Benutzerhandbuch

AWS Einrichtung

AWS Einrichtung: Benutzerhandbuch

Table of Contents

Übersicht

Dieses Handbuch enthält Anweisungen zum Erstellen eines neuen Benutzers AWS-Konto und zum Einrichten Ihres ersten Administratorbenutzers AWS IAM Identity Center gemäß den neuesten bewährten Sicherheitsmethoden.

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

- Container — An AWS-Konto ist ein Container für alle AWS Ressourcen, die Sie als AWS Kunde erstellen können. 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-Ressourcennamen (ARN) identifiziert, der die Konto-ID des Kontos enthält, das die Ressource enthält oder besitzt.
- Sicherheitsgrenze — An 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 föderierte Identitäten, z. B. Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter, dem IAM Identity Center-Verzeichnis oder jedem anderen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Diese Identitäten verfügen über Anmeldeinformationen, mit denen sich jemand anmelden oder authentifizieren kann. AWS Identitäten verfügen auch über Berechtigungsrichtlinien, die festlegen, was die Person, die sich angemeldet hat, mit den Ressourcen im Konto tun darf.

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 legen Einstellungen für die fest und implementieren sie AWS-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 Zugangs- oder Sicherheitsanmeldedaten 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.

Unternehmensanmeldedaten

Die Anmeldeinformationen, die Benutzer beim Zugriff auf ihr Unternehmensnetzwerk und ihre Ressourcen angeben. Ihr Unternehmensadministrator kann Sie so einrichten AWS-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 AWS Builder-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

Bei den Root-Benutzeranmeldedaten handelt es sich um 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 Textnachricht oder E-Mail gesendet werden. Wenden Sie sich an Ihren Administrator, um weitere Informationen zu erhalten.

AWS Benutzer und Anmeldeinformationen

Bei der Interaktion mit geben Sie Ihre AWS Sicherheitsanmeldedaten an AWS, 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 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 Ihrem AWS-Konto. Wenn Sie zum ersten Mal eine erstellen AWS-Konto, beginnen Sie mit einer einzigen Anmeldeidentität, die vollständigen Zugriff auf alle AWS Dienste und Ressourcen im Konto hat. Bei dieser Identität handelt es sich um den 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 Console Als Root-Benutzer anmelden.

> **Important**
>
> Wenn Sie eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

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 haben AWS-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 AWS Zugriffsportal 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 sind AWS , 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 Ihnen AWS-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 Console Als IAM-Benutzer anmelden.

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 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, sollten Sie die Kontoanforderungen überprüfen, überlegen, ob Sie mehr als einen benötigen AWS-Konto, und sich mit den Anforderungen für die Einrichtung Ihres Kontos für den Administratorzugriff in IAM Identity Center vertraut machen.

AWS-Konto Anforderungen

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

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

  Wir empfehlen Ihnen, einen Standard für Kontonamen zu verwenden, damit der Kontoname leicht erkannt und von anderen Konten unterschieden werden kann, die Sie möglicherweise besitzen. Wenn es sich um ein Unternehmenskonto handelt, sollten Sie in Erwägung ziehen, einen Benennungsstandard wie Organisation — Zweck — Umgebung zu verwenden (z. B. AnyCompany— Audit — Produktion). Wenn es sich um ein Privatkonto handelt, sollten Sie erwägen, einen Benennungsstandard wie Vorname — Nachname — Zweck zu verwenden (z. B. paulo-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 wird. Sie müssen in der Lage sein, Nachrichten zu empfangen, die an diese E-Mail-Adresse gesendet wurden. 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 Unternehmensverteilerliste 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`). Auf diese Weise wird sichergestellt, dass Ihr Unternehmen darauf zugreifen kann, AWS-Konto falls 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. Auf diese Weise wird sichergestellt, dass Ihr Unternehmen darauf zugreifen kann, AWS-Konto falls ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt.

- Ein Multi-Faktor-Authentifizierungsgerät — Um Ihre AWS Ressourcen zu schützen, aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für das Root-Benutzerkonto. Zusätzlich zu Ihren regulären Anmeldedaten 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? im IAM-Benutzerhandbuch.
- Support Plan — Sie werden bei der Kontoerstellung aufgefordert, einen der verfügbaren Pläne auszuwählen. Eine Beschreibung der verfügbaren Pläne finden Sie unter Support Tarife vergleichen.

