aws

Benutzerhandbuch

AWSEinrichtung

AWSEinrichtung: Benutzerhandbuch

Table of Contents

Übersicht

Dieses Handbuch enthält Anweisungen zum Erstellen eines neuenAWS-Kontound richten Sie Ihren ersten administrativen Benutzer in einAWS IAM Identity Centerfolgen Sie den neuesten bewährten Sicherheitsmethoden.

EinAWS-Kontoist für den Zugriff erforderlichAWS-Servicesund dient als zwei grundlegende Funktionen:

- Behälter— EinAWS-Kontoist ein Behälter für alleAWSRessourcen, die Sie erstellen können alsAWSKunde. 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 eineRessourcein Ihrem Konto. Jede Ressource wird eindeutig durch einen Amazon-Ressourcennamen (ARN) identifiziert, der die Konto-ID des Kontos enthält, das die Ressource enthält oder besitzt.
- Sicherheitsgrenze— EinAWS-Kontoist die grundlegende Sicherheitsgrenze für IhreAWSRessourcen. 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, gehörenIdentitäten, 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 zugreiftAWS-Servicesindem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. Diese Identitäten verfügen über Anmeldeinformationen, mit denen sich jemand anmelden kann, oderauthentifizierenzuAWS. 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 allgemeine Terminologie, um den Anmeldevorgang zu beschreiben. Wir empfehlen Ihnen, diese Bedingungen zu lesen und zu verstehen.

Administrator

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

Account

Ein Standard AWS-Konto enthält sowohl Ihre AWS Ressourcen als auch 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 Zugangsdaten oder Sicherheitsnachweise bezeichnet. Anmeldeinformationen sind die Informationen, die Benutzer angeben, AWS um sich anzumelden und Zugriff auf AWS Ressourcen zu erhalten. 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 Multifaktor-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. Bei AWS diesen Anmeldeinformationen handelt es sich in der Regel um die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel.

Weitere Informationen zu Anmeldeinformationen finden Sie unter Ihre AWS Anmeldeinformationen verstehen und abrufen.

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

Anmeldeinformationen für Unternehmen

Die Anmeldeinformationen, die Benutzer beim Zugriff auf ihr Unternehmensnetzwerk und ihre Ressourcen angeben. Ihr Unternehmensadministrator kann Sie so einrichtenAWS-Konto, dass Sie mit denselben Anmeldeinformationen zugänglich sind, 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 eine AWS Builder-ID registrieren, erstellen Sie ein Profil. Ihr Profil umfasst die von Ihnen angegebenen Kontaktinformationen und 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. Weitere Informationen zu Ihrem Profil und dessen Beziehung zu einem AWS-Konto finden Sie unter AWSBuilder-ID und andere AWS Anmeldeinformationen.

Benutzer

Ein Benutzer ist eine Person oder Anwendung unter einem Konto, die API-Aufrufe an AWS Produkte tätigt. Jeder Benutzer hat einen eindeutigen Namen AWS-Konto und eine Reihe von Sicherheitsanmeldedaten, die nicht an andere weitergegeben werden. Diese Anmeldeinformationen unterscheiden sich von den Sicherheitsanmeldeinformationen für das AWS-Konto. Jeder Benutzer kann nur einem einzigen AWS-Konto zugeordnet sein.

Anmeldeinformationen des Stammbenutzers

Die Anmeldeinformationen des Root-Benutzers sind dieselben Anmeldeinformationen, mit denen der AWS Management Console Root-Benutzer angemeldet wurde. 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 Bestätigungscodes variieren. Sie können per SMS oder E-Mail gesendet werden. Weitere Informationen erhalten Sie von Ihrem Administrator.

