraum von 24 Stunden durchführen können	Entweder 20 oder die in Ihrer Organisation zulässige maximale Anzahl an Konten, je nachdem, was größer ist. Akzeptierte Einladungen werden nicht auf dieses Kontingent angerechnet. Sobald eine Einladung akzeptiert wird, können Sie am selben Tag eine weitere Einladung senden. Wenn die maximale Anzahl von Konten in Ihrer Organisation weniger als 20 beträgt, erhalten Sie eine Ausnahme „Kontolimit überschritten“, wenn Sie versuchen, mehr Konten einzuladen, als Ihre Organisation enthalten kann. Sie können Einladungen jedoch bis zu 20 Versuche an einem Tag stornieren und neue senden.
Die Anzahl der Mitgliedskonten, die Sie gleichzeitig erstellen können	5 – Sobald eines abgeschlossen ist, können Sie mit einem anderen beginnen. Allerdings können nur fünf zugleich verarbeitet werden.

Die Anzahl der Mitglieds konten, die Sie in einem Zeitraum von 30 Tagen schließen können	10% der Mitgliedskonten in einer Organisation, mit einem Maximum von 1000. • < 100 Konten – Sie können bis zu 10 Mitgliedskonten schließen • 100 — 10.000 Konten — Sie können bis zu 10% Ihrer Mitglieds konten schließen • > 10.000 Konten — Sie können bis zu 1000 Mitgliedskonten schließen Wenn Sie beispielsweise 10.500 Mitgliedskonten haben, können Sie innerhalb von 30 Tagen bis zu 1000 (nicht 1050) Konten schließen. Nachdem Sie dieses Kontingent erreicht haben, können Sie weitere Konten in der AWS Billing -Konsole schließen oder warten, bis Ihr Kontingent zurückgesetzt wird. Weitere Informationen finden Sie im Leitfaden zur Kontoverwaltung unter Was Sie wissen müssen, bevor Sie Ihr AWS Konto schließen.
Die Anzahl der Mitglieds konten, die Sie gleichzei tig schließen können	3 – Es können nur drei Kontoschließungen gleichzeitig ausgeführ t werden. Sobald eine Kontoschließung fertig ist, können Sie ein anderes Konto schließen.
Anzahl der Entitäten, denen eine Richtlinie zugeordnet werden kann	Unbegrenzt
Anzahl der Tags, die Sie einem Stamm, einer OU oder einem Konto zuordnen können	50
Maximale Größe der ressourcenbasierten Delegierungsrichtlinie	40 000 Zeichen

Ablaufzeiten für Handshakes

Im Folgenden sind die Timeouts für den Empfang von Handshakes aufgeführt. AWS Organizations

Einladung zum Beitritt zu einer Organisation	15 Tage
Anforderung zur Aktivierung aller Features in einer Organisation	90 Tage
Handshake wurde gelöscht und erscheint nicht mehr in Listen	30 Tage, nachdem der Handshake abgeschlossen wurde

Anzahl der Richtlinien je Entität

Der Mindest- und Höchstwert hängen vom Richtlinientyp und der Entität ab, an die Sie die Richtlinie anhängen. In der folgenden Tabelle werden die einzelnen Richtlinientypen und die Anzahl der Entitäten aufgeführt, die Sie jedem Typ zuordnen können.

> **Note**
>
> Diese Nummern gelten nur für Richtlinien, die direkt einer Organisationseinheit oder einem Konto zugeordnet sind. Richtlinien, die sich durch Vererbung auf eine OU oder ein Konto auswirken, werden auf diese Beschränkungen nicht angerechnet.

Richtlinientyp	Das einer Entität angefügte Minimum	Das einem Stamm angefügte Maximum	Das einer Organisationseinheit angefügte Maximum	Das einem Konto angefügte Maximum
Service-Kontrollrichtlinie	1 – Jeder Entität muss zu jeder Zeit mindestens eine Service-Kontrollri	5	5	5

Richtlinientyp	Das einer Entität angefügte Minimum	Das einem Stamm angefügte Maximum	Das einer Organisationseinheit angefügte Maximum	Das einem Konto angefügte Maximum
	chtlinie angefügt sein. Es ist nicht möglich, die letzte Service-Kontrollrichtlinie von einer Entität zu entfernen.			
Richtlinie zur Abmeldung von KI-Services	0	5	5	5
Backup-Richtlinie	0	10	10	10
Tag-Richtlinie	0	10	10	10

> **Note**
>
> Derzeit ist nur ein Root-Element je Organisation möglich.

Drosselungsgrenzen

In der folgenden Tabelle sind die AWS Organizations APIs nach Verwaltungskategorien geordnet und die jeweiligen Drosselungsraten auf Konto- und Organisationsebene aufgeführt.

AWS Organizations API	Limit pro Konto (Rate, Burst)	Limit pro Organisation (Rate, Burst)
Kontoverwaltung		

AWS Organizations API	Limit pro Konto (Rate, Burst)	Limit pro Organisation (Rate, Burst)
CloseAccount	.05, 1	
CreateAccount, CreateGovCloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
Verwaltung von Handschlägen		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
Verwaltung der Organisation		
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	

AWS Organizations API	Limit pro Konto (Rate, Burst)	Limit pro Organisation (Rate, Burst)
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	
Verwaltung der Richtlinien		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	

AWS Organizations API	Limit pro Konto (Rate, Burst)	Limit pro Organisation (Rate, Burst)
Serviceverwaltung		
AktivierenAWSServiceAccess, Deaktivieren AWSServic eAccess	1, 2	
ListeAWSServiceAcc essForOrganization, ListDeleg atedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministra tor, DeregisterDelegate dAdministrator	1, 2	

Von AWS verwaltete Richtlinien zur Nutzung mit AWS Organizations

In diesem Abschnitt werden die AWS-verwalteten Richtlinien aufgeführt, die Ihnen zur Verwaltung Ihrer Organisation zur Verfügung gestellt werden. Sie können eine von AWS verwaltete Richtlinie nicht ändern oder löschen. Sie können sie jedoch an Entitäten in Ihrer Organisation anfügen oder sie trennen.