Überlegungen zu IAM Identity Center

Die folgenden Themen enthalten Anleitungen zur Einrichtung von IAM Identity Center für bestimmte Umgebungen. Machen Sie sich mit den Anleitungen vertraut, die für Ihre Umgebung gelten, bevor Sie fortfahrenTeil 2: Einen Administratorbenutzer in IAM Identity Center erstellen.

Themen

- Active Directory oder externer IdP
- AWS Organizations
- IAM-Rollen
- Firewalls und sichere Web-Gateways der nächsten Generation

Active Directory oder externer IdP

Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen IdP verwalten, empfehlen wir Ihnen, eine Verbindung zu dieser Identitätsquelle in Betracht zu ziehen, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Wenn Sie dies tun, bevor Sie Benutzer und Gruppen im standardmäßigen Identity Center-Verzeichnis 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 Sie es verwenden AWS Managed Microsoft AD, müssen Sie IAM Identity Center dort aktivieren AWS-Region , wo Ihr AWS Managed Microsoft AD Verzeichnis eingerichtet ist. IAM Identity Center speichert die Zuweisungsdaten in derselben Region wie das Verzeichnis. Um IAM Identity Center zu verwalten, müssen Sie möglicherweise zu der Region wechseln, in der IAM Identity Center konfiguriert ist. Beachten Sie außerdem, dass das AWS Zugriffsportal dieselbe Zugriffs-URL wie Ihr Verzeichnis verwendet.
- Verwenden Sie ein Active Directory, das sich in Ihrem Verwaltungskonto befindet:

  Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis eingerichtet haben AWS Directory Service, und es muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können nur einen AD Connector oder einen nach AWS Managed Microsoft AD dem anderen verbinden. Wenn Sie mehrere Domänen oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie unter:

  - Stellen Sie im AWS IAM Identity Center Benutzerhandbuch eine Connect AWS Managed Microsoft AD zu IAM Identity Center her.
  - Connect ein selbstverwaltetes Verzeichnis in Active Directory mit dem IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

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

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

Verzeichnis in dem delegierten IAM Identity Center-Administrator-Mitgliedskonto befinden (diesem gehören), falls eines existiert; andernfalls muss es sich im Verwaltungskonto befinden.

AWS Organizations

Ihr Konto AWS-Konto muss von verwaltet werden. AWS Organizations Wenn Sie keine Organisation gegründet haben, müssen Sie das auch nicht tun. Wenn Sie IAM Identity Center aktivieren, wählen Sie aus, ob Sie eine Organisation für Sie AWS erstellen lassen möchten.

Wenn Sie es 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 mit den AWS Management Console Anmeldeinformationen Ihres AWS Organizations Verwaltungskontos bei der anmelden. Sie können IAM Identity Center nicht aktivieren, während Sie mit den Anmeldeinformationen eines AWS Organizations Mitgliedskontos angemeldet sind. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter AWS Organisation erstellen und verwalten.

IAM-Rollen

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

Wenn Sie sich dem Kontingent nähern, sollten Sie erwägen, eine Erhöhung des Kontingents zu beantragen. Andernfalls könnten Probleme mit IAM Identity Center auftreten, wenn Sie Berechtigungssätze für Konten bereitstellen, die das IAM-Rollenkontingent überschritten haben. Informationen dazu, wie Sie eine Kontingenterhöhung beantragen können, finden Sie unter Eine Kontingenterhöhung beantragen im Service Quotas Quota-Benutzerhandbuch.

Firewalls und sichere Web-Gateways der nächsten Generation

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

Spezifische DNS-Domänen

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

Spezifische URL-Endpunkte

- https://*[yourdirectory]*.awsapps.com/start
- https://*[yourdirectory]*.awsapps.com/login
- https://.signin. *[yourregion]* aws/platform/login

Verwenden mehrerer 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.

