



Benutzerhandbuch

AWS Aufstellen



AWS Aufstellen: Benutzerhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Übersicht	1
.....	1
.....	1
Terminologie	2
.....	2
Administrator	2
Account	2
Anmeldeinformationen	2
Unternehmensanmeldedaten	3
Profil	3
Benutzer	3
Anmeldeinformationen des Stammbenutzers	3
Verifizierungscode	4
AWS Benutzer und Anmeldeinformationen	5
Stammbenutzer	5
IAMIdentity Center-Benutzer	6
Verbundidentität	6
IAMBenutzer	6
AWS Builder-ID (Benutzer)	7
Voraussetzungen und Überlegungen	8
AWS-Konto-Voraussetzungen	8
Überlegungen zum IAM Identity Center	9
Active Directory oder externer IdP	10
AWS Organizations	11
IAM-Rollen	11
Firewalls der nächsten Generation und sichere Web-Gateways	11
Verwenden von mehreren AWS-Konten	12
Teil 1: Richten Sie ein neues einAWS-Konto	14
Schritt 1: Registrieren für ein AWS-Konto	14
Schritt 2: Melden Sie sich als Root-Benutzer an	16
So melden Sie sich als Root-Benutzer an	16
Schritt 3: Aktiviere MFA für dein AWS-Konto Root-Benutzer	17
Teil 2: Einen administrativen Benutzer in IAM Identity Center erstellen	18
Schritt 1: IAM Identity Center aktivieren	18

Schritt 2: Wählen Sie Ihre Identitätsquelle	19
Verbinden Sie Active Directory oder einen anderen IdP und geben Sie einen Benutzer an	20
Verwenden Sie das Standardverzeichnis und erstellen Sie einen Benutzer im IAM Identity Center	23
Schritt 3: Einen Administratorberechtigungssatz erstellen	24
Schritt 4: EinrichtenAWS-KontoZugriff für einen administrativen Benutzer	25
Schritt 5: Loggen Sie sich in dieAWSGreifen Sie mit Ihren Administratordaten auf das Portal zu	27
ProblembhebungAWS-KontoProbleme bei der Erstellung	29
Ich habe den Anruf nicht erhalten vonAWSum mein neues Konto zu verifizieren	29
Ich erhalte eine Fehlermeldung über die „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meineAWS-Kontoper Telefon	30
Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert	31
.....	xxxii

Übersicht

Dieses Handbuch enthält Anweisungen zum Erstellen eines neuen AWS-Kontos und richten Sie Ihren ersten administrativen Benutzer in ein AWS IAM Identity Center folgen Sie den neuesten bewährten Sicherheitsmethoden.

Ein AWS-Konto ist für den Zugriff erforderlich AWS-Services und dient als zwei grundlegende Funktionen:

- **Behälter**— Ein AWS-Konto ist ein Behälter für alle AWS-Ressourcen, die Sie erstellen können als AWS-Kunde. Wenn Sie einen Amazon Simple Storage Service (Amazon S3) -Bucket oder eine Amazon Relational Database Service (Amazon RDS) -Datenbank zum Speichern Ihrer Daten oder eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance zur Verarbeitung Ihrer Daten erstellen, erstellen Sie eine Ressource in Ihrem Konto. Jede Ressource wird eindeutig durch einen Amazon-Ressourcenname (ARN) identifiziert, der die Konto-ID des Kontos enthält, das die Ressource enthält oder besitzt.
- **Sicherheitsgrenze**— Ein AWS-Konto ist die grundlegende Sicherheitsgrenze für Ihre AWS-Ressourcen. Ressourcen, die Sie in Ihrem Konto erstellen, stehen nur Benutzern zur Verfügung, die über Anmeldeinformationen für dasselbe Konto verfügen.

Zu den wichtigsten Ressourcen, die Sie in Ihrem Konto erstellen können, gehören Identitäten, wie IAM-Benutzer und -Rollen und Verbundidentitäten, wie Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identity-Provider, dem IAM Identity Center-Verzeichnis oder jedem anderen Benutzer, der darauf zugreift AWS-Services indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. Diese Identitäten verfügen über Anmeldeinformationen, mit denen sich jemand anmelden kann, oder authentifizieren zu AWS. Identitäten verfügen außerdem über Berechtigungsrichtlinien, die festlegen, wozu die Person, die sich angemeldet hat, mit den Ressourcen im Konto berechtigt ist.

Terminologie

Amazon Web Services (AWS) verwendet eine [gängige Terminologie](#), um den Anmeldevorgang zu beschreiben. Wir empfehlen Ihnen, diese Bedingungen zu lesen und zu verstehen.

Administrator

Wird auch als bezeichnet AWS-Konto Administrator oder IAM Administrator. Der Administrator, in der Regel Mitarbeiter der Informationstechnologie (IT), ist eine Person, die ein AWS-Konto. Administratoren haben eine höhere Berechtigungsebene für AWS-Konto als andere Mitglieder ihrer Organisation. Administratoren erstellen und implementieren Einstellungen für AWS-Konto. Sie erstellen IAM auch IAM Identity Center-Benutzer. Der Administrator stellt diesen Benutzern ihre Zugangsdaten und eine Anmeldung URL zur Verfügung, mit der sie sich anmelden können AWS.

Account

Ein Standard AWS-Konto enthält sowohl deine AWS Ressourcen und die Identitäten, die auf diese Ressourcen zugreifen können. Konten sind mit der E-Mail-Adresse und dem Passwort des Kontoinhabers verknüpft.

Anmeldeinformationen

Wird auch als Zugangs- oder Sicherheitsanmeldedaten bezeichnet. Anmeldeinformationen sind die Informationen, die Benutzer zur Verfügung stellen AWS um sich anzumelden und Zugriff zu erhalten AWS Ressourcen schätzen. Zu den Anmeldeinformationen können eine E-Mail-Adresse, ein Benutzername, ein benutzerdefiniertes Passwort, eine Konto-ID oder ein Alias, ein Bestätigungscode und ein Einmalcode für die mehrstufige Authentifizierung (MFA) gehören. Sowohl bei der Authentifizierung als auch bei der Autorisierung nutzt das System Anmeldeinformationen, um den Aufrufer zu bestimmen und zu ermitteln, ob der angeforderte Zugriff gewährt wird. In AWS, bei diesen Anmeldeinformationen handelt es sich in der Regel um die [Zugriffsschlüssel-ID](#) und [den geheimen Zugriffsschlüssel](#).

Weitere Informationen zu Anmeldeinformationen finden Sie unter [Grundlegendes und Abrufen Ihrer AWS Anmeldeinformationen](#).

 Note

Die Art der Anmeldeinformationen, die ein Benutzer einreichen muss, hängt von seinem Benutzertyp ab.

Unternehmensanmeldedaten

Die Anmeldeinformationen, die Benutzer beim Zugriff auf ihr Unternehmensnetzwerk und ihre Ressourcen angeben. Ihr Unternehmensadministrator kann Ihre einrichten AWS-Konto um mit den gleichen Anmeldeinformationen zugänglich zu sein, die Sie für den Zugriff auf Ihr Unternehmensnetzwerk und Ihre Ressourcen verwenden. Diese Anmeldeinformationen werden Ihnen von Ihrem Administrator oder Helpdesk-Mitarbeiter zur Verfügung gestellt.

Profil

Wenn Sie sich für einen anmelden AWS Builder ID, Sie erstellen ein Profil. Ihr Profil umfasst die von Ihnen angegebenen Kontaktinformationen sowie die Möglichkeit, Geräte und aktive Sitzungen mit Multi-Faktor-Authentifizierung (MFA) zu verwalten. In Ihrem Profil können Sie auch mehr über den Datenschutz und den Umgang mit Ihren Daten erfahren. Für weitere Informationen über Ihr Profil und wie es sich auf eine bezieht AWS-Konto, siehe [AWS Builder-ID und andere AWS Anmeldeinformationen](#).