AWS Organizations-verwaltete Richtlinien zur Nutzung mit AWS Identity and Access Management (IAM)

Eine verwaltete IAM-Richtlinie wird von AWS bereitgestellt und verwaltet. Eine verwaltete Richtlinie bietet Berechtigungen für allgemeine Aufgaben, die Sie Ihren Benutzern zuweisen können, indem Sie die verwaltete Richtlinie an den entsprechenden IAM-Benutzer oder das entsprechende Rollenobjekt anhängen. Sie müssen die Richtlinie nicht selbst schreiben, und wenn AWS die Richtlinie entsprechend aktualisiert, um neue Services zu unterstützen, profitieren Sie automatisch und sofort von der Aktualisierung. Sie können die Liste der AWS-verwalteten Richtlinien auf der Seite

Richtlinien in der IAM-Konsole anzeigen. Verwenden Sie das Dropdown-Menü Filterrichtlinien, um AWS-verwaltet auszuwählen.

Sie können die folgenden verwalteten Richtlinien verwenden, um Benutzern in Ihrer Organisation Berechtigungen zu erteilen.

Richtlinienname	Beschreibung	ARN
AWSOrganizationsFullAccess	Stellt alle Berechtigungen bereit, die zum Erstellen und vollständigen Verwalten einer Organisation erforderlich sind. Der Inhalt dieser Richtlinienerklärung wird im folgenden Ausschnitt dargestellt:	arn:aws:iam::aws:policy/AWSOrganizationsFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSOrganizationsFullAccess",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*"
        },
        {
            "Sid": "AWSOrganizationsFullAccessAccount",
            "Effect": "Allow",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:GetAlternateContact",
                "account:GetContactInformation",
                "account:PutContactInformation",
```

Richtlinienname	Beschreibung	ARN

```
                "account:
ListRegions",
                "account:
EnableRegion",
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

Richtlinienname	Beschreibung	ARN

AWSOrganizationsReadOnlyAccess	Bietet schreibgeschützten Zugriff auf Informationen über die Organisation. Es erlaubt dem Benutzer nicht, Änderungen vorzunehmen. Der Inhalt dieser Richtlinienerklärung wird im folgenden Ausschnitt dargestellt:
	
	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Sid": "AWSOrganizationsReadOnly",
	"Effect":"Allow",
	"Action":[
	"organizations:Describe*",
	"organizations:List*"
	],
	"Resource": "*"
	},
	{
	"Sid": "AWSOrganizationsReadOnlyAccount",
	"Effect":"Allow",
	"Action":[
	"account:GetAlternateContact",
	"account:GetContactInformation",
	"account:ListRegions"
	],
	"Resource": "*"
	}
	]
	}
		arn:aws:iam::aws:policy/AWSOrganizationsReadOnlyAccess

Aktualisierungen für Organizations AWS-verwaltete Richtlinien

In der folgenden Tabelle werden die Aktualisierungen AWS-verwalteter Richtlinien aufgeführt, seit dieser Service diese Änderungen nachverfolgt. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS Organizations-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWSOrganizationsFullAccess – aktualisiert, um `Sid` Elemente aufzunehmen, die die Richtlinienanweisung beschreiben.	Organizations hat `Sid` Elemente für die `AWSOrganizationsFullAccess` verwaltete Richtlinie hinzugefügt.	6. Februar 2024
AWSOrganizationsReadOnlyAccess – aktualisiert, um `Sid` Elemente aufzunehmen, die die Richtlinienanweisung beschreiben.	Organizations hat `Sid` Elemente für die `AWSOrganizationsReadOnlyAccess` verwaltete Richtlinie hinzugefügt.	6. Februar 2024
AWSOrganizationsFullAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Aktivieren oder Deaktivieren AWS-Regionen von über die Organizations-Konsole erforderlich sind.	Organizations mit der hinzugefügten Aktion `account:ListRegions`, `account:EnableRegion` und `account:DisableRegion`, um den Schreibzugriff zu aktivieren, um Regionen für ein Konto zu aktivieren oder zu deaktivieren.	22. Dezember 2022
AWSOrganizationsReadOnlyAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Auflisten AWS-Regionen über die Organizations-Konsole erforderlich sind.	Organizations mit der hinzugefügten Aktion `account:ListRegions`, um den Zugriff zum Anzeigen der Regionen für ein Konto zu ermöglichen.	22. Dezember 2022
AWSOrganizationsFullAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Hinzufügen oder Bearbeiten von	Organisationen haben der Richtlinie die `account:GetContactInformation` - und `account:PutContactInformation` -	21. Oktober 2022

Änderung	Beschreibung	Datum
Kontokontakten über die Organizations-Konsole erforderlich sind.	Aktionen hinzugefügt, um den Schreibzugriff zum Ändern alternativer Kontakte für ein Konto zu ermöglichen.	
AWSOrganizationsReadOnlyAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Anzeigen von Kontokontakten über die Organizations-Konsole erforderlich sind.	Organisationen haben der Richtlinie die `account:GetContactInformation` -Aktion hinzugefügt, um den Zugriff zum Anzeigen Kontakte für ein Konto zu ermöglichen.	21. Oktober 2022
AWSOrganizationsFullAccess – aktualisiert, um das Erstellen einer Organisation zu ermöglichen.	Organisationen haben der Richtlinie die Berechtigung `CreateServiceLinkedRole` hinzugefügt, um das Erstellen der serviceverknüpften Rolle zu ermöglichen, die zum Erstellen einer Organisation erforderlich ist. Die Berechtigung ist auf das Erstellen einer Rolle beschränkt, die nur vom `organizations.amazonaws.com` -Service verwendet werden kann.	24. August 2022
AWSOrganizationsFullAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Hinzufügen, Bearbeiten oder Löschen alternativer Kontokontakte über die Organizations-Konsole erforderlich sind.	Organisationen haben der Richtlinie die `account:GetAlternateContact` -, `account:DeleteAlternateContact` -, `account:PutAlternateContact` -Aktionen hinzugefügt, um den Schreibzugriff zum Ändern alternativer Kontakte für ein Konto zu ermöglichen.	7. Februar 2022