AWSBenutzer und Anmeldeinformationen

Bei der Interaktion mit geben Sie Ihre AWS Sicherheitsanmeldedaten anAWS, um zu überprüfen, wer Sie sind und ob Sie berechtigt sind, auf die von Ihnen angeforderten Ressourcen zuzugreifen. AWSverwendet 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 aus Ihren Anmeldedaten hervorgeht, 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 IhremAWS-Konto. Wenn Sie ein AWS-Konto neu erstellen, enthält es zunächst nur eine einzelne Anmeldeidentität, die über Vollzugriff auf sämtliche AWS-Services und -Ressourcen im Konto verfügt. Diese Identität ist der Root-Benutzer des AWS Kontos. Sie können sich mit der E-Mail-Adresse und dem Passwort, mit denen Sie das Konto erstellt haben, AWS Management Consoleals Root-Benutzer anmelden. Eine schrittweise Anleitung zur Anmeldung finden Sie unter AWS Management ConsoleAls Root-Benutzer anmelden.

> **Important**
>
> 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 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 das AWS Zugriffsportal an. Das AWS Zugriffsportal oder die spezifische Anmelde-URL wird von Ihrem Administrator oder Helpdesk-Mitarbeiter bereitgestellt. Wenn Sie einen IAM Identity Center-Benutzer für Ihren erstellt habenAWS-Konto, wurde eine Einladung zum Beitritt zu einem IAM Identity Center-Benutzer an die E-Mail-Adresse des gesendet. AWS-Konto Die spezifische Anmelde-URL ist in der E-Mail-Einladung enthalten. Benutzer von IAM Identity Center können sich nicht über den anmelden. AWS Management Console Eine schrittweise Anleitung zur Anmeldung finden Sie unter Beim AWSZugriffsportal anmelden.

> **Note**
>
> Wir empfehlen Ihnen, die spezifische Anmelde-URL für das AWS Access-Portal mit einem Lesezeichen zu versehen, 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, die einer IAM-Rolle zugeordnet sindAWS, die Berechtigungen zur Nutzung der Ressourcen in Ihrem. AWS-Konto Sie melden sich nicht mit dem Portal an AWS Management Console oder AWS greifen nicht auf das Portal zu. 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 eine Entität erstellen. AWS Dieser Benutzer ist eine Identität innerhalb von IhnenAWS-Konto, der bestimmte benutzerdefinierte Berechtigungen gewährt wurden. Ihre IAM-Benutzeranmeldeinformationen bestehen aus einem Namen und einem Passwort, mit denen Sie sich bei dem AWS Management Consoleanmelden. Eine schrittweise Anleitung zur Anmeldung finden Sie unter AWS Management ConsoleAls IAM-Benutzer anmelden.

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

AWSBuilder-ID-Benutzer

Als AWS Builder ID-Benutzer melden Sie sich ausdrücklich bei dem AWS Service oder Tool an, auf das Sie zugreifen möchten. Ein AWS Builder ID-Benutzer ergänzt alle Benutzer, die AWS-Konto Sie bereits haben oder erstellen möchten. Eine AWS Builder-ID steht für Sie als Person, und Sie können sie verwenden, um ohne eine AWS-Konto auf AWS Dienste und Tools zuzugreifen. Sie haben auch ein Profil, in dem Sie Ihre Informationen einsehen und aktualisieren können. Weitere Informationen finden Sie unter So melden Sie sich mit der AWS Builder-ID an.

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 unterWas ist MFA?in derIAM-Benutzerhandbuch.
- AWS SupportPlanen— Bei der Kontoerstellung werden Sie aufgefordert, einen der verfügbaren Tarife auszuwählen. Eine Beschreibung der verfügbaren Pläne finden Sie unterVergleicheAWS 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 mitTeil 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 verwendestAWS Managed Microsoft AD, Sie müssen das IAM Identity Center in derselben aktivierenAWS-Regionwo deinAWS Managed Microsoft ADVerzeichnis 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 dieAWSDas 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 oderAWS Managed Microsoft ADVerzeichnis eingerichtet inAWS Directory Service, und es muss in deinemAWS OrganizationsVerwaltungskonto. Sie können nur einen AD-Connector oder einen verbindenAWS Managed Microsoft ADzu einer Zeit. Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden SieAWS Managed Microsoft AD. Weitere Informationen finden Sie unter:

  - Verbinde ein Verzeichnis inAWS Managed Microsoft ADzum IAM Identity Centerin derAWS IAM Identity CenterBenutzerleitfaden.
  - Verbinden Sie ein selbstverwaltetes Verzeichnis in Active Directory mit dem IAM Identity Centerin derAWS IAM Identity CenterBenutzerleitfaden.
- 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 oderAWS Managed Microsoft ADVerzeichnis eingerichtet inAWSVerzeichnis, 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

DeinAWS-Kontomuss verwaltet werden vonAWS Organizations. Wenn Sie keine Organisation gegründet haben, müssen Sie das nicht tun. Wenn Sie IAM Identity Center aktivieren, entscheiden Sie, ob SieAWSerstellen Sie eine Organisation für Sie.

Wenn Sie bereits eingerichtet habenAWS 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 beimAWS Management Consoleindem Sie die Anmeldeinformationen IhresAWS OrganizationsVerwaltungskonto. Sie können das IAM Identity Center nicht aktivieren, während Sie mit Anmeldeinformationen von einemAWS OrganizationsMitgliedskonto. Weitere Informationen finden Sie unterErstellung und Verwaltung einerAWSOrganisationin derAWS OrganizationsBenutzerleitfaden.

IAM-Rollen

Wenn Sie bereits IAM-Rollen in Ihrem konfiguriert habenAWS-Konto, empfehlen wir Ihnen, zu überprüfen, ob sich Ihr Konto dem Kontingent für IAM-Rollen nähert. Weitere Informationen finden Sie unterIAM-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 unterQuotenerhöhung beantragenin derService Quotas — Benutzerhandbuch.

Firewalls der nächsten Generation und sichere Web-Gateways

Wenn Sie den Zugriff auf bestimmteAWSDomänen 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/login
- https://*[deine Region]*.signin.aws/platform/login

Verwenden von mehreren AWS-Konten

AWS-Kontendienen als grundlegende Sicherheitsgrenze inAWS. 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 aufAWS-Kontenhilft 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 könnenAWS-Kontodas alle Elemente Ihres Workloads hostet, die unterliegenSicherheitsstandards der Payment Card Industry (PCI).
- Isolierung— EinAWS-Kontoist eine Einheit des Sicherheitsschutzes. Potenzielle Risiken und Sicherheitsbedrohungen sollten in einemAWS-Kontoohne 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 derAllgemeine Datenschutzverordnung (GDPR) der Europäischen Union.

- Geschäftsprozess— Verschiedene Geschäftsbereiche oder Produkte können völlig unterschiedliche Zwecke und Prozesse haben. Mit mehrerenAWS-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 (mitAWS Organizationsund konsolidierte Fakturierung), wobei die Einzelposten getrennt sind durchAWS-Konto.
- Quotenzuweisung—AWSServicekontingente werden für jeden einzeln durchgesetztAWS-Konto. Aufteilung der Workloads in verschiedeneAWS-Kontenverhindert, dass sie Kontingente füreinander verbrauchen.

Alle in diesem Leitfaden beschriebenen Empfehlungen und Verfahren entsprechen denAWSGut 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 kostenlosesAWSService, um all das zu verwaltenAWS-Kontenin Ihrer Organisation.

AWSbietet auchAWS Control Tower, wodurch Schichten von hinzugefügt werdenAWSverwaltete die Automatisierung für Organisationen und integriert sie automatisch in andereAWSDienstleistungen wieAWS CloudTrail,AWS Config, AmazonasCloudWatch,AWS Service Catalogund 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 mitTeil 2: Einen administrativen Benutzer in IAM Identity Center erstellen.

Themen

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 unterAWS-Konto-Voraussetzungen.
6. Lesen und akzeptieren Sie dieAWSVereinbarung mit dem Kunden.

