aws

User Guide

AWS IAM Identity Center

AWS IAM Identity Center: User Guide

Table of Contents

Was ist IAM Identity Center?

AWS IAM Identity Center wird AWS-Service für die Verwaltung des Zugriffs menschlicher Benutzer auf AWS Ressourcen empfohlen. Es handelt sich um einen zentralen Ort, an dem Sie Ihren Mitarbeitern Benutzern — auch bekannt als workforce identities konsistenten Zugriff — auf mehrere AWS-Konten Anwendungen zuweisen können. IAM Identity Center wird ohne zusätzliche Kosten angeboten.

Mit IAM Identity Center können Sie Workforce-Benutzer erstellen oder verbinden und deren Zugriff auf all ihre AWS-Konten Anwendungen zentral verwalten. Sie können Berechtigungen für mehrere Konten verwenden, um Ihren Mitarbeitern Zugriff darauf zuzuweisen. AWS-Konten Sie können Anwendungszuweisungen verwenden, um Ihren Benutzern Zugriff auf AWS verwaltete und vom Kunden verwaltete Anwendungen zuzuweisen.

> **Note**
>
> Obwohl der Dienstname AWS Single Sign-On eingestellt wurde, wird in diesem Handbuch immer noch der Begriff Single Sign-On verwendet, um das Authentifizierungsschema zu beschreiben, das es Benutzern ermöglicht, sich gleichzeitig anzumelden, um auf mehrere Anwendungen und Websites zuzugreifen.

Funktionen von IAM Identity Center

IAM Identity Center umfasst die folgenden Kernfunktionen und Funktionen:

Identitäten von Mitarbeitern verwalten

Menschliche Benutzer, die Workloads erstellen oder verwalten, AWS werden auch als Workforce-Benutzer oder Mitarbeiteridentitäten bezeichnet. Workforce-Benutzer sind Mitarbeiter oder Auftragnehmer, auf die Sie AWS-Konten in Ihrem Unternehmen und in internen Geschäftsanwendungen Zugriff gewähren. Bei diesen Personen kann es sich um Entwickler handeln, die Ihre internen und kundenorientierten Systeme entwickeln, oder um Benutzer interner Datenbanksysteme und -anwendungen. Sie können Workforce-Benutzer und -Gruppen in IAM Identity Center erstellen oder eine Verbindung zu einer vorhandenen Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Weitere Informationen finden Sie unter Verwalte deine Identitätsquelle.

Instanzen von IAM Identity Center verwalten

IAM Identity Center unterstützt zwei Arten von Instanzen: Organisationsinstanzen und Kontoinstanzen. Eine Organisationsinstanz ist die bewährte Methode. Es ist die einzige Instanz, mit der Sie den Zugriff auf Anwendungen verwalten können, AWS-Konten und sie wird für alle produktiven Anwendungen empfohlen. Eine Organisationsinstanz wird im AWS Organizations Verwaltungskonto bereitgestellt und bietet Ihnen einen zentralen Punkt, von dem aus Sie den Benutzerzugriff in der gesamten AWS Umgebung verwalten können.

Kontoinstanzen sind an das gebunden, AWS-Konto in dem sie aktiviert sind. Verwenden Sie Kontoinstanzen von IAM Identity Center nur zur Unterstützung isolierter Bereitstellungen ausgewählter AWS verwalteter Anwendungen. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center verwalten.

Verwalten Sie den Zugriff auf mehrere AWS-Konten

Mit Berechtigungen für mehrere Konten können Sie Berechtigungen für mehrere Konten AWS-Konten gleichzeitig planen und zentral implementieren, ohne jedes Ihrer Konten manuell konfigurieren zu müssen. Sie können Berechtigungen auf der Grundlage gängiger Aufgabenfunktionen erstellen oder benutzerdefinierte Berechtigungen definieren, die Ihren Sicherheitsanforderungen entsprechen. Sie können diese Berechtigungen dann Workforce-Benutzern zuweisen, um deren Zugriff auf bestimmte Konten zu kontrollieren.

Diese optionale Funktion ist nur für Organisationsinstanzen verfügbar. Wenn Sie die IAM-Rollenverwaltung pro Konto in Ihrer Umgebung verwenden, können beide Systeme koexistieren. Wenn Sie Berechtigungen für mehrere Konten ausprobieren möchten, können Sie zunächst dieses System auf begrenzter Basis implementieren und im Laufe der Zeit einen größeren Teil Ihrer Umgebung migrieren, um dieses System zu verwenden.

Verwalten Sie den Zugriff auf Anwendungen

Mit IAM Identity Center können Sie die Verwaltung des Anwendungszugriffs vereinfachen. Mit IAM Identity Center können Sie Ihren Mitarbeitern in IAM Identity Center Single Sign-On-Zugriff auf Anwendungen gewähren.

AWS verwaltete Anwendungen

AWS bietet Anwendungen wie Amazon Redshift Amazon Managed Grafana und Amazon Monitron, die in IAM Identity Center integriert sind. Diese Anwendungen können IAM Identity Center für Authentifizierung, Verzeichnisdienste und die Verbreitung vertrauenswürdiger Identitäten verwenden. Ihre Benutzer profitieren von einem konsistenten Single Sign-On-Erlebnis, und da die Anwendungen eine gemeinsame Ansicht von Benutzern, Gruppen und

Gruppenmitgliedschaften haben, haben Benutzer auch ein einheitliches Erlebnis, wenn sie Anwendungsressourcen mit anderen teilen. Sie können AWS verwaltete Anwendungen direkt in den entsprechenden Anwendungskonsolen oder über die APIs so konfigurieren, dass sie mit IAM Identity Center funktionieren.

Vom Kunden verwaltete Anwendungen

Sie können Ihren Mitarbeitern in IAM Identity Center Single Sign-On-Zugriff auf Anwendungen gewähren, die den Identitätsverbund mit SAML 2.0 unterstützen. Viele häufig verwendete SAML 2.0-Anwendungen, wie Salesforce und Microsoft 365, funktionieren mit IAM Identity Center und sind im Anwendungskatalog in der IAM Identity Center-Konsole verfügbar. Dies ist eine optionale Funktion, die hilfreich sein kann, wenn Sie solche Anwendungen verwenden und Ihre Benutzer und Gruppen im IAM Identity Center erstellen oder wenn Sie Microsoft Active Directory Domain Service als Identitätsquelle verwenden.

Vertrauenswürdige Identitätsverteilung zwischen Anwendungen

Trusted Identity Propagation bietet Benutzern von Abfragetools und Business Intelligence (BI) -Anwendungen, die Zugriff auf Daten in Diensten benötigen, ein optimiertes Single Sign-On-Erlebnis. AWS Das Datenzugriffsmanagement basiert auf der Identität eines Benutzers, sodass Administratoren den Zugriff auf der Grundlage der vorhandenen Benutzer- und Gruppenmitgliedschaften gewähren können. Der Benutzerzugriff auf AWS Dienste und andere Ereignisse wird in dienstspezifischen Protokollen und in CloudTrail Ereignissen aufgezeichnet, sodass Prüfer wissen, welche Aktionen die Benutzer ausgeführt haben und auf welche Ressourcen sie zugegriffen haben.

AWS Zugriff auf das Portal für Ihre Benutzer

Das AWS Zugriffsportal ist ein einfaches Webportal, das Ihren Benutzern einen nahtlosen Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen bietet.

IAM Identity Center umbenennen

Am 26. Juli 2022 wurde AWS Single Sign-On in umbenannt. AWS IAM Identity Center Für Bestandskunden sollen in der folgenden Tabelle einige der gängigsten Begriffsänderungen beschrieben werden, die aufgrund der Umbenennung in diesem Handbuch aktualisiert wurden.

Veralteter Begriff	Aktuelle Laufzeit
AWS SSO-Benutzer oder SSO-Benutzer	Workforce-Benutzer oder Benutzer

Veralteter Begriff	Aktuelle Laufzeit
AWS SSO-Benutzerportal oder Benutzerportal	AWS Zugangsportal
AWS SSO-integrierte Anwendungen	AWS verwaltete Anwendungen
AWS SSO-Verzeichnis	Identity-Center-Verzeichnis
AWS SSO-Speicher oder AWS SSO-Identitätsspeicher	Identitätsspeicher, der von IAM Identity Center verwendet wird

In der folgenden Tabelle werden die entsprechenden Namensänderungen für Benutzer, Entwickler und API-Referenzhandbücher beschrieben, die ebenfalls als Folge dieser Umbenennung vorgenommen wurden.

Legacy-Leitfaden	Aktueller Leitfaden
AWS Single Sign-On-Benutzerhandbuch	IAM Identity Center-Benutzerhandbuch
AWS Entwicklerhandbuch zur Single Sign-On-SCIM-Implementierung	Leitfaden für Entwickler zur SCIM-Implementierung von IAM Identity Center
AWS Referenzhandbuch zur Single Sign-On-API	Referenz zur IAM Identity Center API
AWS Referenzhandbuch zur Single Sign-On Identity Store-API	Referenz zur Identity Store-API
AWS Referenzhandbuch zur OIDC-API für Single Sign-On	Referenz zur OIDC-API von IAM Identity Center
AWS Referenzhandbuch zur Single Sign-On-Portal-API	API-Referenz für das IAM Identity Center Portal

Ältere Namespaces bleiben unverändert

Die Namespaces **`sso`** und die **`identitystore`** API-Namespaces sowie die folgenden verwandten Namespaces bleiben aus Gründen der Abwärtskompatibilität unverändert.

- CLI-Befehle
  - `aws configure sso`
  - `identitystore`
  - `sso`
  - `sso-admin`
  - `sso-oidc`
- Verwaltete Richtlinien, die Präfixe `AWSSSO` und `AWSIdentitySync` Präfixe enthalten
- Dienstendpunkte, die und enthalten `sso` `identitystore`
- AWS CloudFormationRessourcen, die Präfixe enthalten `AWS::SSO`
- Mit dem Dienst verknüpfte Rolle, die enthält `AWSServiceRoleForSSO`
- Konsolen-URLs, die und enthalten `sso` `singlesignon`
- Dokumentations-URLs, die Folgendes enthalten `singlesignon`

Aktivieren AWS IAM Identity Center

Gehen Sie wie folgt vor, um sich bei IAM Identity Center anzumelden AWS Management Console und eine Organisationsinstanz zu aktivieren.