Änderung	Beschreibung	Datum
AWSOrganizationsReadOnlyAccess – aktualisiert, um Konto-API-Berechtigungen zuzulassen, die zum Anzeigen alternativer Kontokontakte über die Organizations-Konsole erforderlich sind.	Organisationen haben der Richtlinie die `account:GetAlternateContact` -Aktion hinzugefügt, um den Zugriff zum Anzeigen alternativer Kontakte für ein Konto zu ermöglichen.	7. Februar 2022

Verwaltete AWS Organizations-Service-Kontrollrichtlinien

Service-Kontrollrichtlinien (Service Control Policies, SCPs) entsprechen IAM-Berechtigungsrichtlinien. Sie sind jedoch Teil von AWS Organizations und nicht von IAM. Sie verwenden die SCPs, um maximale Berechtigungen für betroffene Entitäten anzugeben. Sie können SCPs an Roots, OUs (Organizational Units, Organisationseinheiten) oder Konten innerhalb Ihrer Organisation anhängen. Sie können entweder Ihre eigenen SCPs erstellen oder die von IAM definierten Richtlinien verwenden. Die Liste der Richtlinien in Ihrer Organisation finden Sie auf der Seite Richtlinien in der Organizations-Konsole.

> **Important**
>
> Jeder Root, jede OU und jedes Konto muss über mindestens eine angehängte SCP verfügen.

Richtlinienname	Beschreibung	ARN
VollAWSAccess	Bietet AWS Organizations-Verwaltungskontozugriff auf die Mitgliedskonten.	arn:aws:organizations::aws:policy/service_control_policy/p-FullAWSAccess

Fehlerbehebung bei AWS Organizations

Wenn Sie Probleme bei der Arbeit mit AWS Organizations haben, finden Sie in diesem Abschnitt entsprechende Themen.

Themen

- Fehlerbehebung bei allgemeinen Problemen
- Fehlerbehebung bei AWS Organizations-Richtlinien

Fehlerbehebung bei allgemeinen Problemen

Verwenden Sie die hier aufgeführten Informationen, um Probleme durch Verweigerung des Zugriffs oder andere allgemeine Probleme, die beim Arbeiten mit AWS Organizations auftreten können, zu diagnostizieren und zu beheben.

Themen

- Ich erhalte eine "Zugriff verweigert"-Meldung, wenn ich eine Anfrage an AWS Organizations stelle.
- Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle
- Ich erhalte eine „Zugriff verweigert“-Meldung, wenn ich versuche, eine Organisation als Mitgliedskonto zu verlassen oder ein Mitgliedskonto als Verwaltungskonto zu entfernen
- Ich erhalte eine Meldung „Kontingent überschritten“, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen.
- Ich erhalte die Meldung "Diese Operation benötigt eine Wartezeit", wenn ich Konten hinzufüge oder entferne.
- Ich erhalte eine Meldung, dass die Organisation immer noch initialisiert wird, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen.
- Ich erhalte die Meldung „Einladungen sind deaktiviert“, wenn ich versuche, ein Konto zu meiner Organisation einzuladen.
- Änderungen, die ich vornehme, sind nicht immer direkt sichtbar

Ich erhalte eine "Zugriff verweigert"-Meldung, wenn ich eine Anfrage an AWS Organizations stelle.

- Stellen Sie sicher, dass Sie die entsprechenden Berechtigungen zum Aufrufen der Aktion und Ressource besitzen, die Sie angefordert haben. Ein Administrator muss Berechtigungen erteilen, indem er eine IAM-Richtlinie mit Ihrem Benutzer, Ihrer Gruppe oder Ihrer Rolle verknüpft. Wenn die Richtlinienanweisungen, die diese Berechtigungen gewähren, Bedingungen enthalten, z. B. Einschränkungen der Tageszeit oder der IP-Adressen, müssen Sie diese Anforderungen erfüllen, wenn Sie die Anfrage senden. Weitere Informationen zum Anzeigen oder Ändern von Richtlinien für einen Benutzer, eine Gruppe oder eine Rolle finden Sie unter Arbeiten mit Richtlinien im IAM-Benutzerhandbuch.
- Wenn Sie API-Anfragen manuell signieren (ohne Verwendung von AWS-SDKs), stellen Sie sicher, dass Sie die Anfrage korrekt signiert haben.

Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle

- Stellen Sie sicher, dass der -Benutzer oder die Rolle, die Sie zum Erstellen der Anfrage verwenden, über die entsprechenden Berechtigungen verfügt. Berechtigungen für temporäre Sicherheitsanmeldeinformationen werden von einem -Benutzer oder einer Rolle abgeleitet, sodass die Berechtigungen auf die Berechtigungen des entsprechenden -Benutzers oder der Rolle beschränkt sind. Weitere Informationen über die Berechtigungen für temporäre Sicherheitsanmeldeinformationen finden Sie unter Kontrolle von Berechtigungen für temporäre Sicherheitsanmeldeinformationen im IAM-Benutzerhandbuch.
- Stellen Sie sicher, dass Ihre Anfragen korrekt signiert sind und die Anfrage richtig aufgebaut ist. Weitere Informationen finden Sie in der Toolkit-Dokumentation für das ausgewählte SDK oder unter Verwenden temporärer Sicherheitsanmeldeinformationen zum Anfordern des Zugriffs auf AWS-Ressourcen im IAM-Benutzerhandbuch.
- Stellen Sie sicher, dass die temporären Sicherheitsanmeldeinformationen nicht abgelaufen sind. Weitere Informationen finden Sie unter Anfordern von temporären Sicherheitsanmeldeinformationen im IAM-Benutzerhandbuch.