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

- Sicherheitskontrolle — Verschiedene Anwendungen können unterschiedliche Sicherheitsprofile haben, die unterschiedliche Kontrollrichtlinien und -mechanismen erfordern. So ist es beispielsweise einfacher, mit einem Prüfer zu sprechen und auf ein einzelnes System verweisen zu können AWS-Konto , das alle Elemente Ihres Workloads hostet, die den Sicherheitsstandards der Payment Card Industry (PCI) unterliegen.
- Isolierung — An AWS-Konto ist eine Sicherheitseinheit. Potenzielle Risiken und Sicherheitsbedrohungen sollten in einer enthalten sein, 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 trennen AWS-Konten.
- Datenisolierung — Neben der Isolierung der Teams ist es wichtig, die Datenspeicher für ein Konto zu isolieren. Dies kann dazu beitragen, die Anzahl der Personen zu begrenzen, die auf diesen Datenspeicher zugreifen und ihn verwalten können. Dies trägt dazu bei, den Zugriff auf äußerst private Daten einzudämmen und kann daher zur Einhaltung der Allgemeinen Datenschutzverordnung (DSGVO) der Europäischen Union beitragen.

- Geschäftsprozess — Verschiedene Geschäftsbereiche oder Produkte können völlig unterschiedliche Zwecke und Prozesse haben. Mit mehreren AWS-Konten können Sie die spezifischen Bedürfnisse einer Geschäftseinheit erfüllen.
- Abrechnung — Ein Konto ist die einzig wahre Möglichkeit, Artikel auf Abrechnungsebene zu trennen. Mithilfe mehrerer Konten können Artikel auf Abrechnungsebene nach Geschäftseinheiten, Funktionsteams oder einzelnen Benutzern getrennt werden. Sie können weiterhin alle Ihre Rechnungen an einen einzigen Zahler konsolidieren (mithilfe AWS Organizations und konsolidierter Abrechnung) und gleichzeitig die Einzelposten durch AWS-Konto trennen.
- Kontingentzuweisung — AWS Servicekontingenten werden für jeden Service separat durchgesetzt. AWS-Konto Durch die Aufteilung der Workloads in verschiedene Workloads AWS-Konten wird verhindert, dass sie sich gegenseitig Kontingente verbrauchen.

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

Bevor Sie beginnen, mehrere Konten hinzuzufügen, sollten Sie einen Plan für deren Verwaltung entwickeln. Aus diesem Grund empfehlen wir Ihnen AWS Organizations, diesen kostenlosen AWS Service zu nutzen, um alle Daten AWS-Konten in Ihrem Unternehmen zu verwalten.

AWS bietet auch AWS Control Tower, wodurch Organizations Ebenen AWS verwalteter Automatisierung hinzugefügt und diese automatisch in andere AWS Dienste wie AWS CloudTrail, AWS Config CloudWatch AWS Service Catalog, Amazon und andere integriert werden. Für diese Dienste können zusätzliche Kosten anfallen. Weitere Informationen finden Sie unter AWS Control Tower Preise.

Teil 1: Richten Sie ein neues ein AWS-Konto

Diese Anweisungen helfen Ihnen dabei, Root-Benutzeranmeldeinformationen zu erstellen AWS-Konto und zu sichern. Führen Sie alle Schritte aus, bevor Sie fortfahrenTeil 2: Einen Administratorbenutzer in IAM Identity Center erstellen.

Themen

Schritt 1: Eröffnen Sie ein AWS Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Wählen Sie Create an AWS-Konto.

   > **Note**
   >
   > Wenn Sie sich AWS vor Kurzem angemeldet haben, wählen Sie In der Konsole anmelden. Wenn die Option Neues Konto erstellen AWS-Konto nicht angezeigt wird, wählen Sie zuerst Bei einem anderen Konto anmelden und dann Neues Konto erstellen aus AWS-Konto.

3. Geben Sie Ihre Kontoinformationen ein und wählen Sie dann Weiter.

   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. Wählen Sie Persönlich oder Professionell.

   Der Unterschied zwischen diesen Optionen besteht nur in den Informationen, nach denen wir Sie fragen. Beide Kontotypen haben dieselben Merkmale und Funktionen.
5. Geben Sie Ihre Unternehmens- oder persönlichen Daten gemäß den Anweisungen unter einAWS-Konto Anforderungen.
6. Lesen und akzeptieren Sie die AWS Kundenvereinbarung.

7. Wählen Sie Konto erstellen und Weiter.

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

8. Geben Sie auf der Seite mit den Zahlungsinformationen die Informationen zu Ihrer Zahlungsmethode ein. Wenn Sie eine andere Adresse als die verwenden möchten, mit der Sie das Konto erstellt haben, wählen Sie Neue Adresse verwenden und geben Sie die Adresse ein, die Sie für Rechnungszwecke verwenden möchten.