7. WähleKonto erstellen und fortfahren.

   Zu diesem Zeitpunkt erhalten Sie eine E-Mail-Nachricht, um zu bestätigen, dass IhrAWS-Kontoist 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 verwendenAWSDienste, bis Sie die Aktivierung Ihres Kontos abgeschlossen haben.

8. Auf derInformationen zur ZahlungSeite, 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 SieBenutze eine neue Adresseund geben Sie die Adresse ein, die Sie für Abrechnungszwecke verwenden möchten.

9. WähleÜberprüfen und hinzufügen.

   > **Note**
   >
   > Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Nutzungsvereinbarung für Ihr Konto mit AISPL, einem lokalen UnternehmenAWSVerkäufer 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. DerAWSDas automatische Überprüfungssystem ruft Sie an und gibt Ihnen eine PIN. Geben Sie die PIN mit Ihrem Telefon ein und wählen SieFortfahren.

12. Wählen Sie eineAWS Supportplanen.

    Eine Beschreibung der verfügbaren Pläne finden Sie unterVergleicheAWS 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 neuenAWS-Konto. Bis die Aktivierung abgeschlossen ist, wird möglicherweise einRegistrierung abschließenKnopf. Sie können sie ignorieren.

AWSsendet eine Bestätigungs-E-Mail, wenn die Kontoaktivierung abgeschlossen ist. Überprüfe deine E-Mail und deinen Spam-Ordner auf die Bestätigungs-E-Mail. Nachdem Sie diese Nachricht erhalten haben, haben Sie vollen Zugriff auf alleAWSdienstleistungen.

Schritt 2: Melden Sie sich als Root-Benutzer an

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.

> **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 unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Um sich als Root-Benutzer anzumelden

1. Öffnen Sie die AWS Management Console-Konsole unter 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 fürAWS-Konto.
   > Wenn Sie sich zuvor mit diesem Browser als IAM-Benutzer angemeldet haben, zeigt Ihr Browser möglicherweise stattdessen die Anmeldeseite für IAM-Benutzer an. Um zur Hauptanmeldeseite zurückzukehren, wählen Sie Melden Sie sich mit der E-Mail-Adresse des Stammbenutzers 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 mit Ihrem Konto verknüpfte AWS-Konto 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: Aktivieren Sie MFA für IhrAWS-KontoRoot-Benutzer

Um die Sicherheit Ihrer Root-Benutzeranmeldeinformationen zu erhöhen, empfehlen wir Ihnen, die bewährte Sicherheitsmethode zu befolgen und die Multi-Faktor-Authentifizierung (MFA) für IhrAWS-Konto. Da der Root-Benutzer vertrauliche Vorgänge in Ihrem Konto ausführen kann, können Sie Ihr Konto durch Hinzufügen dieser zusätzlichen Authentifizierungsebene besser schützen. Es sind mehrere Arten von MFA verfügbar.

Anweisungen zur Aktivierung von MFA für den Root-Benutzer finden Sie unterAktivieren von MFA-Geräten für Benutzer inAWSin derIAM-Benutzerhandbuch.

Teil 2: Einen administrativen Benutzer in IAM Identity Center erstellen

Nachdem Sie fertig sindTeil 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 unterErste Schrittein derAWS IAM Identity CenterBenutzerleitfaden.

Themen

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 ausSchritt 3: Aktivieren Sie MFA für IhrAWS-KontoRoot-Benutzerbevor 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 dieIAM Identity Center-Konsole.
3. UnterIAM Identity Center aktivieren, wähleErmöglichen.
4. IAM Identity Center benötigtAWS Organizations. Wenn Sie noch keine Organisation gegründet haben, müssen Sie entscheiden, obAWSerstelle eine für dich. WähleErstellenAWSOrganisationum 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, inAWS Organizations. Weitere Informationen finden Sie unterDelegierte Verwaltungin derAWS IAM Identity CenterBenutzerleitfaden.