Benutzer

Ein Benutzer ist eine Person oder Anwendung unter einem Konto, die API Anrufe tätigt AWS Produkte. Jeder Benutzer hat einen eindeutigen Namen innerhalb der AWS-Konto und eine Reihe von Sicherheitsanmeldedaten, die nicht mit anderen geteilt werden. Diese Anmeldeinformationen sind getrennt von den Sicherheitsanmeldeinformationen für AWS-Konto Jeder Benutzer kann nur einem einzigen zugeordnet sein. AWS-Konto.

Anmeldeinformationen des Stammbenutzers

Bei den Root-Benutzeranmeldedaten handelt es sich um dieselben Anmeldeinformationen, mit denen Sie sich bei dem AWS Management Console als Root-Benutzer. Weitere Informationen zum Root-Benutzer finden Sie unter [Root-Benutzer](#).

Verifizierungscode

Ein Bestätigungscode verifiziert Ihre Identität während des Anmeldevorgangs [mithilfe der Multi-Faktor-Authentifizierung](#) (). MFA Die Versandmethoden für Bestätigungscode variieren. Sie können per Textnachricht oder E-Mail gesendet werden. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu erhalten.

AWS Benutzer und Anmeldeinformationen

Wenn Sie interagieren mit AWS, spezifizieren Sie Ihre AWS Sicherheitsanmeldedaten, um zu überprüfen, wer Sie sind und ob Sie berechtigt sind, auf die von Ihnen angeforderten Ressourcen zuzugreifen. AWS verwendet Sicherheitsanmeldedaten, um Anfragen zu authentifizieren und zu autorisieren.

Wenn Sie z. B. eine geschützte Datei aus einem Amazon Simple Storage Service (Amazon S3)-Bucket herunterladen möchten, müssen Ihre Anmeldeinformationen diesen Zugriff erlauben. Wenn Ihre Anmeldeinformationen zeigen, dass Sie nicht berechtigt sind, die Datei herunterzuladen, AWS lehnt Ihre Anfrage ab. Sicherheitsanmeldedaten sind jedoch nicht erforderlich, um Dateien in öffentlich geteilten Amazon S3 S3-Buckets herunterzuladen.

Stammbenutzer

Wird auch als Kontoinhaber oder Kontostammbenutzer bezeichnet. Als Root-Benutzer haben Sie vollständigen Zugriff auf alle AWS Dienste und Ressourcen in Ihrem AWS-Konto. Wenn Sie zum ersten Mal ein erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle hat AWS Dienste und Ressourcen im Konto. Diese Identität ist die AWS Root-Benutzer des Kontos. Sie können sich anmelden bei [AWS Management Console](#) als Root-Benutzer mit der E-Mail-Adresse und dem Passwort, mit denen Sie das Konto erstellt haben. Eine schrittweise Anleitung zur Anmeldung finden Sie unter [Anmelden bei AWS Management Console als Root-Benutzer](#).

Important

Wenn Sie ein erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle hat AWS-Services und Ressourcen im Konto. Diese Identität wird als AWS-Konto Root-Benutzer. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich](#) sind. IAM

Weitere Informationen zu IAM Identitäten, einschließlich des Root-Benutzers, finden Sie unter [IAM Identitäten \(Benutzer, Benutzergruppen und Rollen\)](#).

IAM Identity Center-Benutzer

Ein IAM Identity Center-Benutzer meldet sich über AWS Zugriffsportal. Das Tool AWS Das Zugriffsportal oder die spezifische Anmeldung URL wird von Ihrem Administrator oder Helpdesk-Mitarbeiter bereitgestellt. Wenn Sie einen IAM Identity Center-Benutzer für Ihr AWS-Konto, wurde eine Einladung, IAM Identity Center-Benutzer beizutreten, an die E-Mail-Adresse des AWS-Konto. Die spezifische Anmeldung URL ist in der E-Mail-Einladung enthalten. IAM Identity Center-Benutzer können sich nicht über das anmelden AWS Management Console. Eine schrittweise Anleitung zur Anmeldung finden Sie unter [Anmelden bei AWS auf das Portal zugreifen](#).

Note

Wir empfehlen Ihnen, die spezifische Anmeldung URL für das mit einem Lesezeichen zu versehen AWS Greifen Sie auf das Portal zu, damit Sie später schnell darauf zugreifen können.

Weitere Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#)

Verbundidentität

Eine föderierte Identität ist ein Benutzer, der sich mit einem bekannten externen Identitätsanbieter (IdP) wie Login with Amazon, Facebook, Google oder einem anderen [OpenID Connect \(OIDC\)](#)-kompatiblen IdP anmelden kann. Mit dem Web-Identitätsverbund können Sie ein Authentifizierungstoken erhalten und dieses Token dann gegen temporäre Sicherheitsanmeldedaten eintauschen AWS die einer IAM Rolle mit Berechtigungen zur Nutzung der Ressourcen in Ihrem zugeordnet sind AWS-Konto. Sie melden sich nicht an mit AWS Management Console or AWS Zugangsportal. Stattdessen bestimmt die verwendete externe Identität, wie Sie sich anmelden.

Weitere Informationen finden Sie unter [Als föderierte Identität anmelden](#).

IAM Benutzer

Ein IAM Benutzer ist eine Entität, in der Sie erstellen AWS. Dieser Benutzer ist eine Identität innerhalb Ihres AWS-Konto dem bestimmte benutzerdefinierte Berechtigungen gewährt werden. Ihre

IAM Benutzeranmeldeinformationen bestehen aus einem Namen und einem Passwort, mit denen Sie sich bei der [AWS Management Console](#). Eine schrittweise Anleitung zur Anmeldung finden Sie unter [Anmelden bei AWS Management Console als IAM Benutzer](#).

Weitere Informationen zu IAM Identitäten, einschließlich des IAM Benutzers, finden Sie unter [IAM Identitäten \(Benutzer, Benutzergruppen und Rollen\)](#).

AWS Builder-ID (Benutzer)

Als AWS Builder ID-Benutzer melden Sie sich speziell bei AWS Dienst oder Tool, auf das Sie zugreifen möchten. Importieren in &S3; AWS Der Builder ID-Benutzer ergänzt jedes AWS-Konto Sie haben es bereits oder möchten es erstellen. Importieren in &S3; AWS Die Builder-ID steht für Sie als Person, und Sie können sie für den Zugriff verwenden AWS Dienste und Tools ohne AWS-Konto. Sie haben auch ein Profil, in dem Sie Ihre Informationen sehen und aktualisieren können. Weitere Informationen finden Sie unter [So melden Sie sich an mit AWS Builder-ID](#).

Voraussetzungen und Überlegungen

Bevor Sie mit der Einrichtung beginnen, überprüfen Sie die Kontoanforderungen und überlegen Sie, ob Sie mehr als ein Konto benötigenAWS-Konto, und machen Sie sich mit den Anforderungen vertraut, die für die Einrichtung Ihres Kontos für den Administratorzugriff im IAM Identity Center erforderlich sind.

AWS-Konto-Voraussetzungen

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

- Ein Kontoname— Der Name des Kontos erscheint an mehreren Stellen, z. B. auf Ihrer Rechnung, und in Konsolen wie dem Abrechnungs- und Kostenmanagement-Dashboard und demAWS OrganizationsKonsole.

Wir empfehlen, dass Sie einen Kontonamensstandard verwenden, damit der Kontoname leicht erkannt und von anderen Konten, die Sie möglicherweise besitzen, unterschieden werden kann. Wenn es sich um ein Unternehmenskonto handelt, sollten Sie erwägen, einen Benennungsstandard wieOrganisation-Zweck-Umwelt(zum BeispielAnyCompany-Prüfung-stupsen). Wenn es sich um ein Privatkonto handelt, sollten Sie erwägen, einen Benennungsstandard zu verwenden, z. B.Vorname-Nachname-Zweck(zum Beispielpaulo-santos-testaccount).