9. Wählen Sie Verifizieren und Hinzufügen.

   > **Note**
   >
   > Wenn sich Ihre Kontaktadresse in Indien befindet, besteht Ihre Benutzervereinbarung für Ihr Konto mit AISPL, einem lokalen AWS Verkäufer in Indien. Sie müssen Ihre Kartenprüfnummer (CVV) als Teil des Verifizierungsprozesses angeben. Abhängig von Ihrer Bank müssen Sie möglicherweise auch ein Einmalpasswort eingeben. AISPL berechnet Ihrer Zahlungsmethode im Rahmen des Überprüfungsprozesses 2 INR. AISPL erstattet die 2 INR nach Abschluss der Überprüfung.

10. Um Ihre Telefonnummer zu verifizieren, wählen Sie Ihre Landes- oder Regionalvorwahl aus der Liste 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. Das AWS automatische Überprüfungssystem ruft Sie an und gibt Ihnen eine PIN. Geben Sie die PIN mit Ihrem Telefon ein und wählen Sie dann Weiter.

12. Wählen Sie einen Support Plan aus.

    Eine Beschreibung der verfügbaren Pläne finden Sie unter Support Tarife vergleichen.

    Eine Bestätigungsseite wird 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 anmelden AWS-Konto. Bis die Aktivierung abgeschlossen ist, wird möglicherweise die Schaltfläche „Registrierung abschließen“ angezeigt. Sie können sie ignorieren.

AWS sendet eine Bestätigungs-E-Mail, wenn die Kontoaktivierung abgeschlossen ist. Suchen Sie in Ihrem E-Mail- und Spam-Ordner nach der Bestätigungs-E-Mail. Nachdem Sie diese Nachricht erhalten haben, haben Sie vollen Zugriff auf alle AWS Dienste.

Schritt 2: Melden Sie sich als Root-Benutzer an

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

Important

Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Um sich als Root-Benutzer anzumelden

1. Öffnen Sie das AWS Management Console 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 für AWS-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: MFA für Ihren AWS-Konto Root-Benutzer aktivieren

Um die Sicherheit Ihrer Root-Benutzeranmeldeinformationen zu erhöhen, empfehlen wir Ihnen, die bewährte Sicherheitsmethode zu befolgen, um die Multi-Faktor-Authentifizierung (MFA) für Ihre zu aktivieren. 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 sind mehrere Arten von MFA verfügbar.

Anweisungen zur Aktivierung von MFA für den Root-Benutzer finden Sie unter Aktivieren von MFA-Geräten für Benutzer AWS im IAM-Benutzerhandbuch.

Teil 2: Einen Administratorbenutzer in IAM Identity Center erstellen

Nachdem Sie den Vorgang abgeschlossen habenTeil 1: Richten Sie ein neues ein AWS-Konto, helfen Ihnen die folgenden Schritte dabei, AWS-Konto den Zugriff für einen Administratorbenutzer einzurichten, der für die Ausführung der täglichen Aufgaben verwendet wird.

> **Note**
>
> Dieses Thema enthält die mindestens erforderlichen Schritte für die erfolgreiche Einrichtung des Administratorzugriffs für einen AWS-Konto und die Erstellung eines Administratorbenutzers in IAM Identity Center. Weitere Informationen finden Sie unter Erste Schritte im AWS IAM Identity Center Benutzerhandbuch.

Themen

Schritt 1: IAM Identity Center aktivieren

> **Note**
>
> Wenn Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer nicht aktiviert haben, schließen Sie den Vorgang ab, Schritt 3: MFA für Ihren AWS-Konto Root-Benutzer aktivieren bevor Sie fortfahren.

Um IAM Identity Center zu aktivieren

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die IAM-Identity-Center-Konsole.
3. Wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren aus.
4. IAM Identity Center erfordert AWS Organizations. Wenn Sie noch keine Organisation eingerichtet haben, müssen Sie wählen, ob Sie eine für Sie AWS erstellen lassen möchten. Wählen Sie AWS Organisation erstellen, um diesen Vorgang abzuschließen.