1. Führen Sie einen der folgenden Schritte aus, um sich bei der AWS Management Console anzumelden.
   - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
   - Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
2. Öffnen Sie die IAM Identity Center-Konsole.
3. Wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren mit. AWS Organizations
4. Optional Fügen Sie Tags hinzu, die Sie dieser Organisationsinstanz zuordnen möchten.
5. Optional: Konfigurieren Sie die delegierte Administration.

> **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 benötigen. AWS Organizations Weitere Informationen finden Sie unter Delegierte Verwaltung.

> **Important**
>
> Die Möglichkeit, Kontoinstanzen von IAM Identity Center zu erstellen, ist standardmäßig aktiviert. Kontoinstanzen von IAM Identity Center umfassen eine Teilmenge der Funktionen, die einer Organisationsinstanz zur Verfügung stehen. Sie können mithilfe einer Service Control-Richtlinie steuern, ob Benutzer auf diese Funktion zugreifen können.

Müssen Sie Firewalls und Gateways aktualisieren?

Wenn Sie den Zugriff auf bestimmte AWS Domänen oder URL-Endpunkte mithilfe einer Lösung zur Filterung von Webinhalten wie Firewalls der nächsten Generation (NGFW) oder Secure Web Gateways (SWG) filtern, müssen Sie die folgenden Domänen oder URL-Endpunkte zu Ihren Zulassungslisten für Web-Content-Filterlösungen hinzufügen. Auf diese Weise können Sie auf Ihr Zugriffsportal zugreifen. AWS

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Überlegungen zur Zulassung von Domains und URL-Endpunkten

Machen Sie sich mit den Auswirkungen der Zulassung von Domains außerhalb des Zugangsportals vertraut AWS .

- Um von Ihrem AWS-Konten Zugriffsportal aus auf die und die IAM Identity Center-Konsole AWS zugreifen zu können, müssen Sie zusätzliche Domains zulassen. AWS Management Console Eine Liste der Domänen finden Sie im Handbuch AWS Management Console Erste Schritte unter Problembehandlung. AWS Management Console
- Um von Ihrem Zugriffsportal aus auf AWS verwaltete Anwendungen AWS zuzugreifen, müssen Sie die entsprechenden Domänen zulassen. Weitere Informationen finden Sie in der jeweiligen Servicedokumentation.

- Diese Zulassungslisten decken AWS Dienste ab. Wenn Sie externe Software verwenden, z. B. externe Software IdPs (z. B. Okta undMicrosoft Entra ID), müssen Sie deren Domänen in Ihre Zulassungslisten aufnehmen.

Sie sind jetzt bereit, IAM Identity Center zu konfigurieren. Wenn Sie IAM Identity Center aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Dies ist der schnellste Weg, um mit der Nutzung von IAM Identity Center zu beginnen. Anweisungen finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren.

Wenn Sie mehr darüber erfahren möchten, wie IAM Identity Center mit Organizations, Identitätsquellen und IAM-Rollen zusammenarbeitet, lesen Sie die folgenden Themen.

Themen

Voraussetzungen und Überlegungen

Die folgenden Themen enthalten Informationen zu den Voraussetzungen und anderen Überlegungen zur Einrichtung von IAM Identity Center.

Überlegungen zur Auswahl eines AWS-Region

Sie können eine IAM Identity Center-Instanz in einer einzigen, unterstützten Instanz AWS-Region Ihrer Wahl aktivieren. Die Auswahl einer Region erfordert eine Bewertung Ihrer Prioritäten auf der Grundlage Ihrer Anwendungsfälle und Unternehmensrichtlinien. Der Zugriff auf AWS-Konten und die Cloud-Anwendungen von Ihrem IAM Identity Center aus hängen nicht von dieser Wahl ab. Der Zugriff auf AWS verwaltete Anwendungen und die Möglichkeit, sie AWS Managed Microsoft AD als Identitätsquelle zu verwenden, können jedoch von dieser Wahl abhängen. Eine Liste der Regionen, die AWS IAM Identity Center unterstützt, finden Sie unter IAM Identity Center-Endpunkte und Kontingente. Allgemeine AWS-Referenz

Wichtige Überlegungen zur Auswahl eines. AWS-Region

- Geografischer Standort — Wenn Sie eine Region auswählen, die der Mehrheit Ihrer Endbenutzer geografisch am nächsten liegt, haben diese eine geringere Latenz beim Zugriff auf das AWS Zugriffsportal und AWS verwaltete Anwendungen wie Amazon SageMaker Studio.

- Verfügbarkeit AWS verwalteter Anwendungen — AWS verwaltete Anwendungen wie Amazon SageMaker können nur in den von AWS-Regionen ihnen unterstützten Anwendungen ausgeführt werden. Aktivieren Sie IAM Identity Center in einer Region, die von den AWS verwalteten Anwendungen unterstützt wird, die Sie damit verwenden möchten. Viele AWS verwaltete Anwendungen können auch nur in derselben Region ausgeführt werden, in der Sie IAM Identity Center aktiviert haben.
- Digitale Souveränität — Vorschriften zur digitalen Souveränität oder Unternehmensrichtlinien können den Einsatz bestimmter AWS-Region Technologien vorschreiben. Wenden Sie sich an die Rechtsabteilung Ihres Unternehmens.
- Identitätsquelle — Wenn Sie AD Connector als Identitätsquelle verwenden AWS Managed Microsoft AD , muss die Heimatregion mit der Region übereinstimmen, AWS-Region in der Sie IAM Identity Center aktiviert haben.
- Regionen standardmäßig deaktiviert — AWS ursprünglich waren alle neu AWS-Regionen für die Verwendung in AWS-Konten standardmäßig aktiviert, sodass Ihre Benutzer automatisch Ressourcen in jeder Region erstellen konnten. Wenn jetzt eine neue Region AWS hinzugefügt wird, ist deren Verwendung standardmäßig in allen Konten deaktiviert. Wenn Sie IAM Identity Center in einer Region bereitstellen, die standardmäßig deaktiviert ist, müssen Sie diese Region in allen Konten aktivieren, für die Sie den Zugriff auf IAM Identity Center verwalten möchten. Dies ist auch dann erforderlich, wenn Sie in diesen Konten keine Ressourcen in dieser Region erstellen möchten.

  Sie können eine Region für die aktuellen Konten in Ihrer Organisation aktivieren und müssen diese Aktion für neue Konten wiederholen, die Sie möglicherweise später hinzufügen. Anweisungen finden Sie im AWS Organizations Benutzerhandbuch unter Aktivieren oder Deaktivieren einer Region in Ihrer Organisation. Um diese zusätzlichen Schritte nicht wiederholen zu müssen, können Sie Ihr IAM Identity Center in einer Region bereitstellen, die standardmäßig aktiviert ist. Zu Referenzzwecken sind die folgenden Regionen standardmäßig aktiviert:

  - US East (Ohio)
  - USA Ost (Nord-Virginia)
  - USA West (Oregon)
  - USA West (Nordkalifornien)
  - Europe (Paris)
  - Südamerika (São Paulo)
  - Asien-Pazifik (Mumbai)
  - Europa (Stockholm)

- Asia Pacific (Seoul)
- Asien-Pazifik (Tokio)
- Europa (Irland)
- Europa (Frankfurt)
- Europa (London)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Kanada (Zentral)
- Asien-Pazifik (Osaka)

- Regionsübergreifende Anrufe — In einigen Regionen ruft IAM Identity Center möglicherweise Amazon Simple Email Service in einer anderen Region an, um E-Mails zu senden. Bei diesen regionsübergreifenden Anrufen sendet IAM Identity Center bestimmte Benutzerattribute an die andere Region. Weitere Informationen zu Regionen finden Sie unter AWS IAM Identity Center Verfügbarkeit in der Region.

Umschalten AWS-Regionen

Sie können Ihre IAM Identity Center-Region nur wechseln, indem Sie die aktuelle Instance löschen und eine neue Instance in einer anderen Region erstellen. Wenn Sie bereits eine AWS verwaltete Anwendung mit Ihrer vorhandenen Instanz aktiviert haben, sollten Sie sie zuerst löschen, bevor Sie Ihr IAM Identity Center löschen. Sie müssen Benutzer, Gruppen, Berechtigungssätze, Anwendungen und Zuweisungen in der neuen Instanz neu erstellen. Sie können die IAM Identity Center-APIs für Konten und Anwendungszuweisungen verwenden, um einen Snapshot Ihrer Konfiguration zu erhalten und diesen Snapshot dann verwenden, um Ihre Konfiguration in einer neuen Region neu aufzubauen. Möglicherweise müssen Sie auch einige IAM Identity Center-Konfigurationen über die Management Console Ihrer neuen Instanz neu erstellen. Anweisungen zum Löschen von IAM Identity Center finden Sie unter. Löschen Sie Ihre IAM Identity Center-Konfiguration

Kontingent für von IAM Identity Center erstellte IAM-Rollen

IAM Identity Center erstellt IAM-Rollen, um Benutzern Berechtigungen für Ressourcen zu erteilen. Wenn Sie einen Berechtigungssatz zuweisen, erstellt IAM Identity Center in jedem Konto die entsprechenden, vom IAM Identity Center kontrollierten IAM-Rollen und fügt diesen Rollen die im Berechtigungssatz angegebenen Richtlinien zu. IAM Identity Center verwaltet die Rolle und ermöglicht es den von Ihnen definierten autorisierten Benutzern, die Rolle über das Zugriffsportal

oder zu übernehmen. AWS AWS CLI Wenn Sie den Berechtigungssatz ändern, stellt IAM Identity Center sicher, dass die entsprechenden IAM-Richtlinien und -Rollen entsprechend aktualisiert werden.

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. Das Standardkontingent für IAM-Rollen pro Konto beträgt 1000 Rollen. 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 User Guide.

> **Note**
>
> Wenn Sie die IAM-Rollen in einem Konto überprüfen, das bereits IAM Identity Center verwendet, fallen Ihnen möglicherweise Rollennamen auf, die mit beginnen. “AWSReservedSSO_” Dies sind die Rollen, die der IAM Identity Center-Dienst für das Konto erstellt hat. Sie stammen aus der Zuweisung eines Berechtigungssatzes für das Konto.