- Eine E-Mail-Adresse— Diese E-Mail-Adresse wird als Anmeldename für den Root-Benutzer des Kontos verwendet und ist für die Kontowiederherstellung erforderlich, z. B. wenn das Passwort vergessen wurde. Sie müssen in der Lage sein, an diese E-Mail-Adresse gesendete Nachrichten zu empfangen. Bevor Sie bestimmte Aufgaben ausführen können, müssen Sie überprüfen, ob Sie Zugriff auf das E-Mail-Konto haben.

Important

Wenn dieses Konto für ein Unternehmen bestimmt ist, empfehlen wir Ihnen, eine Unternehmens-Verteilerliste zu verwenden (z. B.`it.admins@example.com`). Vermeiden Sie es, die Unternehmens-E-Mail-Adresse einer Einzelperson zu verwenden (z. B.`paulo.santos@example.com`). Dies trägt dazu bei, dass Ihr Unternehmen auf die zugreifen kannAWS-Kontowenn ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt. Die E-Mail-Adresse kann verwendet werden, um die Root-

Benutzeranmeldeinformationen des Kontos zurückzusetzen. Stellen Sie sicher, dass Sie den Zugriff auf diese Verteilerliste oder Adresse schützen.

- Eine Telefonnummer— Diese Nummer kann verwendet werden, wenn eine Bestätigung der Kontoinhaberschaft erforderlich ist. Sie müssen in der Lage sein, Anrufe unter dieser Telefonnummer entgegenzunehmen.

Important

Wenn dieses Konto für ein Unternehmen bestimmt ist, empfehlen wir, eine Unternehmenstelefonnummer anstelle einer privaten Telefonnummer zu verwenden. Dies trägt dazu bei, dass Ihr Unternehmen auf die zugreifen kannAWS-Kontowenn ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt.

- Ein Multi-Faktor-Authentifizierungsgerät— Um Ihre zu sichernAWSRessourcen, aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für das Root-Benutzerkonto. Zusätzlich zu Ihren regulären Anmeldeinformationen ist bei der Aktivierung von MFA eine sekundäre Authentifizierung erforderlich, die eine zusätzliche Sicherheitsebene bietet. Weitere Informationen zu MFA finden Sie unter[Was ist MFA?](#)in derIAM-Benutzerhandbuch.
- AWS SupportPlänen— Bei der Kontoerstellung werden Sie aufgefordert, einen der verfügbaren Tarife auszuwählen. Eine Beschreibung der verfügbaren Pläne finden Sie unter[VergleicheAWS SupportPläne](#).

Überlegungen zum IAM Identity Center

Die folgenden Themen enthalten Anleitungen zur Einrichtung des IAM Identity Center für bestimmte Umgebungen. Machen Sie sich mit den Richtlinien vertraut, die für Ihre Umgebung gelten, bevor Sie mit[Teil 2: Einen administrativen Benutzer in IAM Identity Center erstellen](#).

Themen

- [Active Directory oder externer IdP](#)
- [AWS Organizations](#)
- [IAM-Rollen](#)
- [Firewalls der nächsten Generation und sichere Web-Gateways](#)

Active Directory oder externer IdP

Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen IdP verwalten, empfehlen wir, dass Sie erwägen, diese Identitätsquelle zu verbinden, wenn Sie das IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Wenn Sie dies tun, bevor Sie Benutzer und Gruppen im Identity Center-Standardverzeichnis erstellen, können Sie die zusätzliche Konfiguration vermeiden, die erforderlich ist, wenn Sie Ihre Identitätsquelle später ändern.

Wenn Sie Active Directory als Identitätsquelle verwenden möchten, muss Ihre Konfiguration die folgenden Voraussetzungen erfüllen:

- Wenn du verwendest AWS Managed Microsoft AD, Sie müssen das IAM Identity Center in derselben aktivieren AWS-Region wo dein AWS Managed Microsoft AD Verzeichnis ist eingerichtet. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um das IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der das IAM Identity Center konfiguriert ist. Beachten Sie auch, dass die AWS Das Access Portal verwendet dieselbe Zugriffs-URL wie Ihr Verzeichnis.

- Verwenden Sie ein Active Directory, das sich in Ihrem Verwaltungskonto befindet:

Sie müssen über einen vorhandenen AD-Connector verfügen oder AWS Managed Microsoft AD Verzeichnis eingerichtet in AWS Directory Service, und es muss in deinem AWS Organizations Verwaltungskonto. Sie können nur einen AD-Connector oder einen verbinden AWS Managed Microsoft AD zu einer Zeit. Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie unter:

- [Verbinde ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#) in der AWS IAM Identity Center Benutzerleitfaden.
 - [Verbinden Sie ein selbstverwaltetes Verzeichnis in Active Directory mit dem IAM Identity Center](#) in der AWS IAM Identity Center Benutzerleitfaden.
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

Wenn Sie vorhaben, den delegierten Administrator von IAM Identity Center zu aktivieren und Active Directory als Ihre IAM-Identitätsquelle zu verwenden, können Sie einen vorhandenen AD Connector verwenden oder AWS Managed Microsoft AD Verzeichnis eingerichtet in AWS Verzeichnis, das sich im delegierten Administratorkonto befindet.

Wenn Sie beschließen, die IAM Identity Center-Quelle von einer anderen Quelle auf Active Directory oder von Active Directory auf eine andere Quelle zu ändern, muss sich das Verzeichnis

im Mitgliedskonto des delegierten IAM Identity Center-Administrators befinden (sofern vorhanden); andernfalls muss es sich im Verwaltungskonto befinden.

AWS Organizations

Dein AWS-Konto muss verwaltet werden von AWS Organizations. Wenn Sie keine Organisation gegründet haben, müssen Sie das nicht tun. Wenn Sie IAM Identity Center aktivieren, entscheiden Sie, ob Sie erstellen Sie eine Organisation für Sie.

Wenn Sie bereits eingerichtet haben AWS Organizations, stellen Sie sicher, dass alle Funktionen aktiviert sind. Weitere Informationen finden Sie unter [Aktivieren aller Funktionen in Ihrer Organisation](#) im AWS Organizations Benutzerhandbuch.

Um IAM Identity Center zu aktivieren, müssen Sie sich beim AWS Management Console in dem Sie die Anmeldeinformationen Ihres AWS Organizations Verwaltungskonto. Sie können das IAM Identity Center nicht aktivieren, während Sie mit Anmeldeinformationen von einem AWS Organizations Mitgliedskonto. Weitere Informationen finden Sie unter [Erstellung und Verwaltung einer AWS Organisation](#) in der AWS Organizations Benutzerleitfaden.

IAM-Rollen

Wenn Sie bereits IAM-Rollen in Ihrem konfiguriert haben AWS-Konto, empfehlen wir Ihnen, zu überprüfen, ob sich Ihr Konto dem Kontingent für IAM-Rollen nähert. Weitere Informationen finden Sie unter [IAM-Objektkontingente](#).

Wenn Sie sich der Quote nähern, sollten Sie erwägen, eine Quotenerhöhung zu beantragen. Andernfalls können Probleme mit IAM Identity Center auftreten, wenn Sie Berechtigungssätze für Konten bereitstellen, die das IAM-Rollenkontingent überschritten haben. Informationen darüber, wie Sie eine Quotenerhöhung beantragen können, finden Sie unter [Quotenerhöhung beantragen](#) in der Service Quotas — Benutzerhandbuch.

Firewalls der nächsten Generation und sichere Web-Gateways

Wenn Sie den Zugriff auf bestimmte AWS Domänen oder URL-Endpunkte Wenn Sie eine Lösung zur Filterung von Webinhalten wie NGFWs oder SWGs verwenden, müssen Sie die folgenden Domänen oder URL-Endpunkte zu den Zulassungslisten Ihrer Lösung zur Filterung von Webinhalten hinzufügen.