   AWS Organizations sendet 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 in AWS Organizations benötigen. Weitere Informationen finden Sie im Benutzerhandbuch unter Delegierte Administration.AWS IAM Identity Center

Schritt 2: Wählen Sie Ihre Identitätsquelle

Ihre Identitätsquelle in IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Sie können eine der folgenden Optionen 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 ihren AWS-Konten und -Anwendungen deren Zugriffsebene zu.
- Active Directory — Wählen Sie diese Option, wenn Sie weiterhin Benutzer entweder in Ihrem AWS Managed 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 Administratorrechte zu. AWS-Konto

> **Important**
>
> Wenn Sie bereits Benutzer und Gruppen in Active Directory oder einem externen Identitätsanbieter (IdP) verwalten, empfehlen wir Ihnen, eine Verbindung zu dieser Identitätsquelle in Betracht zu ziehen, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Dies sollte geschehen, bevor Sie Benutzer und Gruppen im Identity Center-Standardverzeichnis 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 in IAM Identity Center, den Single Sign-On-Zugriff auf ihre AWS-Konten Anwendungen.

Themen

Connect 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 IAM Identity Center zu verbinden.

Sie können ein AWS Managed Microsoft AD Verzeichnis, ein selbstverwaltetes Verzeichnis in Active Directory oder einen externen IdP mit IAM Identity Center verbinden. Wenn Sie beabsichtigen, ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory

zu verbinden, stellen Sie sicher, dass Ihre Active Directory-Konfiguration die Voraussetzungen unter erfüllt. Active Directory oder externer IdP

> **Note**
>
> Aus Sicherheitsgründen empfehlen wir dringend, die Multi-Faktor-Authentifizierung zu aktivieren. Wenn Sie beabsichtigen, ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory zu verbinden und Sie RADIUS MFA nicht mit verwenden AWS Directory Service, aktivieren Sie MFA in IAM Identity Center. Wenn Sie planen, einen externen Identitätsanbieter zu verwenden, beachten Sie, dass der externe IdP, nicht IAM Identity Center, die MFA-Einstellungen verwaltet. MFA in IAM Identity Center wird für die externe Verwendung nicht unterstützt. IdPs Weitere Informationen finden Sie unter MFA aktivieren im AWS IAM Identity Center Benutzerhandbuch.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unter Connect zu einem Microsoft Active Directory herstellen.
2. Folgen Sie den Schritten unter Ein Verzeichnis mit IAM Identity Center verbinden. AWS Managed Microsoft AD
3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter Synchronisieren eines Administratorbenutzers mit IAM Identity Center.

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitung unter Connect zu einem Microsoft Active Directory herstellen.
2. Folgen Sie den Schritten unter Connect eines selbstverwalteten Verzeichnisses in Active Directory mit dem IAM Identity Center.
3. Konfigurieren Sie Active Directory so, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center synchronisiert wird. Weitere Informationen finden Sie unter Synchronisieren eines Administratorbenutzers in IAM Identity Center.

Externer IdP

1. Lesen Sie die Hinweise unter Connect einem externen Identitätsanbieter herstellen.

2. Folgen Sie den Schritten unter So stellen Sie eine Verbindung zu einem externen Identitätsanbieter her.
3. Konfigurieren Sie Ihren IdP so, dass er Benutzer für das IAM Identity Center bereitstellt.

> **Note**
>
> Bevor Sie die automatische, gruppenbasierte Bereitstellung all Ihrer Mitarbeiteridentitäten von Ihrem IdP in IAM Identity Center einrichten, empfehlen wir Ihnen, den einen Benutzer, dem Sie Administratorrechte gewähren möchten, mit IAM Identity Center zu synchronisieren.

Synchronisieren Sie einen Administratorbenutzer mit IAM Identity Center

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

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, klicken Sie auf „Aktionen“ und anschließend auf „Synchronisation verwalten“.
4. Wählen Sie auf der Seite „Synchronisation verwalten“ die Registerkarte „Benutzer“ und dann „Benutzer und Gruppen hinzufügen“ aus.
5. Geben Sie auf der Registerkarte Benutzer unter Benutzer den genauen Benutzernamen ein und wählen Sie Hinzufügen aus.
6. Gehen Sie unter Hinzugefügte Benutzer und Gruppen wie folgt vor:
   a. Vergewissern Sie sich, dass der Benutzer, dem Sie Administratorrechte gewähren möchten, angegeben ist.
   b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.
   c. Wählen Sie Absenden aus.
7. Auf der Seite „Synchronisation verwalten“ wird der von Ihnen angegebene Benutzer in der Liste „Synchronisierte Benutzer“ angezeigt.
8. Klicken Sie im Navigationsbereich auf Users (Benutzer).