Ich erhalte eine „Zugriff verweigert“-Meldung, wenn ich versuche, eine Organisation als Mitgliedskonto zu verlassen oder ein Mitgliedskonto als Verwaltungskonto zu entfernen

- Sie können ein Mitgliedskonto nur entfernen, nachdem Sie IAM-Benutzerzugriff auf die Fakturierung im Konto aktiviert haben. Weitere Informationen finden Sie unter Gewähren von Zugriff auf die Konsole von Fakturierung und Kostenmanagement im AWS Billing-Benutzerhandbuch.
- Sie können ein Konto nur aus Ihrer Organisation entfernen, wenn es über die Informationen verfügt, die erforderlich sind, um als ein eigenständiges Konto zu funktionieren. Wenn Sie ein Konto in einer Organisation mithilfe der AWS Organizations-Konsole, der API oder von AWS CLI-Befehlen erstellen, werden diese Informationen nicht automatisch gesammelt. Sie müssen für jedes Konto, das Sie als eigenständig einrichten möchten, die AWS-Kundenvereinbarung akzeptieren, einen Support-Plan wählen, die erforderlichen Kontaktinformationen angeben und verifizieren sowie eine aktuelle Zahlungsmethode angeben. AWS verwendet die Zahlungsmethode, um alle gebührenpflichtigen AWS-Aktivitäten (d. h. alle Aktivitäten, die nicht auf des kostenlosen AWS-Kontingents ausgeführt werden) abzurechnen, die ausgeführt werden, wenn das Konto nicht mit einer Organisation verbunden ist. Weitere Informationen finden Sie unter Verlassen einer Organisation in Ihrem Mitgliedskonto.

Ich erhalte eine Meldung „Kontingent überschritten“, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen.

Es gibt ein maximale Anzahl von Konten, die Sie in einer Organisation haben können. Gelöschte oder geschlossene Konten werden weiterhin auf dieses Kontingent angerechnet.

Eine Einladung zur Teilnahme wird auf die maximale Anzahl von Konten in Ihrer Organisation angerechnet. Die Anrechnung entfällt, wenn das eingeladene Konto ablehnt, das Verwaltungskonto die Einladung ablehnt oder die Einladung abgelaufen ist.

- Bevor Sie ein AWS-Konto schließen oder löschen, entfernen Sie es aus Ihrer Organisation, sodass es nicht weiterhin auf Ihr Kontingent angerechnet wird.
- Weitere Informationen zum Anfordern einer Kontingenterhöhung finden Sie unter Höchst- und Mindestwerte.

Ich erhalte die Meldung "Diese Operation benötigt eine Wartezeit", wenn ich Konten hinzufüge oder entferne.

Einige Operationen benötigen eine Wartezeit. Beispielsweise können Sie neu erstellte Konten nicht sofort entfernen. Versuchen Sie die Aktion in einigen Tagen erneut. Wenn beim Hinzufügen und Entfernen von Konten Probleme mit Kontokontingenten auftreten, finden Sie weitere Informationen unter Höchst- und Mindestwerte, um eine Erhöhung des Kontingents zu beantragen.

Ich erhalte eine Meldung, dass die Organisation immer noch initialisiert wird, wenn ich versuche, meiner Organisation ein Konto hinzuzufügen.

Wenn Sie diese Fehlermeldung erhalten und seit der Erstellung der Organisation mehr als eine Stunde vergangen ist, wenden Sie sich an den AWS Support.

Ich erhalte die Meldung „Einladungen sind deaktiviert“, wenn ich versuche, ein Konto zu meiner Organisation einzuladen.

Dies geschieht, wenn Sie alle Funktionen in Ihrer Organisation aktivieren. Dieser Vorgang kann einige Zeit in Anspruch nehmen und erfordert, dass alle Mitgliedskonten reagieren. Bis der Vorgang abgeschlossen ist, können Sie keine neuen Konten zur Teilnahme an der Organisation einladen.

Änderungen, die ich vornehme, sind nicht immer direkt sichtbar

Als Service, auf den Computer in weltweit angesiedelten Rechenzentren zugreifen, nutzt AWS Organizations ein verteiltes Computing-Modell namens Eventual consistency. Jede Änderung, die Sie in AWS Organizations vornehmen, braucht Zeit, bis sie von allen möglichen Endpunkten aus sichtbar ist. Die Verzögerung ergibt sich teilweise aus der Zeit, die erforderlich ist, um die Daten von Server zu Server, von Replikationszone zu Replikationszone und von einer Region der Welt in eine andere zu senden. AWS Organizations verwendet darüber hinaus Zwischenspeicherungen zur Verbesserung der Leistung, doch in einigen Fällen kann dies Zeit erfordern. Die Änderung ist möglicherweise erst sichtbar, wenn die Zeit für die vorher zwischengespeicherten Daten abgelaufen ist.

Entwerfen Sie Ihre globalen Anwendungen unter Berücksichtigung dieser potenziellen Verzögerungen, und stellen Sie sicher, dass sie wie erwartet funktionieren, und zwar auch wenn eine Änderung an einem Standort nicht sofort in einem anderen sichtbar ist.

Weitere Informationen darüber, wie einige andere AWS-Services davon betroffen sind, finden Sie in den folgenden Ressourcen:

- Verwalten der Datenkonsistenz im Datenbankentwicklerhandbuch zu Amazon Redshift
- Amazon-S3-Datenkonsistenzmodell im Benutzerhandbuch für Amazon Simple Storage Service
- Sicherstellen der Konsistenz bei Verwendung von Amazon S3 und Amazon Elastic MapReduce für ETL-Workflows im AWS Big Data-Blog
- letztendliche EC2-Konsistenz in der Amazon-EC2-API-Referenz

Fehlerbehebung bei AWS Organizations-Richtlinien

Verwenden Sie die Informationen in diesem Artikel, um häufige Probleme im Zusammenhang mit AWS Organizations-Richtlinien zu diagnostizieren und zu beheben.