Spezifische DNS-Domänen

- *.awsapps.com (<http://awsapps.com/>)
- *.signin.aws

Spezifische URL-Endpunkte

- [https://\[dein Verzeichnis\].awsapps.com/start](https://[dein Verzeichnis].awsapps.com/start)
- [https://\[dein Verzeichnis\].awsapps.com/login](https://[dein Verzeichnis].awsapps.com/login)
- [https://\[deine Region\].signin.aws/platform/login](https://[deine Region].signin.aws/platform/login)

Verwenden von mehreren AWS-Konten

AWS-Konten dienen als grundlegende Sicherheitsgrenze in AWS. Sie dienen als Ressourcencontainer, der ein nützliches Maß an Isolation bietet. Die Fähigkeit, Ressourcen und Benutzer zu isolieren, ist eine wichtige Voraussetzung für die Einrichtung einer sicheren, gut verwalteten Umgebung.

Teilen Sie Ihre Ressourcen in separate Bereiche auf AWS-Konten hilft Ihnen dabei, die folgenden Prinzipien in Ihrer Cloud-Umgebung zu unterstützen:

- **Sicherheitskontrolle**— Verschiedene Anwendungen können unterschiedliche Sicherheitsprofile haben, die unterschiedliche Kontrollrichtlinien und -mechanismen erfordern. Zum Beispiel ist es einfacher, mit einem Auditor zu sprechen und auf einen einzelnen zeigen zu können AWS-Konto das alle Elemente Ihres Workloads hostet, die unterliegen [Sicherheitsstandards der Payment Card Industry \(PCI\)](#).
- **Isolierung**— Ein AWS-Konto ist eine Einheit des Sicherheitsschutzes. Potenzielle Risiken und Sicherheitsbedrohungen sollten in einem AWS-Konto ohne andere zu beeinträchtigen. Aufgrund unterschiedlicher Teams oder unterschiedlicher Sicherheitsprofile können unterschiedliche Sicherheitsanforderungen bestehen.
- **Viele Teams**— Verschiedene Teams haben unterschiedliche Verantwortlichkeiten und Ressourcenanforderungen. Sie können verhindern, dass sich Teams gegenseitig stören, indem Sie sie voneinander trennen AWS-Konten.
- **Datenisolierung**— Neben der Isolierung der Teams ist es wichtig, die Datenspeicher einem Konto zuzuordnen. Dies kann dazu beitragen, die Anzahl der Personen zu begrenzen, die auf diesen Datenspeicher zugreifen und ihn verwalten können. Dies trägt dazu bei, den Zugriff auf sehr private Daten einzudämmen und kann daher zur Einhaltung der [Allgemeine Datenschutzverordnung \(GDPR\) der Europäischen Union](#).

- **Geschäftsprozess**— Verschiedene Geschäftsbereiche oder Produkte können völlig unterschiedliche Zwecke und Prozesse haben. Mit mehreren AWS-Konten, können Sie die spezifischen Bedürfnisse einer Geschäftseinheit unterstützen.
- **Fakturierung**— Ein Konto ist die einzig wahre Möglichkeit, Artikel auf Abrechnungsebene zu trennen. Mehrere Konten helfen dabei, Artikel auf Abrechnungsebene nach Geschäftsbereichen, Funktionsteams oder einzelnen Benutzern zu trennen. Sie können immer noch alle Ihre Rechnungen an einen einzigen Zahler konsolidieren lassen (mit AWS Organizations und konsolidierte Fakturierung), wobei die Einzelposten getrennt sind durch AWS-Konto.
- **Quotenzuweisung**— AWS Servicekontingente werden für jeden einzelnen durchgesetzten AWS-Konto. Aufteilung der Workloads in verschiedene AWS-Konten verhindert, dass sie Kontingente füreinander verbrauchen.

Alle in diesem Leitfaden beschriebenen Empfehlungen und Verfahren entsprechen den [AWS Gut durchdachtes Framework](#). Dieses Framework soll Ihnen helfen, eine flexible, belastbare und skalierbare Cloud-Infrastruktur zu entwerfen. Auch wenn Sie klein anfangen, empfehlen wir Ihnen, sich an die Richtlinien des Frameworks zu halten. Auf diese Weise können Sie Ihre Umgebung sicher und ohne Beeinträchtigung Ihres laufenden Betriebs skalieren, wenn Sie wachsen.

Bevor Sie beginnen, mehrere Konten hinzuzufügen, sollten Sie einen Plan für deren Verwaltung entwickeln. Dafür empfehlen wir Ihnen, [AWS Organizations](#), das ist ein kostenloses AWS Service, um all das zu verwalten AWS-Konten in Ihrer Organisation.

AWS bietet auch AWS Control Tower, wodurch Schichten von hinzugefügt werden AWS verwaltete die Automatisierung für Organisationen und integriert sie automatisch in andere AWS Dienstleistungen wie AWS CloudTrail, AWS Config, Amazonas CloudWatch, AWS Service Catalog und andere. Für diese Dienste können zusätzliche Kosten anfallen. Weitere Informationen finden Sie unter [AWS Control Tower Preise](#).

Teil 1: Richten Sie ein neues einAWS-Konto

Diese Anleitung hilft Ihnen bei der Erstellung einesAWS-Kontound sichern Sie die Root-Benutzeranmeldeinformationen. Führen Sie alle Schritte aus, bevor Sie mit[Teil 2: Einen administrativen Benutzer in IAM Identity Center erstellen](#).

Themen

- [Schritt 1: Registrieren für ein AWS-Konto](#)
- [Schritt 2: Melden Sie sich als Root-Benutzer an](#)
- [Schritt 3: Aktiviere MFA für dein AWS-Konto Root-Benutzer](#)

Schritt 1: Registrieren für ein AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. WähleErstelle eineAWS-Konto.

Note

Wenn Sie sich angemeldet habenAWSvor kurzem, wähleMelden Sie sich bei der Konsole an. Wenn die OptionErstellen Sie ein neuesAWS-Kontoist nicht sichtbar, wähle zuerstMelden Sie sich mit einem anderen Konto an, und wählen Sie dannErstellen Sie ein neuesAWS-Konto.

3. Geben Sie Ihre Kontoinformationen ein und wählen Sie dannFortfahren.

Vergewissern Sie sich, dass Sie Ihre Kontoinformationen korrekt eingeben, insbesondere Ihre E-Mail-Adresse. Wenn Sie Ihre E-Mail-Adresse falsch eingeben, können Sie nicht auf Ihr Konto zugreifen.

4. WählePersönlichoderProfessionell.

Der Unterschied zwischen diesen Optionen besteht nur in den Informationen, um die wir Sie bitten. Beide Kontotypen haben dieselben Merkmale und Funktionen.

5. Geben Sie Ihre Unternehmens- oder persönlichen Daten ein, basierend auf den Anweisungen unter[AWS-Konto-Voraussetzungen](#).
6. Lesen und akzeptieren Sie die[AWSVereinbarung mit dem Kunden](#).

7. Wähle Konto erstellen und fortfahren.

Zu diesem Zeitpunkt erhalten Sie eine E-Mail-Nachricht, um zu bestätigen, dass Ihr AWS-Konto ist gebrauchsfertig. Sie können sich mit der E-Mail-Adresse und dem Passwort, die Sie bei der Registrierung angegeben haben, in Ihrem neuen Konto anmelden. Sie können jedoch keine AWS-Dienste verwenden, bis Sie die Aktivierung Ihres Kontos abgeschlossen haben.

8. Auf der Informationen zur Zahlung Seite, geben Sie die Informationen zu Ihrer Zahlungsmethode ein. Wenn Sie eine Adresse verwenden möchten, die sich von der Adresse unterscheidet, mit der Sie das Konto erstellt haben, wählen Sie Benutze eine neue Adresse und geben Sie die Adresse ein, die Sie für Abrechnungszwecke verwenden möchten.