9. Auf der Seite Benutzer kann es 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.

Nächster Schritt: Schritt 3: Erstellen Sie einen Administratorberechtigungssatz

Verwenden Sie das Standardverzeichnis und erstellen Sie einen Benutzer in 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 AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die IAM-Identity-Center-Konsole.
3. Folgen Sie den Schritten unter Benutzer hinzufügen, um einen Benutzer zu erstellen.

   Wenn Sie die Benutzerdetails angeben, können Sie entweder eine E-Mail mit den Anweisungen zur Einrichtung des Passworts 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 zum Senden einer E-Mail mit Anweisungen zur Einrichtung des Kennworts beibehalten haben, gehen Sie wie folgt vor:

   a. Sie erhalten eine E-Mail mit dem Betreff Einladung zur Teilnahme an AWS Single Sign-On. Öffnen Sie die E-Mail und wählen Sie Einladung annehmen aus.

   b. Geben Sie auf der Anmeldeseite für neue Benutzer ein Passwort ein, bestätigen Sie es und wählen Sie dann Neues Passwort einrichten.

> **Note**
>
> Achten Sie darauf, Ihr Passwort zu speichern. Sie werden es später auch benötigenSchritt 5: Melden Sie sich mit Ihren Administratoranmeldedaten beim AWS Access Portal an.

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.

Nächster Schritt: Schritt 3: Erstellen Sie einen Administratorberechtigungssatz

Schritt 3: Erstellen Sie einen Administratorberechtigungssatz

Berechtigungssätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, auf die Benutzer und Gruppen zugreifen können. AWS-Konto Führen Sie die folgenden Schritte aus, um einen Berechtigungssatz zu erstellen, der Administratorberechtigungen gewährt.

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die IAM-Identity-Center-Konsole.
3. Wählen Sie im Navigationsbereich von IAM Identity Center unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
4. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
5. Für Schritt 1: Wählen Sie den Typ des Berechtigungssatzes aus, behalten Sie auf der Seite Berechtigungssatztyp auswählen die Standardeinstellungen bei und wählen Sie Weiter. Die Standardeinstellungen gewähren vollen Zugriff auf AWS Dienste und Ressourcen mithilfe des AdministratorAccessvordefinierten Berechtigungssatzes.

> **Note**
>
> Der vordefinierte AdministratorAccessBerechtigungssatz verwendet die AdministratorAccess AWS verwaltete Richtlinie.

6. Für Schritt 2: Details zum Berechtigungssatz angeben behalten Sie auf der Seite Details zum Berechtigungssatz angeben die Standardeinstellungen bei und klicken Sie auf Weiter. Die Standardeinstellung beschränkt Ihre Sitzung auf eine Stunde.
7. Gehen Sie für Schritt 3: Überprüfen und erstellen auf der Seite Überprüfen und erstellen wie folgt vor:

    1. Überprüfen Sie den Typ des Berechtigungssatzes und vergewissern Sie sich, dass dies der Fall ist AdministratorAccess.
    2. Überprüfen Sie die AWS verwaltete Richtlinie und vergewissern Sie sich, dass dies der Fall ist AdministratorAccess.
    3. Wählen Sie Create (Erstellen) aus.

Schritt 4: AWS-Konto Zugriff für einen Administratorbenutzer einrichten

Um den AWS-Konto Zugriff für einen Administratorbenutzer in IAM Identity Center einzurichten, müssen Sie den Benutzer dem AdministratorAccessBerechtigungssatz zuweisen.

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die IAM-Identity-Center-Konsole.
3. Wählen Sie im Navigationsbereich unter Berechtigungen für mehrere Konten die Option AWS-Konten.
4. Auf der AWS-KontenSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Aktivieren Sie das Kontrollkästchen AWS-Konto neben dem, dem Sie Administratorzugriff zuweisen möchten. Wenn Sie in Ihrer Organisation mehrere Konten haben, aktivieren Sie das Kontrollkästchen neben dem Verwaltungskonto.
5. Wählen Sie Benutzer oder Gruppen zuweisen aus.
6. Gehen Sie für Schritt 1: Benutzer und Gruppen auswählen auf der Seite Benutzer und Gruppen zuweisen zu ***AWS-account-name*** "" wie folgt vor:

    1. Wählen Sie auf der Registerkarte Benutzer den Benutzer aus, dem Sie Administratorberechtigungen gewähren möchten.

Um die Ergebnisse zu filtern, geben Sie zunächst den Namen des gewünschten Benutzers in das Suchfeld ein.