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 zuAWS-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 ihreAWS-Kontenund Anwendungen.

Themen

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 verbindenAWS Managed Microsoft ADVerzeichnis, ein selbstverwaltetes Verzeichnis in Active Directory oder ein externer IdP mit IAM Identity Center. Wenn Sie planen, eine Verbindung herzustellenAWS Managed Microsoft ADVerzeichnis oder ein selbstverwaltetes Verzeichnis in

Active Directory, stellen Sie sicher, dass Ihre Active Directory-Konfiguration die Voraussetzungen in erfülltActive Directory oder externer IdP.

> **Note**
>
> Aus Sicherheitsgründen empfehlen wir dringend, die Multi-Faktor-Authentifizierung zu aktivieren. Wenn Sie planen, eine Verbindung herzustellenAWS Managed Microsoft ADVerzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory und Sie verwenden RADIUS MFA nicht mitAWS 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 unterstütztIdPs. Weitere Informationen finden Sie unterMFA aktivierenin derAWS IAM Identity CenterBenutzerleitfaden.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unterStellen Sie eine Verbindung zu einem Microsoft Active Directory her.
2. Folgen Sie den Schritten inVerbinde ein Verzeichnis inAWS Managed Microsoft ADzum 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 unterSynchronisieren Sie einen administrativen Benutzer mit IAM Identity Center.

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unterStellen Sie eine Verbindung zu einem Microsoft Active Directory her.
2. Folgen Sie den Schritten inVerbinden 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 unterSynchronisieren Sie einen administrativen Benutzer in IAM Identity Center.

Externer IdP

1. Lesen Sie die Anleitung unterStellen Sie eine Verbindung zu einem externen Identitätsanbieter her.
2. Folgen Sie den Schritten inSo 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 dieIAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Auf derEinstellungenSeite, wählen Sie dieIdentitätsquelleTab, wähleAktionen, und wählen Sie dannSynchronisierung verwalten.
4. Auf derSynchronisierung verwaltenSeite, wählen Sie dieNutzertippen Sie auf und wählen Sie dannBenutzer und Gruppen hinzufügen.
5. Auf derNutzerTab, unterNutzer, geben Sie den genauen Benutzernamen ein und wählenHinzufügen.
6. UnterBenutzer 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 derSynchronisierung verwaltenSeite, der von Ihnen angegebene Benutzer erscheint in derBenutzer im SynchronisierungsbereichListe.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).
9. Auf derNutzerSeite, 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 dieIAM Identity Center-Konsole.
3. Folgen Sie den Schritten inNutzer hinzufügenum 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 BetreffEinladung zum BeitrittAWSEinmaliges Anmelden. Öffnen Sie die E-Mail und wählen SieEinladung annehmen.
   b. Auf derRegistrierung eines neuen BenutzersSeite, geben Sie ein Passwort ein und bestätigen Sie es und wählen Sie dannNeues Passwort setzen.

> **Note**
>
> Achten Sie darauf, Ihr Passwort zu speichern. Du wirst es später brauchenSchritt 5: Loggen Sie sich in dieAWSGreifen 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 Administratorberechtigungssatz erstellen und den Benutzer diesem Berechtigungssatz zuweisen.

Der nächste Schritt: Schritt 3: Einen Administratorberechtigungssatz erstellen

Schritt 3: Einen Administratorberechtigungssatz erstellen

Berechtigungssätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, die Benutzer und Gruppen auf eineAWS-Konto. Gehen Sie wie folgt vor, um einen Berechtigungssatz 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 dieIAM Identity Center-Konsole.
3. Im Navigationsbereich von IAM Identity Center unterBerechtigungen für mehrere Konten, wähleBerechtigungssätze.
4. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
5. FürSchritt 1: Wählen Sie den Typ des Berechtigungssatzes, auf derWählen Sie den Typ des Berechtigungssatzes ausSeite, behalten Sie die Standardeinstellungen bei und wählen SieWeiter. Die Standardeinstellungen gewähren vollen Zugriff aufAWSDienste und Ressourcen, die denAdministratorAccessvordefinierter Berechtigungssatz.