9. Wähle Überprüfen und hinzufügen.

Note

Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Nutzungsvereinbarung für Ihr Konto mit AISPL, einem lokalen Unternehmen AWS-Verkäufer in Indien. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben. Je nach Bank müssen Sie möglicherweise auch ein Einmalpasswort eingeben. AISPL berechnet Ihrer Zahlungsmethode im Rahmen des Überprüfungsprozesses 2 INR. AISPL erstattet die 2 INR, nachdem die Überprüfung abgeschlossen ist.

10. Um Ihre Telefonnummer zu verifizieren, wählen Sie Ihre Landes- oder Regionalvorwahl aus der Liste aus und geben Sie eine Telefonnummer ein, unter der Sie in den nächsten Minuten angerufen werden können. Geben Sie den CAPTCHA-Code ein und senden Sie ihn ab.
11. Der AWS Das automatische Überprüfungssystem ruft Sie an und gibt Ihnen eine PIN. Geben Sie die PIN mit Ihrem Telefon ein und wählen Sie Fortfahren.
12. Wählen Sie eine AWS Supportplanen.

Eine Beschreibung der verfügbaren Pläne finden Sie unter [Vergleiche AWS SupportPläne](#).

Es wird eine Bestätigungsseite angezeigt, die darauf hinweist, dass Ihr Konto aktiviert wird. Dies dauert normalerweise nur wenige Minuten, kann aber manchmal bis zu 24 Stunden dauern. Während der Aktivierung können Sie sich bei Ihrem neuen AWS-Konto. Bis die Aktivierung abgeschlossen ist, wird möglicherweise ein Registrierung abschließen Knopf. Sie können sie ignorieren.

AWS sendet eine Bestätigungs-E-Mail, wenn die Kontoaktivierung abgeschlossen ist. Überprüfen Sie Ihre E-Mail und Ihren Spam-Ordner auf die Bestätigungs-E-Mail. Nachdem Sie diese Nachricht erhalten haben, haben Sie vollen Zugriff auf alle AWS Dienstleistungen.

Schritt 2: Melden Sie sich als Root-Benutzer an

Wenn Sie zum ersten Mal ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die den vollständigen Zugriff auf alle AWS-Services und Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben.

Important

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 im Benutzerhandbuch unter [Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind](#).
IAM

So melden Sie sich als Root-Benutzer an

1. Öffnen Sie die AWS Management Console bei <https://console.aws.amazon.com/>.

Note

Wenn Sie sich zuvor in diesem Browser als Root-Benutzer angemeldet haben, erinnert sich Ihr Browser möglicherweise an die E-Mail-Adresse für Ihr AWS-Konto.
Wenn Sie sich zuvor mit diesem Browser als IAM-Benutzer angemeldet haben, zeigt Ihr Browser möglicherweise stattdessen die IAM-Benutzeranmeldeseite an. Um zur Hauptanmeldeseite zurückzukehren, wählen Sie Melden Sie sich mit der E-Mail-Adresse des Stammnutzers an.

2. Wenn Sie sich noch nicht mit diesem Browser angemeldet haben, wird die Hauptanmeldeseite angezeigt. Wenn Sie der Kontoinhaber sind, wählen Sie Root-Benutzer. Geben Sie Ihre AWS-Konto-Adresse mit Ihrem Konto verknüpfte E-Mail-Adresse ein und wählen Sie Weiter.

3. Möglicherweise werden Sie aufgefordert, eine Sicherheitsüberprüfung durchzuführen. Füllen Sie dies aus, um mit dem nächsten Schritt fortzufahren. Wenn Sie die Sicherheitsüberprüfung nicht abschließen können, versuchen Sie, sich den Ton anzuhören oder die Sicherheitsüberprüfung auf neue Zeichen zu überprüfen.
4. Geben Sie Ihr Passwort ein und wählen Sie Anmelden.

Schritt 3: Aktiviere MFA für dein AWS-Konto Root-Benutzer

Um die Sicherheit Ihrer Root-Benutzeranmeldedaten zu erhöhen, empfehlen wir Ihnen, die bewährte Sicherheitsmethode zu befolgen und die Multi-Faktor-Authentifizierung (MFA) für Ihre AWS-Konto. Da der Root-Benutzer vertrauliche Operationen in Ihrem Konto ausführen kann, hilft Ihnen das Hinzufügen dieser zusätzlichen Authentifizierungsebene dabei, Ihr Konto besser zu schützen. Es gibt mehrere Typen von MFA verfügbar.

Anweisungen zur Aktivierung MFA für den Root-Benutzer finden Sie unter [MFA Geräte für Benutzer aktivieren in AWS](#) im IAM-Benutzerhandbuch.

Teil 2: Einen administrativen Benutzer in IAM Identity Center erstellen

Nachdem Sie fertig sind [Teil 1: Richten Sie ein neues einAWS-Konto](#), die folgenden Schritte helfen Ihnen bei der EinrichtungAWS-KontoZugriff für einen administrativen Benutzer, der für die Ausführung der täglichen Aufgaben verwendet wird.

Note

Dieses Thema enthält die Mindestschritte, die erforderlich sind, um den Administratorzugriff für eineAWS-Kontound erstellen Sie einen administrativen Benutzer im IAM Identity Center. Weitere Informationen finden Sie unter [Erste Schritte](#) in derAWS IAM Identity CenterBenutzerleitfaden.

Themen

- [Schritt 1: IAM Identity Center aktivieren](#)
- [Schritt 2: Wählen Sie Ihre Identitätsquelle](#)
- [Schritt 3: Einen Administratorberechtigungssatz erstellen](#)
- [Schritt 4: EinrichtenAWS-KontoZugriff für einen administrativen Benutzer](#)
- [Schritt 5: Loggen Sie sich in dieAWSGreifen Sie mit Ihren Administratordaten auf das Portal zu](#)

Schritt 1: IAM Identity Center aktivieren

Note

Wenn Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer nicht aktiviert haben, führen Sie den Vorgang aus [Schritt 3: Aktiviere MFA für dein AWS-Konto Root-Benutzer](#) bevor Sie fortfahren.

So aktivieren Sie IAM Identity Center

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffne die [IAM Identity Center-Konsole](#).
3. Unter IAM Identity Center aktivieren, wähle Ermöglichen.
4. IAM Identity Center benötigt AWS Organizations. Wenn Sie noch keine Organisation gegründet haben, müssen Sie entscheiden, ob AWS erstellen Sie eine für dich. Wähle Erstellen AWS Organisation um diesen Vorgang abzuschließen.

AWS Organizationssendet automatisch eine Bestätigungs-E-Mail an die Adresse, die mit Ihrem Verwaltungskonto verknüpft ist. Es kann eine Verzögerung eintreten, bevor Sie die Verifizierungs-E-Mail erhalten. Überprüfen Sie Ihre E-Mail-Adresse innerhalb von 24 Stunden.

Note

Wenn Sie eine Umgebung mit mehreren Konten verwenden, empfehlen wir, die delegierte Administration zu konfigurieren. Mit der delegierten Verwaltung können Sie die Anzahl der Personen einschränken, die Zugriff auf das Verwaltungskonto benötigen, in AWS Organizations. Weitere Informationen finden Sie unter [Delegierte Verwaltung](#) in der AWS IAM Identity Center Benutzerleitfaden.

Schritt 2: Wählen Sie Ihre Identitätsquelle

Ihre Identitätsquelle im IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Sie können eine der folgenden Quellen als Identitätsquelle wählen:

- IAM Identity Center-Verzeichnis— Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem IAM Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Hier erstellen Sie Ihre Benutzer und Gruppen und weisen deren Zugriffsebene Ihren AWS-Konten und -Anwendungen zu.
- Active Directory— Wählen Sie diese Option, wenn Sie weiterhin Benutzer entweder in Ihrem von AWS verwalteten Microsoft AD-Verzeichnis mithilfe von AWS Directory Service oder in Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) verwalten möchten.