IAM Identity Center und AWS Organizations

AWS Organizations wird für die Verwendung mit IAM Identity Center empfohlen, ist aber nicht erforderlich. Wenn Sie noch keine Organisation eingerichtet haben, müssen Sie das auch nicht tun. Wenn Sie IAM Identity Center aktivieren, wählen Sie aus, ob Sie den Dienst mit AWS Organizations aktivieren möchten. Wenn Sie eine Organisation einrichten, wird die Organisation, AWS-Konto die die Organisation einrichtet, zum Verwaltungskonto der Organisation. Der Root-Benutzer von AWS-Konto ist jetzt der Besitzer des Organisationsverwaltungskontos. Alle weiteren Konten, die AWS-Konten Sie zu Ihrer Organisation einladen, sind Mitgliedskonten. Das Verwaltungskonto erstellt die Ressourcen, Organisationseinheiten und Richtlinien der Organisation, mit denen die Mitgliedskonten verwaltet werden. Berechtigungen werden vom Verwaltungskonto an Mitgliedskonten delegiert.

> **Note**
>
> Wir empfehlen, dass Sie IAM Identity Center mit aktivieren AWS Organizations, wodurch eine Organisationsinstanz von IAM Identity Center erstellt wird. Eine Organisationsinstanz

ist unsere empfohlene bewährte Methode, da sie alle Funktionen von IAM Identity Center unterstützt und zentrale Verwaltungsfunktionen bietet. Weitere Informationen finden Sie unter Organisations- und Kontoinstanzen von IAM Identity Center verwalten.

Wenn Sie IAM Identity Center bereits eingerichtet haben AWS Organizations und es Ihrer Organisation hinzufügen möchten, stellen Sie sicher, dass alle AWS Organizations Funktionen aktiviert sind. Wenn Sie eine Organisation erstellen, werden standardmäßig alle Funktionen aktiviert. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.

Um IAM Identity Center zu aktivieren, müssen Sie sich beim anmelden, AWS Management Console indem Sie sich mit Ihrem AWS Organizations Verwaltungskonto als Benutzer mit Administratoranmeldedaten oder als Root-Benutzer anmelden (nicht empfohlen, es sei denn, es gibt keine anderen Administratorbenutzer). Sie können IAM Identity Center nicht aktivieren, während Sie mit Administratoranmeldedaten von einem AWS Organizations Mitgliedskonto aus angemeldet sind. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter AWS Organisation erstellen und verwalten.

Bestätigen Sie Ihre Identitätsquellen im IAM Identity Center

Ihre Identitätsquelle in IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Nachdem Sie IAM Identity Center aktiviert haben, stellen Sie sicher, dass Sie die Identitätsquelle Ihrer Wahl verwenden.

Bestätigen Sie Ihre Identitätsquelle

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie auf der Dashboard-Seite unter dem Abschnitt Empfohlene Einrichtungsschritte die Option Bestätigen Sie Ihre Identitätsquelle aus. Sie können diese Seite auch aufrufen, indem Sie Einstellungen und dann den Tab Identitätsquelle auswählen.
3. Es gibt keine Aktion, wenn Sie Ihre zugewiesene Identitätsquelle behalten möchten. Wenn Sie es vorziehen, sie zu ändern, wählen Sie Aktionen und dann Identitätsquelle ändern aus.

   Sie können eine der folgenden Optionen als Identitätsquelle wählen:

Identity-Center-Verzeichnis

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Wenn Sie noch keinen anderen externen Identitätsanbieter verwenden, können Sie damit beginnen, Ihre Benutzer und Gruppen zu erstellen und deren Zugriffsebene Ihren Anwendungen AWS-Konten und Anwendungen zuzuweisen. Ein Tutorial zur Verwendung dieser Identitätsquelle finden Sie unterBenutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren.

Active Directory

Wenn Sie bereits Benutzer und Gruppen in Ihrem AWS Managed Microsoft AD Verzeichnis verwalten, indem Sie AWS Directory Service oder Ihr selbstverwaltetes Verzeichnis in verwenden, empfehlen wirActive Directory (AD), dass Sie dieses Verzeichnis verbinden, wenn Sie IAM Identity Center aktivieren. Erstellen Sie keine Benutzer und Gruppen im standardmäßigen Identity Center-Verzeichnis. IAM Identity Center verwendet die von der bereitgestellte Verbindung, AWS Directory Service um Benutzer-, Gruppen- und Mitgliedschaftsinformationen aus Ihrem Quellverzeichnis in Active Directory mit dem IAM Identity Center-Identitätsspeicher zu synchronisieren. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis.

> **Note**
>
> IAM Identity Center unterstützt SAMBA4-basiertes Simple AD nicht als Identitätsquelle.

Externer Identitätsanbieter

Für externe Identitätsanbieter (IdPs) wie Okta oder können Sie IAM Identity Center verwendenMicrosoft Entra ID, um Identitäten IdPs anhand des Security Assertion Markup Language (SAML) 2.0-Standards zu authentifizieren. Das SAML-Protokoll bietet keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Sie machen IAM Identity Center auf diese Benutzer und Gruppen aufmerksam, indem Sie sie in IAM Identity Center bereitstellen. Sie können die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen von Ihrem IdP in IAM Identity Center mithilfe des SCIM-Protokolls (System for Cross-Domain Identity Management) v2.0

durchführen, wenn Ihr IdP SCIM unterstützt. Andernfalls können Sie Ihre Benutzer und Gruppen manuell bereitstellen, indem Sie die Benutzernamen, die E-Mail-Adresse und die Gruppen manuell in IAM Identity Center eingeben.

Eine ausführliche Anleitung zur Einrichtung Ihrer Identitätsquelle finden Sie unterErste Schritte mit Tutorials.

> **Note**
>
> Wenn Sie planen, einen externen Identitätsanbieter zu verwenden, beachten Sie, dass der externe IdP und nicht IAM Identity Center die Einstellungen für die Multi-Faktor-Authentifizierung (MFA) verwaltet. MFA in IAM Identity Center wird für die Verwendung durch externe Benutzer nicht unterstützt. IdPs Weitere Informationen finden Sie unter Benutzer zur MFA auffordern.

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 bestätigt oder geändert 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 in IAM Identity Center 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 Anwendungen. AWS-Konten Weitere Informationen finden Sie unter Überlegungen zum Ändern Ihrer Identitätsquelle.

Nachdem Sie Ihre Identitätsquelle konfiguriert haben, können Sie nach Benutzern oder Gruppen suchen, um ihnen Single Sign-On-Zugriff auf Cloud-Anwendungen oder beides zu AWS-Konten gewähren.

Erste Schritte mit Tutorials

Sie können eine Identitätsquelle pro Organisation haben. Daher ist es wichtig, sich die Zeit zu nehmen, um die Funktionen zu testen, die jeder von ihnen hat.

In diesem Abschnitt können Sie eines der folgenden Tutorials auswählen, um IAM Identity Center mit Ihrer bevorzugten Identitätsquelle einzurichten, einen Administratorbenutzer zu erstellen und Berechtigungssätze zu konfigurieren, um Ihren Benutzern Zugriff auf -Ressourcen zu gewähren.

Bevor Sie mit einem dieser Tutorials beginnen, aktivieren Sie IAM Identity Center. Weitere Informationen finden Sie unter Aktivieren AWS IAM Identity Center.

Themen

- Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren
- Verwenden von Active Directory als Identitätsquelle
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Konfiguration von SAML und SCIM mit einem IAM Google Workspace Identity Center
- Verwenden von IAM Identity Center zum Herstellen einer Verbindung mit Ihrer -JumpCloudVerzeichnisplattform
- Konfiguration von SAML und SCIM mit einem IAM Microsoft Entra ID Identity Center
- Konfiguration von SAML und SCIM mit einem IAM Okta Identity Center
- Einrichten der SCIM-Bereitstellung zwischen OneLogin und IAM Identity Center
- Verwenden von -Ping IdentityProdukten mit IAM Identity Center

Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert, sodass Sie keine Identitätsquelle auswählen müssen. Wenn Ihr Unternehmen einen anderen Identitätsanbieter wie AWS Directory Service for Microsoft Active Directory, verwendet, oder Okta erwägen SieMicrosoft Entra ID, diese Identitätsquelle in IAM Identity Center zu integrieren, anstatt die Standardkonfiguration zu verwenden.

Zielsetzung

In diesem Tutorial verwenden Sie das Standardverzeichnis als Identitätsquelle und richten den Benutzerzugriff ein und testen ihn. In diesem Szenario verwalten Sie alle Benutzer und Gruppen in IAM Identity Center. Benutzer melden sich über das AWS Zugriffsportal an. Dieses Tutorial richtet sich an Benutzer, die IAM noch nicht AWS kennen oder bereits verwendet haben, um Benutzer und Gruppen zu verwalten. In den nächsten Schritten werden Sie Folgendes erstellen:

- Ein Administratorbenutzer namens *Nikki Wolf*
- Eine Gruppe namens *Admin team*
- Ein Berechtigungssatz mit dem Namen *AdminAccess*

Um zu überprüfen, ob alles korrekt erstellt wurde, melden Sie sich an und legen das Passwort des Administratorbenutzers fest. Nach Abschluss dieses Tutorials können Sie den Administratorbenutzer verwenden, um weitere Benutzer in IAM Identity Center hinzuzufügen, zusätzliche Berechtigungssätze zu erstellen und den organisatorischen Zugriff auf Anwendungen einzurichten.

Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter. Aktivieren AWS IAM Identity Center

Bevor Sie beginnen:

Gehen Sie wie folgt vor, um sich bei der AWS Management Console anzumelden.

- Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie AWS-Konto Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
- Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.

Öffnen Sie die IAM Identity Center-Konsole.

Schritt 1: Fügen Sie einen Benutzer hinzu

1. Wählen Sie im Navigationsbereich von IAM Identity Center Benutzer und anschließend Benutzer hinzufügen aus.
2. Geben Sie auf der Seite „Benutzerdetails angeben“ die folgenden Informationen ein:
   - Nutzername — Geben Sie für dieses Tutorial *nikkiw* ein.

Wählen Sie beim Erstellen von Benutzern Benutzernamen, die leicht zu merken sind. Ihre Benutzer müssen sich den Benutzernamen merken, um sich im AWS Access Portal anmelden zu können. Sie können ihn später nicht ändern.