Service-Kontrollrichtlinien

Service-Kontrollrichtlinien (Service Control Policies, SCPs) in AWS Organizations entsprechen IAM-Richtlinien. Sie arbeiten mit einer gemeinsamen Syntax. Diese Syntax beginnt mit den Regeln der JavaScript Object Notation (JSON). JSON beschreibt ein Objekt über Name/Wert-Paare für das Objekt. Die IAM-Richtliniensyntax baut auf dieser Vorgehensweise auf. Sie definiert, welche Namen und Werte welche Bedeutung haben und wie diese von den AWS-Services zur Gewährung von Berechtigungen genutzt werden.

AWS Organizations nutzt eine Teilmenge der IAM-Syntax. Details hierzu finden Sie unter SCP-Syntax.

Häufige Fehler bei Richtlinien

- Mehr als ein Richtlinienobjekt
- Mehr als ein Statement-Element
- Richtliniendokument überschreitet die maximal zulässige Größe

Mehr als ein Richtlinienobjekt

Eine SCP darf nur ein JSON-Objekt haben. Ein Objekt wird mithilfe von {}-Klammern definiert. Obwohl Sie andere Objekte innerhalb eines JSON-Objekts verschachteln können, indem Sie zusätzliche { }-Klammern in das äußere Paar einbetten, kann eine Richtlinie nur ein äußerstes Paar von { }-Klammern enthalten. Das folgende Beispiel ist falsch. Es enthält zwei Objekte auf oberster Ebene (in *Rot*):

```
{
```

```
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

Mit der richtigen Schreibweise können Sie das Beispiel jedoch in eine korrekte Richtlinie umwandeln. Statt zwei vollständige Richtlinienobjekte mit jeweils eigenen `Statement`-Elementen zu nutzen, können Sie die beiden Blöcke in einem einzelnen `Statement`-Element kombinieren. Im folgenden Beispiel hat das `Statement`-Element zwei Objekte als Wert:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Dieses Beispiel kann nicht noch weiter in ein `Statement` mit einem Element zusammengefasst werden (die beiden Elemente haben unterschiedliche Effekte). Grundsätzlich können Sie Anweisungen nur dann kombinieren, wenn die Elemente `Effect` und `Resource` der Anweisungen identisch sind.

Mehr als ein Statement-Element

Dieser Fehler sieht möglicherweise zunächst wie eine Variante des Fehlers im vorherigen Abschnitt aus. Syntaktisch handelt es sich jedoch um einen anderen Fehler. Im folgenden Beispiel gibt es auf der obersten Ebene nur ein Richtlinienobjekt (durch die {}-Klammern definiert). Das Objekt enthält jedoch zwei `Statement`-Elemente.

Eine SCP darf nur ein `Statement`-Element enthalten. Dies setzt sich aus dem Namen (`Statement`) links vom Doppelpunkt und dem Wert auf der rechten Seite des Doppelpunktes zusammen. Der Wert eines `Statement`-Elements muss ein Objekt sein (durch {}-Klammern definiert). Es muss ein `Effect`-Element, ein `Action`-Element und ein `Resource`-Element enthalten. Das folgende Beispiel ist falsch. Es enthält zwei `Statement`-Elemente in der Richtlinie:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Da ein Wert-Objekt eine Gruppe mit mehreren Wert-Objekten sein kann, können Sie dieses Problem lösen, indem Sie die zwei `Statement`-Elemente in einem Element mit einer Objekt-Gruppe kombinieren:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Der Wert des `Statement`-Elements ist eine Objekt-Gruppe. Die Gruppe im Beispiel besteht aus zwei Objekten. Jedes Objekt ist ein gültiger Wert für ein `Statement`-Element. Die Objekte in der Gruppe werden durch Kommas getrennt.

Richtliniendokument überschreitet die maximal zulässige Größe

Die maximal zulässige Größe eines SCP-Dokuments ist 5.120 Bytes. Diese maximale Größe umfasst alle Zeichen einschließlich Leerzeichen. Zur Reduzierung der Größe Ihrer Service-Kontrollrichtlinie können Sie alle Leerraumzeichen (wie z. B. Leerzeichen und Zeilenumbrüche), die sich außerhalb von Anführungszeichen befinden, entfernen.

Aufrufen der API mittels HTTP-Abfrageanforderungen

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

> **Note**
>
> Anstatt die AWS Organizations-Query-API direkt aufzurufen, können Sie auch eine der AWS-SDKs verwenden. Die AWS-SDKs bestehen aus Bibliotheken und Beispiel-Code für verschiedene Programmiersprachen und Plattformen (darunter Java, Ruby, .NET, iOS und Android). Die SDKs sind gut zur Einrichtung des programmgesteuerten Zugriffs auf AWS Organizations und AWS geeignet. Mithilfe der SDKs lassen sich unter anderem Anforderungen kryptografisch signieren, Fehler verwalten und Anforderungen automatisch wiederholen. Weitere Informationen über die AWS-SDKs, das Herunterladen und die Installation finden Sie unter Tools für Amazon Web Services.

Die Abfrage-API für AWS Organizations dient zum Aufrufen von Serviceaktionen. Abfrage-API-Anforderungen sind HTTPS-Anforderungen, in denen eine auszuführende Operation mittels eines `Action`-Parameters angegeben wird. AWS Organizations unterstützt GET- und POST-Anforderungen für alle Operationen. Dies bedeutet, es ist für API nicht erforderlich, je nach Aktion zwischen GET- und POST-Anforderungen zu unterscheiden. Allerdings unterliegen GET-Anforderungen der Größenbeschränkung von URLs. Diese sind abhängig vom Browser; die übliche Beschränkung liegt bei 2.048 Byte. Für größere Abfrage-API-Anforderungen muss daher eine POST-Anforderung verwendet werden.