2. Nachdem Sie bestätigt haben, dass der richtige Benutzer ausgewählt wurde, wählen Sie Weiter.

7. Wählen Sie für Schritt 2: Berechtigungssätze auswählen auf der Seite „Berechtigungssätze zuweisen***AWS-account-name***“ unter Berechtigungssätze den AdministratorAccessBerechtigungssatz aus.
8. Wählen Sie Weiter.
9. Gehen Sie für Schritt 3: Überprüfen und abschicken auf der Seite Aufgaben überprüfen und einreichen an ***AWS-account-name*** "" wie folgt vor:

   1. Überprüfen Sie den ausgewählten Benutzer und den ausgewählten Berechtigungssatz.
   2. Nachdem Sie sich vergewissert haben, dass dem AdministratorAccessBerechtigungssatz der richtige Benutzer zugewiesen wurde, wählen Sie Senden aus.

   > **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.
    - Sie verwenden ein AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory als Identitätsquelle und Sie verwenden RADIUS MFA nicht mit. AWS Directory Service

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

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

Schritt 5: Melden Sie sich mit Ihren Administratoranmeldedaten beim AWS Access Portal an

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass Sie sich mit den Anmeldeinformationen des Administratorbenutzers beim AWS Access Portal anmelden können und dass Sie auf das zugreifen können AWS-Konto.

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
2. Öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
3. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
4. Kopieren Sie auf der Dashboard-Seite unter Zusammenfassung der Einstellungen die URL des AWS Zugriffsportals.
5. Öffnen Sie einen separaten Browser, fügen Sie die kopierte AWS Access-Portal-URL ein und drücken Sie die Eingabetaste.
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 AdministratorAccessBerechtigungssatz in IAM Identity Center zugewiesen haben.
   - 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 sich angemeldet haben, wird im Portal ein AWS-KontoSymbol angezeigt.
8. Wenn Sie das AWS-KontoSymbol auswählen, werden der Kontoname, die Konto-ID und die E-Mail-Adresse angezeigt, die dem Konto zugeordnet sind.

9. Wählen Sie den Namen des Kontos, für das der AdministratorAccessBerechtigungssatz angezeigt werden soll, und klicken Sie rechts neben auf den Link Management Console AdministratorAccess.

   Wenn Sie sich anmelden, wird der Name des Berechtigungssatzes, dem der Benutzer zugewiesen ist, als verfügbare Rolle im AWS Zugriffsportal angezeigt. Da Sie diesen Benutzer dem `AdministratorAccess` Berechtigungssatz zugewiesen haben, wird die Rolle im AWS Access-Portal wie folgt angezeigt:`AdministratorAccess/`*`username`*
10. Wenn Sie zur AWS Management Console weitergeleitet werden, haben Sie 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 beim IAM Identity Center angemeldet AWS Management Console und es eingerichtet haben, und melden Sie sich von Ihrem AWS-Konto Root-Benutzer ab.

> **Important**
>
> Wir empfehlen Ihnen dringend, sich an die bewährte Methode zu halten und die Anmeldeinformationen des Administratorbenutzers zu verwenden, wenn Sie sich im AWS Access Portal anmelden, und dass Sie die Root-Benutzeranmeldedaten nicht für Ihre täglichen Aufgaben verwenden.

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

Behebung AWS-Konto von Problemen bei der Erstellung

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

Problembereiche

- Ich habe den Anruf von AWS zur Bestätigung meines neuen Kontos nicht erhalten
- Ich erhalte die Fehlermeldung „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine Versuche AWS-Konto telefonisch zu verifizieren
- Es ist mehr als 24 Stunden her und mein Konto ist nicht aktiviert

Ich habe den Anruf von AWS zur Bestätigung meines neuen Kontos nicht erhalten

Wenn Sie eine erstellen AWS-Konto, müssen Sie eine Telefonnummer angeben, unter der Sie entweder eine SMS-Textnachricht oder einen Sprachanruf empfangen können. Sie geben an, mit welcher Methode die Nummer verifiziert werden soll.