- Passwort — Wählen Sie Diesem Benutzer eine E-Mail mit Anweisungen zur Einrichtung des Passworts senden (empfohlen).

  Diese Option sendet dem Benutzer eine von Amazon Web Services adressierte E-Mail mit der Betreffzeile Invitation to join IAM Identity Center (Nachfolger von AWS Single Sign-On). Die E-Mail stammt entweder von oder`no-reply@signin.aws`. `no-reply@login.awsapps.com` Fügen Sie diese E-Mail-Adressen zu Ihrer Liste der zugelassenen Absender hinzu.
- E-Mail-Adresse — Geben Sie eine E-Mail-Adresse für den Benutzer ein, an den Sie die E-Mail erhalten können. Geben Sie sie dann erneut ein, um sie zu bestätigen. Jeder Benutzer muss eine eindeutige E-Mail-Adresse haben.
- Vorname — Geben Sie den Vornamen für den Benutzer ein. Geben Sie für dieses Tutorial *`Nikki`* ein.
- Nachname — Geben Sie den Nachnamen des Benutzers ein. Geben Sie für dieses Tutorial *`Wolf`* ein.
- Anzeigename — Der Standardwert ist der Vor- und Nachname des Benutzers. Wenn Sie den Anzeigenamen ändern möchten, können Sie einen anderen Namen eingeben. Der Anzeigename ist im Anmeldeportal und in der Benutzerliste sichtbar.
- Füllen Sie bei Bedarf die optionalen Informationen aus. Es wird in diesem Tutorial nicht verwendet und kann später geändert werden.

3. Wählen Sie Weiter aus. Die Seite „Benutzer zu Gruppen hinzufügen“ wird angezeigt. Wir werden eine Gruppe erstellen, der wir Administratorrechte zuweisen können, anstatt sie direkt *`Nikki`* zu geben.

   Wähle Gruppe erstellen

   Ein neuer Browser-Tab wird geöffnet, auf dem die Seite Gruppe erstellen angezeigt wird.

   a. Geben Sie unter Gruppendetails im Feld Gruppenname einen Namen für die Gruppe ein. Wir empfehlen einen Gruppennamen, der die Rolle der Gruppe identifiziert. Geben Sie für dieses Tutorial *`Admin team`* ein.

   b. Wählen Sie Gruppe erstellen

c. Schließen Sie den Browser-Tab „Gruppen“, um zum Browser-Tab „Benutzer hinzufügen“ zurückzukehren

4. Wählen Sie im Bereich Gruppen die Schaltfläche Aktualisieren aus. Die Gruppe *Admin-Team* wird in der Liste angezeigt.

   Aktivieren Sie das Kontrollkästchen neben *Admin-Team* und wählen Sie dann Weiter aus.

5. Bestätigen Sie auf der Seite Benutzer überprüfen und hinzufügen Folgendes:

   - Die primären Informationen werden so angezeigt, wie Sie es beabsichtigt haben
   - Unter Gruppen wird der Benutzer angezeigt, der zu der von Ihnen erstellten Gruppe hinzugefügt wurde

   Wenn Sie Änderungen vornehmen möchten, wählen Sie Bearbeiten. Wenn alle Angaben korrekt sind, wählen Sie Benutzer hinzufügen.

   Eine Benachrichtigung informiert Sie darüber, dass der Benutzer hinzugefügt wurde.

Als Nächstes fügst du Administratorberechtigungen für die *Admin-Teamgruppe* hinzu, sodass *Nikki* Zugriff auf Ressourcen hat.

Schritt 2: Fügen Sie Administratorberechtigungen hinzu

1. Wählen Sie im Navigationsbereich von IAM Identity Center unter Berechtigungen für mehrere Konten die Option. AWS-Konten
2. Auf der AWS-KontenSeite „Organisationsstruktur“ wird Ihre Organisation mit Ihren Konten darunter in der Hierarchie angezeigt. Aktivieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:

   a. Für Schritt 1: Benutzer und Gruppen auswählen wählen Sie die *Admin-Teamgruppe* aus, die Sie erstellt haben. Wählen Sie anschließend Weiter.

   b. Für Schritt 2: Berechtigungssätze auswählen Wählen Sie Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Teilschritte führt, die zur Erstellung eines Berechtigungssatzes erforderlich sind.

      i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:

- Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
- Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

Wählen Sie Weiter aus.

ii. Für Schritt 2: Geben Sie die Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter aus.

Mit den Standardeinstellungen wird ein Berechtigungssatz *AdministratorAccess*mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist. Sie können den Namen des Berechtigungssatzes ändern, indem Sie einen neuen Namen in das Feld Name des Berechtigungssatzes eingeben.

iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ des Berechtigungssatzes die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen. Auf der Seite Berechtigungssätze wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diese Registerkarte jetzt in Ihrem Webbrowser schließen.

Auf der Browser-Registerkarte „Benutzer und Gruppen zuweisen“ befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *AdministratorAccess*Berechtigungssatz wird in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter.

c. Vergewissern Sie sich auf der Seite Schritt 3: Aufgaben überprüfen und einreichen, dass die Gruppe *Admin-Team* und der *AdministratorAccess*Berechtigungssatz ausgewählt sind, und klicken Sie dann auf Absenden.

Die Seite wird mit der Meldung aktualisiert, dass Ihr gerade konfiguriert AWS-Konto wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. In einer Benachrichtigung werden Sie darüber informiert, dass Ihr AWS-Konto Konto erneut bereitgestellt und der aktualisierte Berechtigungssatz angewendet wurde.

> **Herzlichen Glückwunsch!**
>
> Sie haben Ihren ersten Benutzer, Ihre erste Gruppe und Ihren ersten Berechtigungssatz erfolgreich eingerichtet.

Im nächsten Teil dieses Tutorials testest du *Nikkis* Zugriff, indem du dich mit ihren Administratordaten beim AWS Zugangsportal anmeldest und ihr Passwort festlegst. Melden Sie sich jetzt von der Konsole ab.

Schritt 3: Testen des Benutzerzugriffs

Da *Nikki Wolf* nun ein Benutzer in Ihrer Organisation ist, kann sie sich anmelden und auf die Ressourcen zugreifen, für die sie gemäß ihrem Berechtigungssatz berechtigt sind. Um zu überprüfen, ob der Benutzer korrekt konfiguriert ist, verwenden Sie im nächsten Schritt die Anmeldeinformationen *von Nikki*, um sich anzumelden und sein Passwort einzurichten. Als du den Benutzer *Nikki Wolf* in Schritt 1 hinzugefügt hast, hast du ausgewählt, dass *Nikki* eine E-Mail mit Anweisungen zur Einrichtung des Passworts erhält. Es ist an der Zeit, diese E-Mail zu öffnen und wie folgt vorzugehen:

1. Wählen Sie in der E-Mail den Link Einladung annehmen aus, um die Einladung anzunehmen.

   > **Note**
   >
   > Die E-Mail enthält auch *Nikkis* Benutzernamen und die URL des AWS Zugriffsportals, mit der sie sich bei der Organisation anmelden werden. Notieren Sie sich diese Informationen für future Verwendung.

   Sie werden zur Anmeldeseite für neue Benutzer weitergeleitet, auf der Sie das Passwort *von Nikki* festlegen können.
2. Nachdem du *das Passwort von Nikki* festgelegt hast, wirst du zur Anmeldeseite weitergeleitet. Gib ***nikkiw*** ein und wähle Weiter. Gib dann ***Nikkis*** Passwort ein und wähle Anmelden.
3. Das AWS Zugangsportal wird geöffnet und zeigt die Organisation und die Anwendungen an, auf die Sie zugreifen können.

Wählen Sie die Organisation aus, um sie zu einer Liste zu erweitern, und wählen Sie AWS-Konten dann das Konto aus, um die Rollen anzuzeigen, mit denen Sie auf Ressourcen im Konto zugreifen können.

Jeder Berechtigungssatz verfügt über zwei Verwaltungsmethoden, die Sie verwenden können, entweder Rollen - oder Zugriffstasten.

- Rolle, zum Beispiel *`AdministratorAccess`*— Öffnet die AWS Console Home.
- Zugriffstasten — Stellt Anmeldeinformationen bereit, die Sie mit dem AWS CLI oder und dem AWS SDK verwenden können. Enthält Informationen zur Verwendung von kurzfristigen Anmeldeinformationen, die automatisch aktualisiert werden, oder kurzfristigen Zugriffsschlüsseln. Weitere Informationen finden Sie unter Abrufen der IAM Identity Center-Benutzeranmeldedaten für die AWS CLI oder SDKs AWS.

4. Wählen Sie den Link Rolle, um sich bei der anzumelden AWS Console Home.

Sie sind angemeldet und haben die AWS Console Home Seite aufgerufen. Erkunden Sie die Konsole und vergewissern Sie sich, dass Sie den erwarteten Zugriff haben.

Nächste Schritte

Nachdem Sie nun einen Administratorbenutzer in IAM Identity Center erstellt haben, können Sie:

- Anwendungen zuweisen
- Fügen Sie weitere Benutzer hinzu
- Weisen Sie Benutzer Konten zu
- Konfigurieren Sie zusätzliche Berechtigungssätze

> **Note**
>
> Sie können demselben Benutzer mehrere Berechtigungssätze zuweisen. Um der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten zu folgen, erstellen Sie nach der Erstellung Ihres Administratorbenutzers einen restriktiveren Berechtigungssatz und weisen Sie ihn demselben Benutzer zu. Auf diese Weise können Sie nur AWS-Konto mit den Berechtigungen auf Ihre zugreifen, die Sie benötigen, und nicht mit Administratorberechtigungen.

Nachdem Ihre Benutzer ihre Einladung zur Aktivierung ihres Kontos angenommen und sich beim AWS Access-Portal angemeldet haben, werden im Portal nur noch Elemente für die AWS-Konten Rollen und Anwendungen angezeigt, denen sie zugewiesen sind.

> **Important**
>
> Wir empfehlen dringend, die Multi-Faktor-Authentifizierung (MFA) für Ihre Benutzer zu aktivieren. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung für Identity Center-Benutzer.

Verwenden von Active Directory als Identitätsquelle

Wenn Sie Benutzer in Ihrem AWS Managed Microsoft AD Verzeichnis mithilfe von Active Directory (AD) AWS Directory Service oder Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) verwalten, können Sie Ihre IAM Identity Center-Identitätsquelle so ändern, dass sie mit diesen Benutzern funktioniert. Wir empfehlen 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.