Die Antwort erfolgt in Form eines XML-Dokuments. Weitere Informationen über die Antwort finden Sie auf den Seiten zu den einzelnen Aktionen in der AWS Organizations-API-Referenz.

Themen

- Endpunkte
- HTTPS erforderlich
- Signieren von AWS Organizations-API-Anforderungen

Endpunkte

AWS Organizations verfügt über einen einzelnen globalen API-Endpunkt, der in der Region USA Ost (Nord-Virginia) gehostet wird.

Weitere Informationen zu AWS Endpunkten und Regionen für alle Services finden Sie unter Regionale Endpunkte im Allgemeine AWS-Referenz.

HTTPS erforderlich

Die Abfrage-API gibt vertrauliche Informationen wie Sicherheitsanmeldeinformationen zurück; daher müssen Sie zum Verschlüsseln aller API-Anforderungen HTTPS verwenden.

Signieren von AWS Organizations-API-Anforderungen

Anforderungen müssen über eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel signiert werden. Wir raten nachdrücklich davon ab, Ihre Root-Benutzer des AWS-Kontos-Anmeldeinformationen für die tägliche Arbeit mit AWS Organizations zu verwenden. Sie können die Anmeldeinformationen für einen Benutzer oder eine Rolle nutzen.

Zum Signieren von API-Anforderungen müssen Sie Signature Version 4 für AWS verwenden. Weitere Informationen zur Verwendung von Signature Version 4 finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

AWS Organizations unterstützt keine älteren Versionen, wie z. B. Signature Version 2.

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 für die Verwendung des IAM-Service zum Backup von AWS-Ressourcen, einschließlich der in AWS Organizations.
- Temporäre Sicherheitsanmeldeinformationen in IAM – Beschreibt die Erstellung und Verwendung von temporären Sicherheitsanmeldeinformationen.

Dokumentverlauf für AWS Organizations

Die folgende Tabelle beschreibt die wesentlichen Dokumentationsupdates für AWS Organizations.

- API-Version: 2016-11-28

Änderung	Beschreibung	Datum
Aktualisierte Richtlinienanweisungen	Neue `Sid` Elemente zu den AWS Organizations verwalteten Richtlinienanweisungen hinzugefügt.	6. Februar 2024
Neues Thema zum Schließen eines Verwaltungskontos	Links zu Überlegungen und detaillierten Schritten wurden hinzugefügt, in denen beschrieben wird, wie Sie ein Verwaltungskonto schließen.	1. Februar 2024
Bewährte Methoden wurden aktualisiert	Im Abschnitt mit bewährten Methoden wurden zur Angleichung an die bewährten Methoden für IAM neue Informationen hinzugefügt.	12. Juni 2023
Die von AWSOrganizationsFullAccess und AWSOrganizationsReadOnlyAccess verwalteten Richtlinien wurden aktualisiert	Beide verwalteten Richtlinien wurden aktualisiert, um Schreib- oder Lesezugriff auf Kontakte für Konten zu ermöglichen.	21. Oktober 2022
Die AWSOrganizationsFullAccess von verwaltete Richtlinie wurde aktualisiert	Die verwaltete Richtlinie wurde aktualisiert, um das Erstellen einer Organisation zu ermöglichen, indem die erforderliche Berechtigung zum Erstellen der serviceve	24. August 2022

	rknüpften Rolle hinzugefü gt wird, die für eine neue Organisation erforderlich ist.	
Organisationen schließen die Kontofähigkeit von der AWS Organizations-Konsole	Prinzipale im Verwaltun gskonto können Mitglieds konten über die AWS Organizations-Konsole schließen und Mitgliedskonten mithilfe von IAM-Richtlinien vor versehentlichem Schließen schützen.	29. März 2022
Aktualisierte Ankündigung zum Aktualisieren alternati ver Kontakte mit der AWS Organizations-Konsole	Organisationen bieten jetzt die Möglichkeit, alternative Kontakte für Konten innerhalb Ihrer Organisation mithilfe der AWS Organizations-Konsole zu aktualisieren. Kündigen Sie neue Funktione n an und verweisen Sie auf die Kontoverwaltungsreferenz für Anweisungen.	8. Februar 2022
Von Organisationen verwaltet e Richtlinienaktualisierungen – Aktualisieren auf eine vorhandene Richtlinie	Die von AWSOrganizationsFu llAccess und AWSOrgani zationsReadOnlyAccess verwalteten Richtlinien wurden aktualisiert, um Konto-API-Berechtigungen zu gewähren, die zum Aktualisi eren oder Anzeigen alternati ver Kontokontakte über die AWS Organizations Konsole erforderlich sind.	7. Februar 2022

Integration von Organizations mit Amazon DevOpsGuru	Sie können Amazon DevOpsGuru mit integrier enAWS Organizations, um den Anwendungszustand ganzheitlich über alle Ihre Organisationskonten hinweg zu überwachen und Erkenntni sse zu gewinnen.	3. Januar 2022
Integration von Organizations mit Amazon Detective	Sie können Amazon Detective mit AWS Organizations integrieren, um sicherzus tellen, dass Ihr Detective-Verhaltensdiagramm einen Einblick in die Aktivität für alle Konten der Organisation bietet.	16. Dezember 2021
Die Integration von Organizat ions mit AWS Config unterstüt zt jetzt die Datenaggregation für mehrere Konten und Regionen.	Sie können ein delegiertes Administratorkonto verwenden , um Ressourcenkonfigur ations- und Compliance-Daten aus allen Mitgliedskonten Ihrer Organisation zu aggregieren. Weitere Informationen finden Sie unter Datenaggregation für mehrere Konten und Regionen im AWS Config-Entwicklerh andbuch.	16. Juni 2021