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

- Sie haben bei der Registrierung die richtige Telefonnummer eingegeben und die richtige Landesvorwahl ausgewählt.
- Wenn Sie ein Mobiltelefon verwenden, stellen Sie sicher, dass Sie über ein Mobilfunksignal verfügen, mit dem Sie SMS-Textnachrichten oder Anrufe empfangen können.
- Die Informationen, die Sie für Ihre Zahlungsmethode eingegeben haben, sind korrekt.

Wenn Sie keine SMS-Textnachricht oder keinen Anruf erhalten haben, um den Identitätsprüfungsprozess abzuschließen, Support kann Ihnen dies bei der AWS-Konto manuellen Aktivierung helfen. Gehen Sie dazu wie folgt vor:

1. Stellen Sie sicher, dass Sie unter der Telefonnummer erreichbar sind, die Sie für Ihre angegeben haben AWS-Konto.
2. Öffnen Sie die AWS -Support Konsole und wählen Sie dann Kundenvorgang erstellen aus.
   a. Wählen Sie Konto- und -Rechnungssupportservice aus.

b. Wählen Sie als Typ die Option Konto aus.

c. Wählen Sie als Kategorie die Option Aktivierung aus.

d. Geben Sie im Abschnitt Fallbeschreibung ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.

e. Wählen Sie im Abschnitt Kontaktoptionen die Option Chat für Kontaktmethoden aus.

f. Wählen Sie Absenden aus.

> **Note**
>
> Sie können einen Kundenvorgang mit erstellen, Support auch wenn Ihr AWS-Konto Konto nicht aktiviert ist.

Ich erhalte die Fehlermeldung „maximale Anzahl fehlgeschlagener Versuche“, wenn ich versuche, meine Versuche AWS-Konto telefonisch zu verifizieren

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

1. Melden Sie sich AWS-Konto mit der E-Mail-Adresse und dem Passwort an, die Sie bei der Erstellung Ihres Kontos angegeben haben.
2. Öffnen Sie die Support Konsole und wählen Sie dann Kundenvorgang erstellen aus.
3. Wählen Sie Konto- und Abrechnungssupport.
4. Wählen Sie als Typ die Option Konto aus.
5. Wählen Sie als Kategorie die Option Aktivierung aus.
6. Geben Sie im Abschnitt Fallbeschreibung ein Datum und eine Uhrzeit an, zu der Sie erreichbar sind.
7. Wählen Sie im Abschnitt Kontaktoptionen die Option Chat für Kontaktmethoden aus.
8. Wählen Sie Absenden aus.

Support wird sich mit Ihnen in Verbindung setzen und versuchen, Ihre manuell zu aktivieren AWS-Konto.

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

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

- Beenden Sie den Kontoaktivierungsprozess.

  Wenn Sie das Fenster für den Anmeldevorgang geschlossen haben, bevor Sie alle erforderlichen Informationen hinzugefügt haben, öffnen Sie die Registrierungsseite. Wählen Sie Bei vorhandenem AWS-Konto Konto anmelden und melden Sie sich mit der E-Mail-Adresse und dem Passwort an, die Sie für das Konto ausgewählt haben.
- Überprüfe die mit deiner Zahlungsmethode verknüpften Informationen.

  Überprüfen Sie in der AWS Fakturierung und Kostenmanagement Konsole die Zahlungsmethoden auf Fehler.
- Wenden Sie sich an Ihr Finanzinstitut.

  Manchmal lehnen Finanzinstitute Autorisierungsanfragen von ab AWS. Wenden Sie sich an die Institution, die mit Ihrer Zahlungsmethode verknüpft 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 auf den Kontoauszügen Ihres Finanzinstituts dennoch als geringe Gebühr (normalerweise 1 USD) erscheinen.
- Suchen Sie in Ihrem E-Mail- und Spam-Ordner nach Anfragen nach weiteren Informationen.
- Versuchen Sie es mit einem anderen Browser.
- Kontakt AWS -Support.

  Kontakt AWS -Supportfür Hilfe. Erwähnen Sie alle Schritte zur Fehlerbehebung, die Sie bereits versucht haben.

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