- **Externer Identitätsanbieter**— Wählen Sie diese Option, wenn Sie Benutzer in einem externen Identitätsanbieter (IdP) wie Okta oder Azure Active Directory verwalten möchten.

Nachdem Sie IAM Identity Center aktiviert haben, müssen Sie Ihre Identitätsquelle auswählen. Die von Ihnen gewählte Identitätsquelle bestimmt, wo IAM Identity Center nach Benutzern und Gruppen sucht, die Single Sign-On-Zugriff benötigen. Nachdem Sie Ihre Identitätsquelle ausgewählt haben, erstellen oder spezifizieren Sie einen Benutzer und weisen ihm Administratorberechtigungen zu AWS-Konto.

Important

Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen Identitätsanbieter (IdP) verwalten, empfehlen wir, dass Sie erwägen, diese Identitätsquelle zu verbinden, wenn Sie das IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Dies sollte geschehen, bevor Sie Benutzer und Gruppen im standardmäßigen Identity Center-Verzeichnis erstellen und Zuweisungen vornehmen. Wenn Sie bereits Benutzer und Gruppen in einer Identitätsquelle verwalten, werden durch den Wechsel zu einer anderen Identitätsquelle möglicherweise alle Benutzer- und Gruppenzuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben. In diesem Fall verlieren alle Benutzer, einschließlich des Administratorbenutzers im IAM Identity Center, den Single Sign-On-Zugriff auf ihre AWS-Konten und Anwendungen.

Themen


- [Verbinden Sie Active Directory oder einen anderen IdP und geben Sie einen Benutzer an](#)
- [Verwenden Sie das Standardverzeichnis und erstellen Sie einen Benutzer im IAM Identity Center](#)

Verbinden Sie Active Directory oder einen anderen IdP und geben Sie einen Benutzer an

Wenn Sie bereits Active Directory oder einen externen Identitätsanbieter (IdP) verwenden, helfen Ihnen die folgenden Themen dabei, Ihr Verzeichnis mit dem IAM Identity Center zu verbinden.

Sie können eine verbinden AWS Managed Microsoft AD Verzeichnis, ein selbstverwaltetes Verzeichnis in Active Directory oder ein externer IdP mit IAM Identity Center. Wenn Sie planen, eine Verbindung herzustellen AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in

Active Directory, stellen Sie sicher, dass Ihre Active Directory-Konfiguration die Voraussetzungen in [erfüllt Active Directory oder externer IdP](#).

 Note

Aus Sicherheitsgründen empfehlen wir dringend, die Multi-Faktor-Authentifizierung zu aktivieren. Wenn Sie planen, eine Verbindung herzustellen [AWS Managed Microsoft AD](#) Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory und Sie verwenden RADIUS MFA nicht mit [AWS Directory Service](#), aktivieren Sie MFA im IAM Identity Center. Wenn Sie planen, einen externen Identitätsanbieter zu verwenden, beachten Sie, dass der externe IdP und nicht das IAM Identity Center die MFA-Einstellungen verwaltet. MFA in IAM Identity Center wird für die Verwendung durch externe Benutzer nicht unterstützt. Weitere Informationen finden Sie unter [MFA aktivieren](#) in der [AWS IAM Identity Center](#) Benutzerleitfaden.

AWS Managed Microsoft AD


1. Lesen Sie die Anleitung unter [Stellen Sie eine Verbindung zu einem Microsoft Active Directory her](#).
2. Folgen Sie den Schritten in [Verbinde ein Verzeichnis in AWS Managed Microsoft AD zum IAM Identity Center](#).
3. Konfigurieren Sie Active Directory, um den Benutzer, dem Sie Administratorberechtigungen gewähren möchten, mit IAM Identity Center zu synchronisieren. Weitere Informationen finden Sie unter [Synchronisieren Sie einen administrativen Benutzer mit IAM Identity Center](#).

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unter [Stellen Sie eine Verbindung zu einem Microsoft Active Directory her](#).
2. Folgen Sie den Schritten in [Verbinden Sie ein selbstverwaltetes Verzeichnis in Active Directory mit dem IAM Identity Center](#).
3. Konfigurieren Sie Active Directory, um den Benutzer, dem Sie Administratorberechtigungen gewähren möchten, mit IAM Identity Center zu synchronisieren. Weitere Informationen finden Sie unter [Synchronisieren Sie einen administrativen Benutzer in IAM Identity Center](#).

Externer IdP

1. Lesen Sie die Anleitung unter [Stellen Sie eine Verbindung zu einem externen Identitätsanbieter her](#).
2. Folgen Sie den Schritten in [So stellen Sie eine Verbindung zu einem externen Identitätsanbieter her](#).
3. Konfigurieren Sie Ihren IdP, um Benutzern das IAM Identity Center zur Verfügung zu stellen.

 Note

Bevor Sie die automatische, gruppenbasierte Bereitstellung all Ihrer Workforce-Identitäten von Ihrem IdP in IAM Identity Center einrichten, empfehlen wir, den einen Benutzer, dem Sie Administratorberechtigungen gewähren möchten, mit IAM Identity Center zu synchronisieren.

Synchronisieren Sie einen administrativen Benutzer mit IAM Identity Center

Nachdem Sie Ihr Verzeichnis mit IAM Identity Center verbunden haben, können Sie einen Benutzer angeben, dem Sie Administratorberechtigungen gewähren möchten, und diesen Benutzer dann aus Ihrem Verzeichnis mit IAM Identity Center synchronisieren.

1. Öffne die [IAM Identity Center-Konsole](#).
2. Wählen Sie Settings (Einstellungen) aus.
3. Auf der [Einstellungen](#) Seite, wählen Sie die [Identitätsquelle](#) Tab, wähle [Aktionen](#), und wählen Sie dann [Synchronisierung](#) verwalten.
4. Auf der [Synchronisierung](#) verwalten Seite, wählen Sie die [Nutzertippen](#) Sie auf und wählen Sie dann [Benutzer](#) und [Gruppen](#) hinzufügen.
5. Auf der [Nutzer](#) Tab, unter [Nutzer](#), geben Sie den genauen Benutzernamen ein und wählen [Hinzufügen](#).
6. Unter [Benutzer](#) und [Gruppen](#) hinzugefügt, gehen Sie wie folgt vor:
 - a. Vergewissern Sie sich, dass der Benutzer angegeben ist, dem Sie Administratorberechtigungen gewähren möchten.
 - b. Markieren Sie das Kontrollkästchen links neben dem Benutzernamen.
 - c. Wählen Sie [Submit \(Absenden\)](#) aus.

7. In der Synchronisierung verwalten Seite, der von Ihnen angegebene Benutzer erscheint in der Benutzer im Synchronisierungsbereich Liste.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf der Nutzer Seite, es kann einige Zeit dauern, bis der von Ihnen angegebene Benutzer in der Liste erscheint. Wählen Sie das Aktualisierungssymbol, um die Benutzerliste zu aktualisieren.

Zu diesem Zeitpunkt hat Ihr Benutzer keinen Zugriff auf das Verwaltungskonto. Sie richten den Administratorzugriff auf dieses Konto ein, indem Sie einen Administratorberechtigungssatz erstellen und den Benutzer diesem Berechtigungssatz zuweisen.

Der nächste Schritt: [Schritt 3: Einen Administratorberechtigungssatz erstellen](#)

Verwenden Sie das Standardverzeichnis und erstellen Sie einen Benutzer im IAM Identity Center

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem IAM Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Gehen Sie wie folgt vor, um einen Benutzer in IAM Identity Center zu erstellen.

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffne die [IAM Identity Center-Konsole](#).
3. Folgen Sie den Schritten in [Nutzer hinzufügen](#) um einen Benutzer zu erstellen.

Wenn Sie die Benutzerdetails angeben, können Sie entweder eine E-Mail mit den Anweisungen zur Passwortkonfiguration senden (dies ist die Standardoption) oder ein Einmalkennwort generieren. Wenn Sie eine E-Mail senden, stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie zugreifen können.