Die Integration von Organizations mit AWS Firewall Manager unterstützt jetzt die Unterstützung für einen delegierten Administrator	Sie können nun ein Mitgliedskonto in Ihrer Organisation als Firewall-Manager-Administrator für die gesamte Organisation festlegen. Dies ermöglicht eine bessere Trennung der Berechtigungen vom Verwaltungskonto der Organisation.	30. April 2021
Die Backup-Richtlinien in Organizations unterstützen jetzt kontinuierliche Backups	Sie können das AWS Backup-Feature für kontinuierliche Backups mit den Backup-Richtlinien Ihrer Organisation verwenden.	10. März 2021
Die Integration von Organizations mit AWS CloudFormation StackSets unterstützt jetzt die Unterstützung für einen delegierten Administrator	Sie können jetzt ein Mitgliedskonto in Ihrer Organisation als AWS CloudFormation StackSets Administrator für die gesamte Organisation festlegen. Dies ermöglicht eine bessere Trennung der Berechtigungen vom Verwaltungskonto der Organisation.	18. Februar 2021
Einladen von Konten fortsetzen, während Sie alle Funktionen aktivieren	AWS hat den Prozess aktualisiert, um alle Funktionen in einer Organisation zu aktivieren. Sie können nun weiterhin neue Konten einladen, um Ihrer Organisation beizutreten, während Sie warten, bis vorhandene Konten auf ihre Einladungen antworten.	3. Februar 2021

Einführung der Version 2.0 der AWS Organizations-Konsole	AWS führte eine neue Version der AWS-Konsole ein. Die gesamte Dokumentation wurde aktualisiert, um die neue Art und Weise der Ausführung von Aufgaben widerzuspiegeln.	21. Januar 2021
Organizations unterstützt ab sofort die Integration mit AWS Marketplace	Sie können AWS Marketplace jetzt aktivieren, um Ihre Softwarelizenzen einfacher für alle Konten in Ihrer Organisation freizugeben.	3. Dezember 2020
Organizations unterstützt ab sofort die Integration mit Amazon S3 Lens	Amazon S3 Lens unterstützt sowohl vertrauenswürdigen Zugriff als auch delegierte Administratoren mit Organizations. Details dazu finden Sie unter Amazon-S3-Storage-Lens im Entwicklerhandbuch für Amazon Simple Storage Service.	18. November 2020
Kontoübergreifende Backup-Kopien	Wenn Sie Backup-Richtlinien verwenden, um die Ressourcen in Ihrer Organisation zu sichern, können Sie jetzt Kopien Ihres Backups in anderen AWS-Konten in der Organisation speichern.	18. November 2020

AWS-Regionen unterstützt jetzt AWS Resource Access Manager in China als vertrauenswürdigen Dienst für Organizations	Sie können jetzt AWS RAM-Funktionen verwenden, die in Organizations als vertrauenswürdiger Dienst integriert werden, wenn Sie Organizations und AWS RAM in China verwendet.	18. November 2020
Organizations unterstützt ab sofort die Integration mit AWS Security Hub	Sie können den Security Hub für alle Konten in Ihrer Organisation aktivieren und eines der Mitgliedskonten Ihrer Organisation als delegiertes Administratorkonto für Security Hub festlegen.	12. November 2020
Hauptkonto umbenannt	AWS Organizations änderte den Namen des „Hauptkontos“ in „Verwaltungskonto“. Dies ist nur eine Namensänderung, die Funktionalität bleibt unverändert.	20. Oktober 2020
Neuer Abschnitt für bewährte Methoden und neue Themen	Neuer Abschnitt für bewährte Methoden für AWS Organizations hinzugefügt. Der neue Abschnitt enthält Themen, in denen bewährte Methoden für das Verwaltungskonto und die Stammbenutzer des Mitgliederkontos sowie die Passwortverwaltung erläutert werden.	6. Oktober 2020

Neuer Abschnitt für bewährte Methoden und die ersten beiden Seiten hinzugefügt	Es gibt einen neuen Abschnitt für Themen, die bewährte Methoden für AWS Organizations beschreiben. Dieses Update enthält ein Thema für bewährte Methoden für das Verwaltungskonto einer Organisation und ein Thema für bewährte Methoden für Mitgliedskonten.	2. Oktober 2020
Backup-Richtlinien von Organizations unterstützen jetzt anwendungskonsistente Backups auf Windows-EC2-Instances mithilfe von VSS (Volume Shadow Copy Service)	Backup-Richtlinien unterstützen einen neuen `advanced_backup_settings` -Abschnitt. Der erste Eintrag in diesem neuen Abschnitt ist eine `ec2`-Einstellung namens `WindowsVSS` die Sie aktivieren oder deaktivieren können. Details dazu finden Sie unter Erstellen einer VSS-fähigen Windows-Backups im AWS Backup-Entwicklerhandbuch.	24. September 2020

Organizations unterstützt tag-on-create und Tag-basierte Zugriffskontrolle	Sie können Tags zu Organizations-Ressourcen hinzufügen, wenn Sie sie erstellen. Sie können Tag-Richtlinien verwenden, um die Tag-Nutzung auf Organizationsressourcen zu standardisieren. Sie können IAM-Richtlinien zum Beschränken des Zugriffs auf Ressourcen, die Tags und Werte angegeben haben verwenden.	15. September 2020
AWS Health als vertrauenswürdigen Service hinzugefügt	Sie können AWS Health-Ereignisse über Konten in Ihrer Organisation hinweg aggregieren.	4. August 2020
Opt-out-Richtlinien für künstliche Intelligenz-(KI)-Services	Sie können die Opt-out-Richtlinien für AWS-KI-Services verwenden, um zu steuern, ob KI-Services von diesen Services verarbeitete Kundeninhalte (KI-Inhalte) für die Entwicklung und kontinuierliche Verbesserung von AWS-KI-Services und -Technologien speichern und verwenden dürfen.	8. Juli 2020