Um Active Directory als Identitätsquelle verwenden zu können, muss Ihre Konfiguration die folgenden Voraussetzungen erfüllen:

- Wenn Sie IAM Identity Center verwendenAWS Managed Microsoft AD, müssen Sie es dort aktivierenAWS-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 im Verwaltungskonto befindet:

  Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis eingerichtet habenAWS Directory Service, und es muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können jeweils nur ein AD Connector Connector-Verzeichnis oder ein Verzeichnis verbinden. AWS Managed Microsoft AD Wenn Sie mehrere Domänen oder

Gesamtstrukturen unterstützen müssen, verwenden SieAWS Managed Microsoft AD. Weitere Informationen finden Sie hier:

- Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center
- Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center

- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

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

  Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle 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.

Dieses Tutorial führt Sie durch die grundlegenden Einstellungen für die Verwendung von Active Directory als IAM Identity Center-Identitätsquelle.

Schritt 1: Active Directory Connect und einen Benutzer angeben

Wenn Sie Active Directory bereits verwenden, helfen Ihnen die folgenden Themen bei der Vorbereitung der Verbindung Ihres Verzeichnisses mit IAM Identity Center.

> **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 verwendenAWS Directory Service, aktivieren Sie MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitung unter. Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis
2. Führen Sie die Schritte unter Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center aus.

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 unterHerstellen einer Verbindung mit einem Microsoft AD Verzeichnis.
2. Führen Sie die Schritte unter Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center aus.
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.

Schritt 2: 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 Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“, dann „Aktionen“ und anschließend „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. Weitere Informationen finden Sie unter Berechtigungssatz erstellen.

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisierung) von Benutzerinformationen von CyberArk Directory Platform in IAM Identity Center. Diese Bereitstellung verwendet das System for Cross-Domain Identity Management (SCIM) v2.0-Protokoll. Sie konfigurieren diese Verbindung in CyberArk mit Ihrem IAM-Identity-Center-SCIM-Endpunkt und Zugriffstoken. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute in CyberArk zu den benannten Attributen in IAM Identity Center. Dies führt dazu, dass die erwarteten Attribute zwischen IAM Identity Center und übereinstimmenCyberArk.

Dieses Handbuch basiert auf CyberArk dem Stand August 2021. Die Schritte für neuere Versionen können variieren. Dieses Handbuch enthält einige Hinweise zur Konfiguration der Benutzerauthentifizierung über SAML.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu überprüfenÜberlegungen zur Verwendung der automatischen Bereitstellung. Lesen Sie dann weitere Überlegungen im nächsten Abschnitt.

Themen

- Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center
- Schritt 2: Konfigurieren der Bereitstellung in CyberArk
- (Optional) Schritt 3: Konfigurieren von Benutzerattributen in CyberArk für die Zugriffskontrolle (ABAC) in IAM Identity Center
- (Optional) Übergeben von Attributen für die Zugriffskontrolle

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- CyberArk -Abonnement oder kostenlose Testversion. Um sich für eine kostenlose Testversion anzumelden, besuchen Sie CyberArk.
- Ein IAM-Identity-Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Eine SAML-Verbindung von Ihrem CyberArk Konto zu IAM Identity Center, wie in der CyberArk Dokumentation für IAM Identity Center beschrieben.
- Ordnen Sie den IAM-Identity-Center-Konnektor den Rollen, Benutzern und Organisationen zu, denen Sie den Zugriff auf erlauben möchten AWS-Konten.

Überlegungen zu SCIM

Bei der Verwendung des CyberArk Verbunds für IAM Identity Center sind folgende Überlegungen zu beachten:

- Nur Rollen, die im Abschnitt Bereitstellung der Anwendung zugeordnet sind, werden mit IAM Identity Center synchronisiert.
- Das Bereitstellungsskript wird nur im Standardstatus unterstützt, sobald die SCIM-Bereitstellung geändert wurde, schlägt die SCIM-Bereitstellung möglicherweise fehl.
  - Es kann nur ein Telefonnummernattribut synchronisiert werden und der Standardwert ist „Workphone“.
- Wenn die Rollenzuordnung in der CyberArk IAM-Identity-Center-Anwendung geändert wird, wird das folgende Verhalten erwartet:
  - Wenn die Rollennamen geändert werden – keine Änderungen an den Gruppennamen im IAM Identity Center.

  - Wenn die Gruppennamen geändert werden – neue Gruppen werden im IAM Identity Center erstellt, alte Gruppen bleiben erhalten, haben jedoch keine Mitglieder.
- Das Benutzersynchronisierungs- und Bereitstellungsverhalten kann über die CyberArk IAM-Identity-Center-Anwendung eingerichtet werden. Stellen Sie sicher, dass Sie das richtige Verhalten für Ihre Organisation einrichten. Dies sind die Optionen, die Sie haben:
  - Überschreiben (oder nicht) Sie Benutzer im Identity-Center-Verzeichnis mit demselben Prinzipalnamen.
  - Heben Sie die Bereitstellung von Benutzern aus dem IAM Identity Center auf, wenn der Benutzer aus der CyberArk Rolle entfernt wird.
  - Benutzerverhalten aufheben – deaktivieren oder löschen.

Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM-Identity-Center-Konsole, um die automatische Bereitstellung zu aktivieren.

So aktivieren Sie die automatische Bereitstellung in IAM Identity Center

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Feld Informationen zur automatischen Bereitstellung und wählen Sie dann Aktivieren aus. Dies aktiviert sofort die automatische Bereitstellung im IAM Identity Center und zeigt die erforderlichen SCIM-Endpunkt- und Zugriffstokeninformationen an.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehenden Datenverkehr jeden der Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
   a. SCIM-Endpunkt
   b. Zugriffstoken
5. Klicken Sie auf Schließen.

Nachdem Sie nun die Bereitstellung in der IAM-Identity-Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mit der CyberArk IAM-Identity-Center-Anwendung abschließen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren der Bereitstellung in CyberArk

Gehen Sie wie folgt in der CyberArk IAM-Identity-Center-Anwendung vor, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die CyberArk IAM-Identity-Center-Anwendung bereits zu Ihrer CyberArk Administratorkonsole unter Web Apps hinzugefügt haben. Wenn Sie dies noch nicht getan haben, lesen Sie die und führen Sie dann dieses Verfahren ausVoraussetzungen, um die SCIM-Bereitstellung zu konfigurieren.

So konfigurieren Sie die Bereitstellung in CyberArk

1. Öffnen Sie die CyberArk IAM-Identity-Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für hinzugefügt haben CyberArk (Apps > Web-App). Siehe Voraussetzungen.
2. Wählen Sie die IAM-Identity-Center-Anwendung aus und gehen Sie zum Abschnitt Bereitstellung.
3. Aktivieren Sie das Kontrollkästchen Bereitstellung für diese Anwendung aktivieren und wählen Sie Live-Modus aus.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert aus IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Service-URL ein. Legen Sie in der CyberArk IAM-Identity-Center-Anwendung den Autorisierungstyp als Autorisierungs-Header fest. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen.
5. Legen Sie den Header-Typ auf Bearer-Token fest.
6. Aus dem vorherigen Verfahren haben Sie den Wert für das Zugriffstoken in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Bearer-Token in der CyberArk IAM-Identity-Center-Anwendung ein.
7. Klicken Sie auf Überprüfen, um die Konfiguration zu testen und anzuwenden.
8. Wählen Sie unter Sync-Optionen das richtige Verhalten aus, für das die ausgehende Bereitstellung von CyberArk funktionieren soll. Sie können vorhandene IAM-Identity-Center-Benutzer mit ähnlichem Prinzipalnamen und dem Aufhebungsverhalten überschreiben (oder nicht).
9. Richten Sie unter Rollenzuordnung die Zuordnung von CyberArk Rollen im Feld Name zur IAM-Identity-Center-Gruppe unter der Zielgruppe ein.
10. Klicken Sie unten auf Speichern, sobald Sie fertig sind.
11. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM-Identity-Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte

Benutzer von CyberArk werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt - Konten zugewiesen werden und innerhalb von IAM Identity Center eine Verbindung herstellen.

(Optional) Schritt 3: Konfigurieren von Benutzerattributen in CyberArk für die Zugriffskontrolle (ABAC) in IAM Identity Center

Dies ist ein optionales Verfahren für , CyberArk wenn Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre - AWS Ressourcen zu verwalten. Die Attribute, die Sie in definieren, CyberArk werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie einen Berechtigungssatz in IAM Identity Center, um den Zugriff basierend auf den Attributen zu verwalten, die Sie von übergeben habenCyberArk.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die Attribute für Zugriffskontrolle Funktion aktivieren. Weitere Information dazu finden Sie unter Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle.

So konfigurieren Sie Benutzerattribute in CyberArk für die Zugriffskontrolle in IAM Identity Center

1. Öffnen Sie die CyberArk IAM-Identity-Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben CyberArk (Apps > Web-Apps).
2. Gehen Sie zur Option SAML Response.
3. Fügen Sie unter Attribute der Tabelle die relevanten Attribute nach der folgenden Logik hinzu:
    a. Der Attributname ist der ursprüngliche Attributname aus CyberArk.
    b. Attributwert ist der Attributname, der in der SAML-Assertion an IAM Identity Center gesendet wird.
4. Wählen Sie Speichern.

(Optional) Übergeben von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein -`AttributeElement` mit dem -`Name`Attribut auf festzulegen`https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Um beispielsweise das Tag-Schlüssel-Wert-Paar zu übergeben`CostCenter = blue`, verwenden Sie das folgende Attribut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates -`AttributeElement` hinzu.