4. Nachdem Sie den Benutzer hinzugefügt haben, kehren Sie zu diesem Verfahren zurück. Wenn Sie die Standardoption beibehalten haben, um eine E-Mail mit den Anweisungen zur Passwortkonfiguration zu senden, gehen Sie wie folgt vor:
 - a. Sie erhalten eine E-Mail mit dem Betreff **Einladung zum Beitritt AWS Einmaliges Anmelden**. Öffnen Sie die E-Mail und wählen Sie **Einladung annehmen**.
 - b. Auf der **Registrierung eines neuen Benutzers** Seite, geben Sie ein Passwort ein und bestätigen Sie es und wählen Sie dann **Neues Passwort setzen**.

Note

Achten Sie darauf, Ihr Passwort zu speichern. Du wirst es später brauchen [Schritt 5: Loggen Sie sich in die AWS Greifen Sie mit Ihren Administratordaten auf das Portal zu](#).

Zu diesem Zeitpunkt hat Ihr Benutzer keinen Zugriff auf das Verwaltungskonto. Sie richten den Administratorzugriff auf dieses Konto ein, indem Sie einen Administratorberechtigungsatz erstellen und den Benutzer diesem Berechtigungsatz zuweisen.

Der nächste Schritt: [Schritt 3: Einen Administratorberechtigungsatz erstellen](#)

Schritt 3: Einen Administratorberechtigungsatz erstellen

Berechtigungsätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, die Benutzer und Gruppen auf eine AWS-Konto. Gehen Sie wie folgt vor, um einen Berechtigungsatz zu erstellen, der Administratorberechtigungen gewährt.

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffne die [IAM Identity Center-Konsole](#).
3. Im Navigationsbereich von IAM Identity Center unter Berechtigungen für mehrere Konten, wähle Berechtigungsätze.
4. Wählen Sie Create permission set (Berechtigungsatz erstellen) aus.
5. Für Schritt 1: Wählen Sie den Typ des Berechtigungsatzes, auf der Wählen Sie den Typ des Berechtigungsatzes aus Seite, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter. Die Standardeinstellungen gewähren vollen Zugriff auf AWS Dienste und Ressourcen, die den AdministratorAccess vordefinierter Berechtigungsatz.

Note

Das Vordefinierte AdministratorAccess Der Berechtigungsatz verwendet die AdministratorAccess AWS verwaltete Richtlinie.

6. Für Schritt 2: Geben Sie die Details des Berechtigungssatzes an, auf der Details zum Berechtigungssatz angeben Seite, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter. Die Standardeinstellung begrenzt Ihre Sitzung auf eine Stunde.
7. Für Schritt 3: Überprüfen und erstellen, auf der Überprüfen und erstellen Seite, gehen Sie wie folgt vor:
 1. Überprüfen Sie den Typ des Berechtigungssatzes und vergewissern Sie sich, dass er AdministratorAccess.
 2. Überprüfen Sie die AWS verwaltete Richtlinie und bestätige, dass dies der Fall ist AdministratorAccess.
 3. Wählen Sie Create (Erstellen) aus.

Schritt 4: Einrichten AWS-Konto Zugriff für einen administrativen Benutzer

Zum Einrichten AWS-Konto Zugriff für einen Administratorbenutzer im IAM Identity Center, Sie müssen den Benutzer dem zuweisen AdministratorAccess Berechtigungssatz.

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffne die [IAM Identity Center-Konsole](#).
3. Im Navigationsbereich unter Berechtigungen für mehrere Konten, wähle AWS-Konten.
4. Auf der AWS-Konten Seite, eine Baumstruktur mit einer Liste Ihrer Organisation wird angezeigt. Markieren Sie das Kontrollkästchen neben dem AWS-Konto dem Sie Administratorzugriff zuweisen möchten. Wenn Sie in Ihrer Organisation mehrere Konten haben, aktivieren Sie das Kontrollkästchen neben dem Verwaltungskonto.
5. Wähle Benutzer oder Gruppen zuweisen.
6. Für Schritt 1: Benutzer und Gruppen auswählen, auf der Weisen Sie Benutzer und Gruppen zu **„AWS-Kontoname“** Seite, gehen Sie wie folgt vor:
 1. Auf der Nutzer klicken Sie auf der Registerkarte und wählen Sie den Benutzer aus, dem Sie Administratorberechtigungen gewähren möchten.


Um die Ergebnisse zu filtern, beginnen Sie, den Namen des gewünschten Benutzers in das Suchfeld einzugeben.

2. Nachdem Sie bestätigt haben, dass der richtige Benutzer ausgewählt wurde, wählen Sie **Weiter**.
7. Für Schritt 2: Wählen Sie die Berechtigungssätze, auf der Ordnen Sie“ Berechtigungssätze zu **AWS-Kontoname**„Seite, unter Berechtigungssätze, wählen Sie die **AdministratorAccess** Berechtigungssatz.
8. Wählen Sie **Weiter** aus.
9. Für Schritt 3: Überprüfen und Absenden, auf der Aufgaben überprüfen und einreichen an“ **AWS-Kontoname**„Seite, gehen Sie wie folgt vor:
 1. Überprüfen Sie den ausgewählten Benutzer und den ausgewählten Berechtigungssatz.
 2. Nachdem Sie bestätigt haben, dass der richtige Benutzer dem zugewiesen ist **AdministratorAccess** Berechtigungssatz, wählen **Einreichen**.

 **Important**

Der Vorgang der Benutzerzuweisung kann einige Minuten dauern. Lassen Sie diese Seite geöffnet, bis der Vorgang erfolgreich abgeschlossen ist.

10. Wenn einer der folgenden Punkte zutrifft, folgen Sie den Schritten unter [MFA aktivieren](#) um MFA für IAM Identity Center zu aktivieren:
 - Sie verwenden das standardmäßige Identity Center-Verzeichnis als Identitätsquelle.
 - Du verwendest eine **AWS Managed Microsoft AD** Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory als Ihre Identitätsquelle und Sie verwenden **RADIUS MFA** nicht mit **AWS Directory Service**.

 **Note**

Wenn Sie einen externen Identitätsanbieter verwenden, beachten Sie, dass der externe IdP und nicht das IAM Identity Center die MFA-Einstellungen verwaltet. MFA in IAM Identity Center wird für die Verwendung durch externe Benutzer nicht unterstützt IdPs.

Wenn Sie den Kontozugriff für den Administratorbenutzer einrichten, erstellt IAM Identity Center eine entsprechende IAM-Rolle. Diese Rolle, die vom IAM Identity Center gesteuert wird, wird in der entsprechenden AWS-Konto, und die im Berechtigungssatz angegebenen Richtlinien sind der Rolle zugeordnet.

Schritt 5: Loggen Sie sich in die AWS Greifen Sie mit Ihren Administratordaten auf das Portal zu


Gehen Sie wie folgt vor, um zu bestätigen, dass Sie sich bei der anmelden können AWS mit den Anmeldeinformationen des Administratorbenutzers auf das Portal zugreifen, und dass Sie auf das AWS-Konto.

1. Melden Sie sich bei der [AWS Management Console](#) als Kontobesitzer an, indem Sie Stammbenutzer auswählen und Ihre AWS-Konto-E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die AWS IAM Identity Center-Konsole unter <https://console.aws.amazon.com/singlesignon/>.
3. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
4. Auf der Armaturenbrettseite, unter Zusammenfassung der Einstellungen, kopiere die AWS auf die Portal-URL zugreifen.
5. Öffnen Sie einen separaten Browser und fügen Sie den AWS greifen Sie auf die Portal-URL zu, die Sie kopiert haben, und drücken Sie Geben Sie ein.
6. Melden Sie sich mit einer der folgenden Methoden an:
 - Wenn Sie Active Directory oder einen externen Identitätsanbieter (IdP) als Identitätsquelle verwenden, melden Sie sich mit den Anmeldeinformationen des Active Directory- oder IdP-Benutzers an, den Sie dem AdministratorAccessIm IAM Identity Center festgelegte Berechtigung.
 - Wenn Sie das standardmäßige IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, melden Sie sich mit dem Benutzernamen an, den Sie bei der Erstellung des Benutzers angegeben haben, und dem neuen Passwort, das Sie für den Benutzer angegeben haben.
7. Nachdem Sie angemeldet sind, ein AWS-Konto Das Symbol wird im Portal angezeigt.
8. Wenn Sie das auswählen AWS-Konto Symbol, der Kontoname, die Konto-ID und die mit dem Konto verknüpfte E-Mail-Adresse werden angezeigt.