Backup-Richtlinien und Integration mit AWS Backup hinzugefügt	Sie können Backup-Richtlinien verwenden, um Backup-Richtlinien für alle Konten in Ihrer Organisation zu erstellen und durchzusetzen.	24. Juni 2020

Unterstützung der delegierten Administration für IAM Access Analyzer	Dies ermöglicht das Delegieren des Administratorzugriffs für Access Analyzer in Ihrer Organisation an ein designtes Mitgliedskonto.	30. März 2020
Integration in AWS CloudFormation StackSets	Sie können ein serviceverwaltetes Stack-Set erstellen, um Stack-Instances für Konten bereitzustellen, die von AWS Organizations verwaltet werden.	11. Februar 2020
Integration mit Compute Optimizer	Compute Optimizer wurde als Service hinzugefügt, der für Konten Ihrer Organisation ausgeführt werden kann.	4. Februar 2020
Tag-Richtlinien	Mithilfe von Tag-Richtlinien können Sie Tags für alle Ressourcen in den Konten Ihrer Organisation standardisieren.	26. November 2019
Integration mit Systems Manager	In Systems Manager Explorer können Sie Betriebsdaten für alle AWS-Konten in Ihrer Organisation synchronisieren.	26. November 2019
aws:PrincipalOrgPaths	Der neue globale Bedingungsschlüssel überprüft den AWS Organizations-Pfad für den IAM-Benutzer, die IAM-Rolle oder den Stammbenutzer des AWS-Konto, der die Anforderung stellt.	20. November 2019

Integration in AWS Config-Regeln	Mithilfe von AWS Config-API-Operationen können Sie AWS Config-Regeln für alle AWS-Konten in Ihrer Organisation verwalten.	8. Juli 2019
Neuer Service für den vertrauenswürdigen Zugriff	Service Quotas wurde als Service hinzugefügt, der für Konten Ihrer Organisation ausgeführt werden kann.	24. Juni 2019
Integration mit AWS Control Tower	AWS Control Tower wurde als Service hinzugefügt, der für Konten Ihrer Organisation ausgeführt werden kann.	24. Juni 2019
Integration in AWS Identity and Access Management	IAM stellt die Daten zum letzten Servicezugriff für die Entitäten Ihrer Organisation bereit (Organisationsstamm, Organisationseinheiten und Konten). Sie können diese Daten verwenden, um den Zugriff auf die AWS-Services zu beschränken, die Sie benötigen.	20. Juni 2019
Tagging von Konten	Sie können Tags zu Konten in Ihrer Organisation hinzufügen bzw. von diesen entfernen und Tags auf einem Konto in Ihrer Organisation anzeigen.	6. Juni 2019

Ressourcen, Bedingungen und das Element `NotAction` in Service-Kontrollrichtlinien (SCPs)	Sie können nun Ressourcen, Bedingungen und das Element `NotAction` in Service-Kontrollrichtlinien (SCPs) angeben, um den kontoüber greifenden Zugriff in Ihrer Organisation oder Organisat ionseinheit (OU) zu verweiger n.	25. März 2019
Neue Services für den vertrauenswürdigen Zugriff	AWS License Manager und Service Catalog wurden als Services hinzugefügt, die mit den Konten in Ihrer Organisat ion verwendet werden können.	21. Dezember 2018
Neue Services für den vertrauenswürdigen Zugriff	AWS CloudTrail und AWS RAM wurden als Services hinzugefügt, die für Konten Ihrer Organisation ausgeführt werden können.	4. Dezember 2018
Neuer Service für den vertrauenswürdigen Zugriff	AWS Directory Service wurde als Service hinzugefügt, der für Konten Ihrer Organisation ausgeführt werden kann.	25. September 2018
Verifizierung der E-Mail-Ad resse	Sie müssen überprüfen, ob Sie sich im Besitz der E-Mail-Ad resse befinden, die mit dem Verwaltungskonto verknüpft ist, bevor Sie vorhandene Konten zu Ihrer Organisation einladen können.	20. September 2018

CreateAccount -Benachrichtigungen	`CreateAccount` -Benachrichtigungen werden in den CloudTrail Protokollen des Verwaltungskontos veröffentlicht.	28. Juni 2018
Neuer Service für den vertrauenswürdigen Zugriff	AWS Artifact wurde als Service hinzugefügt, der für Konten Ihrer Organisation ausgeführt werden kann.	20. Juni 2018
Neue Services für den vertrauenswürdigen Zugriff	AWS Config und AWS Firewall Manager wurden als Services hinzugefügt, die für Konten Ihrer Organisation ausgeführt werden können.	18. April 2018
Vertrauenswürdiger Servicezugriff	Ab sofort können Sie den Zugriff für ausgewählte AWS-Services zum Arbeiten mit Konten Ihrer Organisation aktivieren oder deaktivieren. IAM Identity Center ist der erste unterstützte vertrauenswürdige Service.	29. März 2018
Kontoentfernung ist jetzt Self-Service	Sie können jetzt Konten entfernen, die innerhalb von AWS Organizations erstellt wurden, ohne sich an AWS Support wenden zu müssen.	19. Dezember 2017
Unterstützung für den neuen Service AWS IAM Identity Center wurde hinzugefügt.	AWS Organizations unterstützt jetzt die Integration mit AWS IAM Identity Center (IAM Identity Center).	7. Dezember 2017

AWS hat eine serviceverknüpfte Rolle zu allen Organisationskonten hinzugefügt	Eine servicegebundene Rolle namens `AWSServiceRoleForOrganizations` wird allen Konten in einer Organisation hinzugefügt, um die Integration zwischen AWS Organizations und anderen AWS-Services zu ermöglichen.	11. Oktober 2017
Erstellte Konten können jetzt entfernt werden	Kunden können nun erstellte Konten mithilfe von AWS Support aus ihrer Organisation entfernen.	15. Juni 2017
Servicestart	Erste Version der AWS Organizations-Dokumentation zum Start des neuen Service.	17. Februar 2017

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.