Konfiguration von SAML und SCIM mit einem IAM Google Workspace Identity Center

Wenn Ihr Unternehmen IAM Identity Center verwendet, können Google Workspace Sie Ihre Benutzer und Gruppen aus dem Google Workspace IAM Identity Center integrieren, um ihnen Zugriff auf Ressourcen zu AWS gewähren. Sie können diese Integration erreichen, indem Sie Ihre IAM Identity Center-Identitätsquelle von der standardmäßigen IAM Identity Center-Identitätsquelle auf ändern. Google Workspace

Benutzerinformationen von Google Workspace werden mithilfe des SCIM-Protokolls (System for Cross-Domain Identity Management) v2.0 mit IAM Identity Center synchronisiert. Sie konfigurieren diese Verbindung Google Workspace mithilfe Ihres SCIM-Endpunkts für IAM Identity Center und eines IAM Identity Center-Trägertoken. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Google Workspace zu den benannten Attributen in IAM Identity Center. Diese Zuordnung entspricht den erwarteten Benutzerattributen zwischen IAM Identity Center und. Google Workspace Dazu müssen Sie sich als IAM-Identitätsanbieter und Google Workspace als IAM Identity Center-Identitätsanbieter einrichten.

Zielsetzung

Die Schritte in diesem Tutorial helfen Ihnen beim Herstellen der SAML-Verbindung zwischen Google Workspace und AWS. Später werden Sie Benutzer Google Workspace mithilfe von SCIM synchronisieren. Um zu überprüfen, ob alles korrekt konfiguriert ist, melden Sie sich nach Abschluss der Konfigurationsschritte als Google Workspace Benutzer an und überprüfen den Zugriff AWS

auf Ressourcen. Beachten Sie, dass dieses Tutorial auf einer Testumgebung mit kleinen Google Workspace Verzeichnissen basiert. Verzeichnisstrukturen wie Gruppen und Organisationseinheiten sind nicht enthalten. Nach Abschluss dieses Tutorials können Ihre Benutzer mit Ihren Google Workspace Anmeldeinformationen auf das AWS Zugangsportal zugreifen.

> **Note**
>
> Um sich für eine kostenlose Testversion anzumelden, Google Workspace besuchen Sie Google Workspaceunsere Google's Website.
> Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unterAktivieren AWS IAM Identity Center.

Überlegungen

- Bevor Sie die SCIM-Bereitstellung zwischen Google Workspace und IAM Identity Center konfigurieren, empfehlen wir Ihnen, dies zunächst zu überprüfen. Überlegungen zur Verwendung der automatischen Bereitstellung
- Die automatische SCIM-Synchronisierung von Google Workspace ist derzeit auf die Benutzerbereitstellung beschränkt. Die automatische Gruppenbereitstellung wird derzeit nicht unterstützt. Gruppen können manuell mit dem AWS CLI Identity Store-Befehl create-group oder der AWS Identity and Access Management (IAM) -API erstellt werden. CreateGroup Alternativ können Sie ssosync verwenden, um Google Workspace Benutzer und Gruppen mit dem IAM Identity Center zu synchronisieren.
- Für jeden Google Workspace Benutzer müssen die Werte Vorname, Nachname, Benutzername und Anzeigename angegeben werden.
- Jeder Google Workspace Benutzer hat nur einen einzigen Wert pro Datenattribut, z. B. E-Mail-Adresse oder Telefonnummer. Alle Benutzer mit mehreren Werten können nicht synchronisiert werden. Wenn es Benutzer gibt, deren Attribute mehrere Werte enthalten, entfernen Sie die doppelten Attribute, bevor Sie versuchen, den Benutzer in IAM Identity Center bereitzustellen. Beispielsweise kann nur ein Telefonnummernattribut synchronisiert werden, da das Standard-Telefonnummernattribut „Geschäftstelefon“ ist. Verwenden Sie das Attribut „Geschäftstelefon“, um die Telefonnummer des Benutzers zu speichern, auch wenn es sich bei der Telefonnummer des Benutzers um ein Festnetz oder ein Mobiltelefon handelt.
- Attribute werden weiterhin synchronisiert, wenn der Benutzer in IAM Identity Center deaktiviert, aber immer noch aktiv ist. Google Workspace

- Wenn im Identity Center-Verzeichnis bereits ein Benutzer mit demselben Benutzernamen und derselben E-Mail-Adresse vorhanden ist, wird der Benutzer überschrieben und mit SCIM von synchronisiert. Google Workspace
- Bei der Änderung Ihrer Identitätsquelle sind weitere Überlegungen zu beachten. Weitere Informationen finden Sie unter the section called “Wechseln von IAM Identity Center zu einem externen IdP”.

Schritt 1Google Workspace: Konfigurieren Sie die SAML-Anwendung

1. Melden Sie sich mit einem Konto mit GoogleSuperadministratorrechten bei Ihrer Admin-Konsole an.
2. Wählen Sie im linken Navigationsbereich Ihrer GoogleAdmin-Konsole Apps und dann Web- und Mobilanwendungen aus.
3. Wählen Sie in der Dropdownliste App hinzufügen die Option Nach Apps suchen aus.
4. Geben Sie in das Suchfeld Amazon Web Services ein und wählen Sie dann die Amazon Web Services (SAML) -App aus der Liste aus.
5. Auf der Seite GoogleIdentity Provider-Details — Amazon Web Services können Sie einen der folgenden Schritte ausführen:

   a. Laden Sie IdP-Metadaten herunter.

   b. Kopieren Sie die SSO-URL, die Entitäts-ID-URL und die Zertifikatsinformationen.

   In Schritt 2 benötigen Sie entweder die XML-Datei oder die URL-Informationen.
6. Lassen Sie diese Seite geöffnet und wechseln Sie zur IAM Identity Center-Konsole, bevor Sie mit dem nächsten Schritt in der Google Admin-Konsole fortfahren.

Schritt 2: IAM Identity Center undGoogle Workspace: Ändern Sie die IAM Identity Center-Identitätsquelle und richten Sie sie Google Workspace als SAML-Identitätsanbieter ein

1. Melden Sie sich mit einer Rolle mit Administratorrechten bei der IAM Identity Center-Konsole an.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Option Aktionen und dann Identitätsquelle ändern aus.

- Wenn Sie IAM Identity Center nicht aktiviert haben, finden Sie IAM Identity Center aktivieren weitere Informationen unter. Nachdem Sie IAM Identity Center zum ersten Mal aktiviert und darauf zugegriffen haben, gelangen Sie zum Dashboard, wo Sie Ihre Identitätsquelle auswählen können.

4. Wählen Sie auf der Seite Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.
5. Die Seite Externen Identitätsanbieter konfigurieren wird geöffnet. Um diese Seite und die Google Workspace Seite in Schritt 1 abzuschließen, müssen Sie Folgendes ausführen:

   - Im Abschnitt mit den Metadaten des Identitätsanbieters in der IAM Identity Center-Konsole müssen Sie einen der folgenden Schritte ausführen:

     i. Laden Sie die GoogleSAML-Metadaten als IdP-SAML-Metadaten in die IAM Identity Center-Konsole hoch.

     ii. Kopieren Sie die GoogleSSO-URL und fügen Sie sie in das Feld IdP-Anmelde-URL und die GoogleAussteller-URL in das Feld IdP-Aussteller-URL ein und laden Sie das GoogleZertifikat als IdP-Zertifikat hoch.

6. Nachdem Sie die Google Metadaten im Abschnitt mit den Metadaten des Identitätsanbieters der IAM Identity Center-Konsole angegeben haben, kopieren Sie die Anmelde-URL für das AWS Zugriffsportal, die URL des IAM Identity Assertion Consumer Service (ACS) und die IAM Identity Center-Aussteller-URL. Sie müssen diese URLs im nächsten Schritt in der Google Admin-Konsole angeben.
7. Lassen Sie die Seite mit der IAM Identity Center-Konsole geöffnet und kehren Sie zur Google Admin-Konsole zurück. Sie sollten sich auf der Seite Amazon Web Services — Service Provider-Details befinden. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite mit den Service Provider-Details die Werte ACS-URL, Entitäts-ID und Start-URL ein. Sie haben diese Werte im vorherigen Schritt kopiert und sie befinden sich in der IAM Identity Center-Konsole.

   - Fügen Sie die URL des IAM Identity Center Assertion Consumer Service (ACS) in das ACS-URL-Feld ein
   - Fügen Sie die IAM Identity Center-Aussteller-URL in das Feld Entitäts-ID ein.
   - Fügen Sie die Anmelde-URL für das AWS Access Portal in das Feld Start-URL ein.

9. Füllen Sie auf der Seite mit den Service Provider-Details die Felder unter Name ID wie folgt aus:

- Wählen Sie für das Format Name ID die Option EMAIL aus
- Wählen Sie für Name ID die Option Basisinformationen > Primäre E-Mail-Adresse

10. Klicken Sie auf Weiter.
11. Wählen Sie auf der Seite Attributzuordnung unter Attribute die Option ZUORDNUNG HINZUFÜGEN aus, und konfigurieren Sie dann diese Felder unter GoogleVerzeichnisattribut:
    - Wählen Sie für das `https://aws.amazon.com/SAML/Attributes/RoleSessionName` App-Attribut das Feld Basisinformationen, Primäre E-Mail-Adresse aus den Google DirectoryAttributen aus.
    - Wählen Sie für das `https://aws.amazon.com/SAML/Attributes/Role` App-Attribut beliebige Google DirectoryAttribute aus. Ein Google Verzeichnisattribut könnte Abteilung sein.
12. Wählen Sie Fertig stellen
13. Kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Weiter. Überprüfen Sie auf der Seite Überprüfen und Bestätigen die Informationen und geben Sie dann ACCEPT in das dafür vorgesehene Feld ein. Wählen Sie Identitätsquelle ändern aus.

Sie sind jetzt bereit, die Amazon Web Services Services-App zu aktivieren, Google Workspace damit Ihre Benutzer im IAM Identity Center bereitgestellt werden können.

Schritt 3Google Workspace: Aktivieren Sie die Apps

1. Kehren Sie zur GoogleAdmin-Konsole und Ihrer AWS IAM Identity Center Anwendung zurück, die Sie unter Apps sowie Web- und Mobil-Apps finden.
2. Klicken Sie im Bereich Benutzerzugriff neben Benutzerzugriff auf den Abwärtspfeil, um den Benutzerzugriff zu erweitern und den Dienststatusbereich anzuzeigen.
3. Wählen Sie im Bereich „Servicestatus“ die Option für alle aktiviert und anschließend SPEICHERN aus.

> **Note**
>
> Um das Prinzip der geringsten Rechte beizubehalten, empfehlen wir, den Dienststatus nach Abschluss dieses Tutorials für alle auf AUS zu ändern. Nur für Benutzer, die Zugriff auf benötigen, AWS sollte der Dienst aktiviert sein. Sie können Google Workspace Gruppen oder

Organisationseinheiten verwenden, um Benutzern Zugriff auf eine bestimmte Teilmenge Ihrer Benutzer zu gewähren.