> **Note**
>
> Das VordefinierteAdministratorAccessDer Berechtigungssatz verwendet dieAdministratorAccess AWSverwaltete Richtlinie.

6. FürSchritt 2: Geben Sie die Details des Berechtigungssatzes an, auf derDetails zum Berechtigungssatz angebenSeite, behalten Sie die Standardeinstellungen bei und wählen SieWeiter. Die Standardeinstellung begrenzt Ihre Sitzung auf eine Stunde.
7. FürSchritt 3: Überprüfen und erstellen, auf derÜberprüfen und erstellenSeite, gehen Sie wie folgt vor:

    1. Überprüfen Sie den Typ des Berechtigungssatzes und vergewissern Sie sich, dass erAdministratorAccess.
    2. Überprüfen Sie dieAWSverwaltete Richtlinie und bestätige, dass dies der Fall istAdministratorAccess.
    3. Wählen Sie Create (Erstellen) aus.

Schritt 4: EinrichtenAWS-KontoZugriff für einen administrativen Benutzer

Zum EinrichtenAWS-KontoZugriff für einen Administratorbenutzer im IAM Identity Center, Sie müssen den Benutzer dem zuweisenAdministratorAccessBerechtigungssatz.

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 dieIAM Identity Center-Konsole.
3. Im Navigationsbereich unterBerechtigungen für mehrere Konten, wähleAWS-Konten.
4. Auf derAWS-KontenSeite, eine Baumstruktur mit einer Liste Ihrer Organisation wird angezeigt. Markieren Sie das Kontrollkästchen neben demAWS-Kontodem Sie Administratorzugriff zuweisen möchten. Wenn Sie in Ihrer Organisation mehrere Konten haben, aktivieren Sie das Kontrollkästchen neben dem Verwaltungskonto.
5. WähleBenutzer oder Gruppen zuweisen.
6. FürSchritt 1: Benutzer und Gruppen auswählen, auf derWeisen Sie Benutzer und Gruppen zu“***AWS-Kontoname***„Seite, gehen Sie wie folgt vor:

    1. Auf derNutzerklicken 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 SieWeiter.

7. FürSchritt 2: Wählen Sie die Berechtigungssätze, auf derOrdnen Sie“ Berechtigungssätze zu***AWS-Kontoname***„Seite, unterBerechtigungssätze, wählen Sie dieAdministratorAccessBerechtigungssatz.
8. Wählen Sie Weiter aus.
9. FürSchritt 3: Überprüfen und Absenden, auf derAufgaben 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 istAdministratorAccessBerechtigungssatz, wählenEinreichen.

   > **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 unterMFA aktivierenum MFA für IAM Identity Center zu aktivieren:

    - Sie verwenden das standardmäßige Identity Center-Verzeichnis als Identitätsquelle.
    - Du verwendest eineAWS Managed Microsoft ADVerzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory als Ihre Identitätsquelle und Sie verwenden RADIUS MFA nicht mitAWS 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 unterstütztIdPs.

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 entsprechendenAWS-Konto, und die im Berechtigungssatz angegebenen Richtlinien sind der Rolle zugeordnet.

Schritt 5: Loggen Sie sich in dieAWSGreifen Sie mit Ihren Administratordaten auf das Portal zu

Gehen Sie wie folgt vor, um zu bestätigen, dass Sie sich bei der anmelden könnenAWSmit den Anmeldeinformationen des Administratorbenutzers auf das Portal zugreifen, und dass Sie auf dasAWS-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 derArmaturenbrettSeite, unterZusammenfassung der Einstellungen, kopiere dieAWSauf die Portal-URL zugreifen.
5. Öffnen Sie einen separaten Browser und fügen Sie denAWSgreifen Sie auf die Portal-URL zu, die Sie kopiert haben, und drücken SieGeben 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 demAdministratorAccessIm 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, einAWS-KontoDas Symbol wird im Portal angezeigt.
8. Wenn Sie das auswählenAWS-KontoSymbol, 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 anzuzeigenAdministratorAccessBerechtigungssatz, und wählen Sie dieManagement-KonsoleLink rechts vonAdministratorAccess.