9. Wählen Sie den Namen des Kontos aus, um das anzuzeigen AdministratorAccessBerechtigungssatz, und wählen Sie die Management-Konsole Link rechts von AdministratorAccess.

Wenn Sie sich anmelden, wird der Name des Berechtigungssatzes, dem der Benutzer zugewiesen ist, als verfügbare Rolle in der AWS auf das Portal zugreifen. Weil Sie diesen Benutzer dem zugewiesen haben AdministratorAccessBerechtigungssatz, die Rolle erscheint in der AWS das Portal aufrufen als: AdministratorAccess/*Nutzername*

10. Wenn Sie umgeleitet werden zur AWS Management Console, Sie haben die Einrichtung des Administratorzugriffs auf die erfolgreich abgeschlossen AWS-Konto. Fahren Sie mit Schritt 10 fort.
11. Wechseln Sie zu dem Browser, mit dem Sie sich bei der AWS Management Console und richten Sie das IAM Identity Center ein und melden Sie sich von Ihrem ab AWS-Konto Root-Benutzer.

 **Important**

Wir empfehlen Ihnen dringend, sich an die bewährte Methode zu halten und die Anmeldeinformationen des Administratorbenutzers zu verwenden, wenn Sie sich bei AWS auf das Portal zugreifen und dass Sie die Root-Benutzeranmeldeinformationen nicht für Ihre täglichen Aufgaben verwenden.

Um anderen Benutzern den Zugriff auf Ihre Konten und Anwendungen zu ermöglichen und das IAM Identity Center zu verwalten, sollten Sie Berechtigungssätze nur über IAM Identity Center erstellen und zuweisen.

Problembereiche AWS-Konto-Probleme bei der Erstellung

Verwenden Sie die Informationen hier, um Ihnen bei der Behebung von Problemen im Zusammenhang mit der Erstellung eines AWS-Kontos.

Problembereiche

- [Ich habe den Anruf nicht erhalten von AWS um mein neues Konto zu verifizieren](#)
- [Ich erhalte eine Fehlermeldung über die „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine AWS-Kontoper Telefon](#)
- [Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert](#)

Ich habe den Anruf nicht erhalten von AWS um mein neues Konto zu verifizieren

Wenn Sie ein neues AWS-Konto erstellen, müssen Sie eine Telefonnummer angeben, unter der Sie entweder eine SMS-Textnachricht oder einen Sprachanruf empfangen können. Sie geben an, welche Methode zur Überprüfung der Nummer verwendet werden soll.


Wenn Sie die Nachricht oder den Anruf nicht erhalten, überprüfen Sie Folgendes:

- Sie haben während des Anmeldevorgangs die richtige Telefonnummer eingegeben und die richtige Landesvorwahl ausgewählt.
- Wenn Sie ein Mobiltelefon verwenden, stellen Sie sicher, dass Sie über ein Mobilfunksignal verfügen, um SMS-Textnachrichten oder Anrufe zu empfangen.
- Die Informationen, die Sie für Ihre eingetragene [Zahlungsmethode](#) richtig.

Wenn Sie keine SMS-Textnachricht oder keinen Anruf erhalten haben, um den Identitätsprüfungsprozess abzuschließen, kann AWS Support Ihnen helfen, Ihr AWS-Konto manuell zu aktivieren. Gehen Sie dazu wie folgt vor:

1. Stellen Sie sicher, dass Sie erreichbar sind unter [Telefonnummer](#), die Sie für Ihr Konto bereitgestellt haben.
2. Öffnen Sie die [AWS Support-Konsole](#), und wählen Sie dann **Fall erstellen**.
 - a. Wählen Sie **Konto- und Rechnungssupportservice** aus.

- b. FürTyp, wählenKonto.
- c. FürKategorie, wählenAktivierung.
- d. In derBeschreibung des FallsAbschnitt, geben Sie ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.
- e. In derKontaktmöglichkeitenAbschnitt, wählenPlaudernzumMethoden der Kontaktaufnahme.
- f. Wählen Sie Submit (Absenden) aus.

 Note

Sie können einen Fall erstellen mitAWS Supportauch wenn deinAWS-Kontoist nicht aktiviert.

Ich erhalte eine Fehlermeldung über die „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meineAWS-Kontoper Telefon

AWS Supportkann Ihnen helfen, Ihr Konto manuell zu aktivieren. Dazu gehen Sie wie folgt vor:

1. [Loggen Sie sich in IhrAWS-Konto](#)mit der E-Mail-Adresse und dem Passwort, die Sie bei der Erstellung Ihres Kontos angegeben haben.
2. Öffne die[AWS SupportKonsole](#), und wählen Sie dannFall erstellen.
3. Wählen SieKonto- und Abrechnungsunterstützung.
4. FürTyp, wählenKonto.
5. FürKategorie, wählenAktivierung.
6. In derBeschreibung des FallsAbschnitt, geben Sie ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.
7. In derKontaktmöglichkeitenAbschnitt, wählenPlaudernzumMethoden der Kontaktaufnahme.
8. Wählen Sie Submit (Absenden) aus.

AWS Supportwird sich mit Ihnen in Verbindung setzen und versuchen, Ihre manuell zu aktivierenAWS-Konto.

Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert

Die Kontoaktivierung kann manchmal verzögert werden. Wenn der Vorgang länger als 24 Stunden dauert, überprüfen Sie Folgendes:

- Beenden Sie den Kontoaktivierungsprozess.

Wenn Sie das Fenster für den Anmeldevorgang geschlossen haben, bevor Sie alle erforderlichen Informationen hinzugefügt haben, öffnen Sie die [Anmeldung](#)-Seite. Wählen Sie **Melden Sie sich bei einem bestehenden AWS-Konto**, und melden Sie sich mit der E-Mail-Adresse und dem Passwort an, die Sie für das Konto ausgewählt haben.

- Prüfen Sie die mit Ihrer Zahlungsmethode verknüpften Informationen.

In der **AWS Billing and Cost Management**-Konsole, checken Sie die [Zahlungsmethoden](#) auf Fehler.

- Wenden Sie sich an Ihr Finanzinstitut.

Manchmal lehnen Finanzinstitute Autorisierungsanfragen von **ab AWS**. Wenden Sie sich an die Institution, die Ihrer Zahlungsmethode zugeordnet ist, und bitten Sie sie, Autorisierungsanfragen von **zu genehmigen AWS**. **AWS** storniert die Autorisierungsanfrage, sobald sie von Ihrem Finanzinstitut genehmigt wurde, sodass Ihnen die Autorisierungsanfrage nicht in Rechnung gestellt wird. Autorisierungsanfragen können dennoch als geringe Gebühr (in der Regel 1 USD) auf den Kontoauszügen Ihres Finanzinstituts erscheinen.

- Überprüfen Sie Ihre E-Mail und Ihren Spam-Ordner auf Anfragen nach zusätzlichen Informationen.
- Versuche es mit einem anderen Browser.
- Kontakt **AWS Support**.

Kontakt [AWS Support](#) um Hilfe. Erwähnen Sie alle Schritte zur Fehlerbehebung, die Sie bereits versucht haben.

Note

Geben Sie in keiner Korrespondenz mit vertraulichen Informationen wie Kreditkartennummern an **AWS**.

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.