Schritt 4: IAM Identity Center: Richten Sie die automatische Bereitstellung von IAM Identity Center ein

1. Kehren Sie zur IAM Identity Center-Konsole zurück.
2. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
3. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten die einzelnen Werte für die folgenden Optionen. In Schritt 5 dieses Tutorials geben Sie diese Werte ein, um die automatische Bereitstellung zu konfigurieren. Google Workspace

   - SCIM-Endpunkt
   - Zugriffstoken

   > ⚠ Warning
   >
   > Dies ist das einzige Mal, dass Sie den SCIM-Endpunkt und das Zugriffstoken erhalten können. Stellen Sie sicher, dass Sie diese Werte kopieren, bevor Sie fortfahren.

4. Klicken Sie auf Schließen.

   Nachdem Sie die Bereitstellung in der IAM Identity Center-Konsole eingerichtet haben, konfigurieren Sie im nächsten Schritt die auto Bereitstellung in. Google Workspace

Schritt 5Google Workspace: auto Bereitstellung konfigurieren

1. Kehren Sie zur Google Admin-Konsole und zu Ihrer AWS IAM Identity Center Anwendung zurück, die Sie unter Apps sowie Web- und Mobil-Apps finden. Wählen Sie im Abschnitt auto Bereitstellung die Option Automatische Bereitstellung konfigurieren aus.
2. Im vorherigen Verfahren haben Sie den Wert des Zugriffstokens in die IAM Identity Center-Konsole kopiert. Fügen Sie diesen Wert in das Feld Zugriffstoken ein und wählen Sie Weiter.

Außerdem haben Sie im vorherigen Verfahren den SCIM-Endpunktwert in die IAM Identity Center-Konsole kopiert. Fügen Sie diesen Wert in das Feld Endpunkt-URL ein. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen, und wählen Sie Weiter.

3. Stellen Sie sicher, dass alle obligatorischen IAM Identity Center-Attribute (die mit einem* markierten) Attributen zugeordnet sind. Google Cloud Directory Wenn nicht, wählen Sie den Abwärtspfeil und ordnen Sie das entsprechende Attribut zu. Klicken Sie auf Weiter.
4. Im Abschnitt Bereitstellungsbereich können Sie eine Gruppe mit Ihrem Google Workspace Verzeichnis auswählen, um Zugriff auf die Amazon Web Services Services-App zu gewähren. Überspringen Sie diesen Schritt und wählen Sie Weiter.
5. Im Abschnitt Deprovisioning können Sie auswählen, wie auf verschiedene Ereignisse reagiert werden soll, die einem Benutzer den Zugriff entziehen. Für jede Situation können Sie den Zeitraum bis zum Beginn der Deprovisionierung angeben, um:

   - innerhalb von 24 Stunden
   - nach einem Tag
   - nach sieben Tagen
   - nach 30 Tagen

   In jeder Situation gibt es eine Zeiteinstellung, in der festgelegt wird, wann der Zugriff auf ein Konto gesperrt und wann das Konto gelöscht werden soll.

   > **Tip**
   >
   > Lege immer mehr Zeit für das Löschen eines Benutzerkontos fest als für die Sperrung eines Benutzerkontos.

6. Wählen Sie Finish (Abschließen). Sie werden zur Amazon Web Services Services-App-Seite zurückgeleitet.
7. Schalten Sie im Bereich Automatische Bereitstellung den Kippschalter ein, um ihn von Inaktiv in Aktiv zu ändern.

> **Note**
>
> Der Aktivierungsschieberegler ist deaktiviert, wenn IAM Identity Center für Benutzer nicht aktiviert ist. Wählen Sie Benutzerzugriff und schalten Sie die App ein, um den Schieberegler zu aktivieren.

8. Wählen Sie im Bestätigungsdialogfeld die Option Einschalten aus.
9. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM Identity Center-Konsole zurück und wählen Sie Benutzer aus. Auf der Seite Benutzer werden die Benutzer aus Ihrem Google Workspace Verzeichnis aufgeführt, die von SCIM erstellt wurden. Wenn Benutzer noch nicht aufgeführt sind, ist die Bereitstellung möglicherweise noch im Gange. Die Bereitstellung kann bis zu 24 Stunden dauern, obwohl sie in den meisten Fällen innerhalb von Minuten abgeschlossen ist. Achten Sie darauf, das Browserfenster alle paar Minuten zu aktualisieren.

   Wählen Sie einen Benutzer aus und sehen Sie sich dessen Details an. Die Informationen sollten mit den Informationen im Google Workspace Verzeichnis übereinstimmen.

> **Herzlichen Glückwunsch!**
>
> Sie haben erfolgreich eine SAML-Verbindung zwischen Google Workspace und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert. Sie können diese Benutzer jetzt Konten und Anwendungen in IAM Identity Center zuweisen. Für dieses Tutorial bestimmen wir im nächsten Schritt einen der Benutzer als IAM Identity Center-Administrator, indem wir ihm Administratorrechte für das Verwaltungskonto gewähren.

Schritt 6: IAM Identity Center: Gewähren Sie Google Workspace Benutzern Zugriff auf Konten

1. Kehren Sie zur IAM Identity Center-Konsole zurück. Wählen Sie im IAM Identity Center-Navigationsbereich unter Berechtigungen für mehrere Konten die Option. AWS-Konten
2. Auf der AWS-KontenSeite „Organisationsstruktur“ wird Ihr Organisationsstamm mit Ihren Konten darunter in der Hierarchie angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.

3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:

   a. Wählen Sie für Schritt 1: Benutzer und Gruppen auswählen den Benutzer aus, der die Administratorfunktion ausführen soll. Wählen Sie anschließend Weiter.

   b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Teilschritte führt, die zur Erstellung eines Berechtigungssatzes erforderlich sind.

      i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:

         - Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
         - Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

         Wählen Sie Weiter aus.

      ii. Für Schritt 2: Geben Sie Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter aus.

         Mit den Standardeinstellungen wird ein Berechtigungssatz *AdministratorAccess*mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist.

      iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen. Auf der Seite Berechtigungssätze wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diese Registerkarte jetzt in Ihrem Webbrowser schließen.

      iv. Auf der Browser-Registerkarte „Benutzer und Gruppen zuweisen“ befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

      v. Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *AdministratorAccess*Berechtigungssatz wird in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter.

   c. Überprüfen Sie für Schritt 3: Überprüfen und Absenden den ausgewählten Benutzer und den ausgewählten Berechtigungssatz und wählen Sie dann Senden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihr AWS-Konto System gerade konfiguriert wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. In einer Benachrichtigung werden Sie darüber informiert, dass Ihr AWS-Konto Konto erneut bereitgestellt und der aktualisierte Berechtigungssatz angewendet wurde. Wenn sich der Benutzer anmeldet, hat er die Möglichkeit, die Rolle auszuwählen. `AdministratorAccess`

> **Note**
>
> Die automatische SCIM-Synchronisierung von unterstützt Google Workspace nur die Bereitstellung von Benutzern. Die automatische Gruppenbereitstellung wird derzeit nicht unterstützt. Mit dem können Sie keine Gruppen für Ihre Google Workspace Benutzer erstellen. AWS Management Console Nachdem Sie Benutzer bereitgestellt haben, können Sie Gruppen mit dem AWS CLI Identity Store-Befehl create-group oder der IAM-API erstellen. CreateGroup

Schritt 7Google Workspace: Bestätigen Sie Google Workspace den Benutzerzugriff auf Ressourcen AWS

1. Melden Sie sich Google mit einem Testbenutzerkonto an. Informationen zum Hinzufügen von Benutzern finden Sie in Google Workspace der Google WorkspaceDokumentation.
2. Wählen Sie das Google apps Launcher-Symbol (Waffel) aus.
3. Scrollen Sie zum Ende der App-Liste, in der sich Ihre benutzerdefinierten Google Workspace Apps befinden. Zwei Apps werden angezeigt: Amazon Web Services und AWS Access Portal.
4. Wählen Sie die AWS Access-Portal-App aus. Sie sind im Portal angemeldet und können das AWS-Konto Symbol sehen. Erweitern Sie dieses Symbol, um die Liste der Symbole anzuzeigen AWS-Konten , auf die der Benutzer zugreifen kann. In diesem Tutorial haben Sie nur mit einem einzigen Konto gearbeitet, sodass beim Erweitern des Symbols nur ein Konto angezeigt wird.

> **Note**
>
> Wenn Sie die Amazon Web Services Services-App auswählen, erhalten Sie einen SAML-Fehler. Diese App wird für Google Workspace Benutzer verwendet, die als IAM-

Benutzer bereitgestellt wurden. In diesem Tutorial werden Ihre Benutzer als Google Workspace Benutzer im IAM Identity Center bereitgestellt.

5. Wählen Sie das Konto aus, um die für den Benutzer verfügbaren Berechtigungssätze anzuzeigen. In diesem Tutorial haben Sie den AdministratorAccessBerechtigungssatz erstellt.
6. Neben dem Berechtigungssatz befinden sich Links für den Zugriffstyp, der für diesen Berechtigungssatz verfügbar ist. Bei der Erstellung des Berechtigungssatzes haben Sie angegeben, dass sowohl die Verwaltungskonsole als auch der programmgesteuerte Zugriff aktiviert werden sollen, sodass diese beiden Optionen verfügbar sind. Wählen Sie Managementkonsole aus, um die zu öffnen. AWS Management Console
7. Der Benutzer ist an der Konsole angemeldet.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein `Attribute` Element zu übergeben, dessen `Name` Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates `Attribute` Element hinzu.

Nächste Schritte

Nachdem Sie nun Google Workspace als Identitätsanbieter konfiguriert und Benutzer in IAM Identity Center bereitgestellt haben, können Sie:

- Verwenden Sie den AWS CLI Identity Store-Befehl create-group oder die IAM-API, um Gruppen CreateGroupfür Ihre Benutzer zu erstellen.