   Wenn Sie sich anmelden, wird der Name des Berechtigungssatzes, dem der Benutzer zugewiesen ist, als verfügbare Rolle in derAWSauf das Portal zugreifen. Weil Sie diesen Benutzer dem zugewiesen haben`AdministratorAccess`Berechtigungssatz, die Rolle erscheint in derAWSdas Portal aufrufen als:`AdministratorAccess/`*`Nutzername`*
10. Wenn Sie umgeleitet werden zurAWSManagement Console, Sie haben die Einrichtung des Administratorzugriffs auf die erfolgreich abgeschlossenAWS-Konto. Fahren Sie mit Schritt 10 fort.
11. Wechseln Sie zu dem Browser, mit dem Sie sich bei derAWS Management Consoleund richten Sie das IAM Identity Center ein und melden Sie sich von Ihrem abAWS-KontoRoot-Benutzer.

    > **Important**
    >
    > Wir empfehlen Ihnen dringend, sich an die bewährte Methode zu halten und die Anmeldeinformationen des Administratorbenutzers zu verwenden, wenn Sie sich beiAWSauf 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.

ProblembehebungAWS-KontoProbleme bei der Erstellung

Verwenden Sie die Informationen hier, um Ihnen bei der Behebung von Problemen im Zusammenhang mit der Erstellung einesAWS-Konto.

Problembereiche

- Ich habe den Anruf nicht erhalten vonAWSum mein neues Konto zu verifizieren
- Ich erhalte eine Fehlermeldung über die „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meineAWS-Kontoper Telefon
- Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert

Ich habe den Anruf nicht erhalten vonAWSum mein neues Konto zu verifizieren

Wenn Sie eine erstellenAWS-Konto, 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 eingegeben habenZahlungsmethodeist richtig.

Wenn Sie keine SMS-Textnachricht oder keinen Anruf erhalten haben, um den Identitätsprüfungsprozess abzuschließen,AWS Supportkann dir helfen, deinAWS-Kontomanuell. Gehen Sie dazu wie folgt vor:

1. Stellen Sie sicher, dass Sie erreichbar sind unterTelefonnummerdie du für deine bereitgestellt hastAWS-Konto.
2. Öffne dieAWS SupportKonsole, und wählen Sie dannFall 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-Kontomit der E-Mail-Adresse und dem Passwort, die Sie bei der Erstellung Ihres Kontos angegeben haben.
2. Öffne dieAWS 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 dasAnmeldungSeite. Wählen SieMelden Sie sich bei einem bestehendenAWS-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 derAWS Billing and Cost ManagementKonsole, checkZahlungsmethodenfür Fehler.
- Wenden Sie sich an Ihr Finanzinstitut.

  Manchmal lehnen Finanzinstitute Autorisierungsanfragen von abAWS. Wenden Sie sich an die Institution, die Ihrer Zahlungsmethode zugeordnet ist, und bitten Sie sie, Autorisierungsanfragen von zu genehmigenAWS.AWSstorniert die Autorisierungsanfrage, sobald sie von Ihrem Finanzinstitut genehmigt wurde, sodass Ihnen die Autorisierungsanfrage nicht in Rechnung gestellt wird. Autorisierungsanfragen können 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.
- KontaktAWS Support.

  KontaktAWS Supportum Hilfe. Erwähnen Sie alle Schritte zur Fehlerbehebung, die Sie bereits versucht haben.

> **Note**
>
> Geben Sie in keiner Korrespondenz mit vertraulichen Informationen wie Kreditkartennummern anAWS.

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.