  Gruppen sind nützlich, wenn Sie Zugriff auf Anwendungen zuweisen möchten. AWS-Konten Anstatt jeden Benutzer einzeln zuzuweisen, erteilen Sie einer Gruppe Berechtigungen. Wenn Sie später Benutzer zu einer Gruppe hinzufügen oder daraus entfernen, erhält oder verliert der Benutzer dynamisch Zugriff auf Konten und Anwendungen, die Sie der Gruppe zugewiesen haben.

- Konfigurieren Sie Berechtigungen auf der Grundlage von Aufgabenfunktionen. Weitere Informationen finden Sie unter Erstellen von Berechtigungssätzen.

  Berechtigungssätze definieren die Zugriffsebene, auf die Benutzer und Gruppen zugreifen können AWS-Konto. Berechtigungssätze werden im IAM Identity Center gespeichert und können für einen oder mehrere Personen bereitgestellt werden. AWS-Konten Sie können einem Benutzer mehrere Berechtigungssätze zuweisen.

> **Note**
>
> Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere IdP-Zertifikate durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein IdP-Zertifikat ersetzen, wenn sich das Ablaufdatum des Zertifikats nähert. Der Vorgang des Ersetzens eines älteren Zertifikats durch ein neueres wird als Zertifikatsrotation bezeichnet. Lesen Sie unbedingt, wie Sie die SAML-Zertifikate für Google Workspace verwalten.

Verwenden von IAM Identity Center zum Herstellen einer Verbindung mit Ihrer -JumpCloudVerzeichnisplattform

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisierung) von Benutzerinformationen von JumpCloud Directory Platform in IAM Identity Center. Diese Bereitstellung verwendet das System for Cross-Domain Identity Management (SCIM) v2.0-Protokoll. Sie konfigurieren diese Verbindung in JumpCloud mit Ihrem IAM-Identity-Center-SCIM-Endpunkt und Zugriffstoken. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute in JumpCloud zu den benannten Attributen in IAM Identity Center. Dies führt dazu, dass die erwarteten Attribute zwischen IAM Identity Center und übereinstimmenJumpCloud.

Dieses Handbuch basiert auf JumpCloud dem Stand Juni 2021. Die Schritte für neuere Versionen können variieren. Dieses Handbuch enthält einige Hinweise zur Konfiguration der Benutzerauthentifizierung über SAML.

Die folgenden Schritte führen Sie durch die Aktivierung der automatischen Bereitstellung von Benutzern und Gruppen von JumpCloud zu IAM Identity Center mithilfe des SCIM-Protokolls.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu überprüfenÜberlegungen zur Verwendung der automatischen Bereitstellung. Lesen Sie dann weitere Überlegungen im nächsten Abschnitt.

Themen

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- JumpCloud -Abonnement oder kostenlose Testversion. Um sich für eine kostenlose Testversion anzumelden, besuchen Sie JumpCloud.
- Ein IAM-Identity-Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Eine SAML-Verbindung von Ihrem JumpCloud Konto zu IAM Identity Center, wie in JumpCloud der Dokumentation für IAM Identity Center beschrieben.
- Ordnen Sie den IAM-Identity-Center-Konnektor den Gruppen zu, denen Sie den Zugriff auf AWS Konten erlauben möchten.

Überlegungen zu SCIM

Im Folgenden finden Sie Überlegungen zur Verwendung des JumpCloud Verbunds für IAM Identity Center.

- Nur Gruppen, die dem AWS Single-Sign-On-Konnektor in zugeordnet JumpCloud sind, werden mit SCIM synchronisiert.
- Es kann nur ein Telefonnummernattribut synchronisiert werden und der Standardwert ist „Workphone“.
- Benutzer im JumpCloud Verzeichnis müssen Vor- und Nachnamen konfiguriert haben, um mit SCIM mit IAM Identity Center synchronisiert zu werden.
- Attribute werden weiterhin synchronisiert, wenn der Benutzer im IAM Identity Center deaktiviert, aber weiterhin in aktiviert istJumpCloud.
- Sie können die SCIM-Synchronisierung nur für Benutzerinformationen aktivieren, indem Sie die Option „Verwaltung von Benutzergruppen und Gruppenmitgliedschaft aktivieren“ im Konnektor deaktivieren.
- Wenn im Identity-Center-Verzeichnis ein Benutzer mit demselben Benutzernamen und derselben E-Mail vorhanden ist, wird der Benutzer von überschrieben und mit SCIM synchronisiertJumpCloud.

Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM-Identity-Center-Konsole, um die automatische Bereitstellung zu aktivieren.

So aktivieren Sie die automatische Bereitstellung in IAM Identity Center

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Feld Informationen zur automatischen Bereitstellung und wählen Sie dann Aktivieren aus. Dies aktiviert sofort die automatische Bereitstellung im IAM Identity Center und zeigt die erforderlichen SCIM-Endpunkt- und Zugriffstokeninformationen an.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehenden Datenverkehr jeden der Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

a. SCIM-Endpunkt
b. Zugriffstoken

5. Klicken Sie auf Schließen.

Nachdem Sie nun die Bereitstellung in der IAM-Identity-Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mit dem JumpCloud IAM-Identity-Center-Konnektor abschließen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren der Bereitstellung in JumpCloud

Gehen Sie wie folgt im JumpCloud IAM-Identity-Center-Konnektor vor, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie den JumpCloud IAM-Identity-Center-Konnektor bereits zu Ihrem JumpCloud Administratorportal und Ihren Gruppen hinzugefügt haben. Wenn Sie dies noch nicht getan haben, lesen Sie , und führen Sie dann dieses Verfahren ausVoraussetzungen, um die SCIM-Bereitstellung zu konfigurieren.

So konfigurieren Sie die Bereitstellung in JumpCloud

1. Öffnen Sie den JumpCloud IAM-Identity-Center-Konnektor, den Sie im Rahmen der Konfiguration von SAML für installiert haben JumpCloud (Benutzerauthentifizierung > IAM Identity Center). Siehe Voraussetzungen.
2. Wählen Sie den IAM-Identity-Center-Konnektor und dann die dritte Registerkarte Identity Management aus.
3. Aktivieren Sie das Kontrollkästchen Verwaltung von Benutzergruppen und Gruppenmitgliedschaft in dieser Anwendung aktivieren, wenn Sie Gruppen für die SCIM-Synchronisierung verwenden möchten.
4. Klicken Sie auf Konfigurieren.
5. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Basis-URL im JumpCloud IAM-Identity-Center-Konnektor ein. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen.
6. Aus dem vorherigen Verfahren haben Sie den Wert für das Zugriffstoken in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Token-Schlüssel im JumpCloud IAM-Identity-Center-Konnektor ein.
7. Klicken Sie auf Aktivieren, um die Konfiguration anzuwenden.
8. Stellen Sie sicher, dass neben Single Sign-On aktiviert ein grüner Indikator angezeigt wird.

9. Wechseln Sie zur vierten Registerkarte Benutzergruppen und überprüfen Sie die Gruppen, die Sie mit SCIM bereitstellen möchten.
10. Klicken Sie unten auf Speichern, sobald Sie fertig sind.
11. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM-Identity-Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von JumpCloud werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt Konten innerhalb von IAM Identity Center zugewiesen werden.

(Optional) Schritt 3: Konfigurieren von Benutzerattributen in JumpCloud für die Zugriffskontrolle in IAM Identity Center

Dies ist ein optionales Verfahren für , JumpCloud wenn Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre -AWSRessourcen zu verwalten. Die Attribute, die Sie in definieren, JumpCloud werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie einen Berechtigungssatz in IAM Identity Center, um den Zugriff basierend auf den Attributen zu verwalten, die Sie von übergeben habenJumpCloud.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zunächst die Funktion Attribute für die Zugriffskontrolle aktivieren. Weitere Informationen dazu finden Sie unter Aktivieren und Konfigurieren von Attributen für die Zugriffskontrolle.

So konfigurieren Sie Benutzerattribute in JumpCloud für die Zugriffskontrolle in IAM Identity Center

1. Öffnen Sie den JumpCloud IAM-Identity-Center-Konnektor, den Sie im Rahmen der Konfiguration von SAML für installiert haben JumpCloud (Benutzerauthentifizierung > IAM Identity Center).
2. Wählen Sie den IAM-Identity-Center-Konnektor aus. Wählen Sie dann die zweite Registerkarte IAM Identity Center aus.
3. Unten auf dieser Registerkarte haben Sie die Benutzerattributzuordnung , wählen Sie Neues Attribut hinzufügen und gehen dann wie folgt vor: Sie müssen diese Schritte für jedes Attribut ausführen, das Sie zur Verwendung in IAM Identity Center für die Zugriffskontrolle hinzufügen.

    a. Geben Sie im Feld Name des Service-Attributs angeben Ersetzen `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` Sie durch **`AttributeName`** den Namen des Attributs, das Sie in IAM Identity Center erwarten. Beispiel: `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**

b. Wählen Sie im Feld JumpCloud Attributname Benutzerattribute aus Ihrem JumpCloud Verzeichnis aus. Zum Beispiel E-Mail (Work).

4. Wählen Sie Speichern.

(Optional) Übergeben von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein -`AttributeElement` mit dem -`Name`Attribut auf festzulegen`https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Um beispielsweise das Tag-Schlüssel-Wert-Paar zu übergeben`CostCenter = blue`, verwenden Sie das folgende Attribut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates -`AttributeElement` hinzu.

Konfiguration von SAML und SCIM mit einem IAM Microsoft Entra ID Identity Center

AWS IAM Identity Centerunterstützt die Integration mit Security Assertion Markup Language (SAML) 2.0 sowie die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen aus Microsoft Entra ID (früher bekannt als Azure Active Directory oder) in IAM Identity Center mithilfe des Systems for Cross-Domain Identity Management (SCIMAzure AD) 2.0-Protokoll.

Zielsetzung

In diesem Tutorial richten Sie ein Testlabor ein und konfigurieren eine SAML-Verbindung und SCIM-Bereitstellung zwischen dem IAM Identity Microsoft Entra ID Center. Während der ersten Vorbereitungsschritte erstellen Sie sowohl in IAM Identity Center als auch in IAM Identity Center einen Testbenutzer (Nikki Wolf), mit dem Sie die SAML-Verbindung in beide Microsoft Entra ID Richtungen testen können. Später, im Rahmen der SCIM-Schritte, erstellen Sie einen anderen Testbenutzer (Richard Roe), um zu überprüfen, ob neue Attribute erwartungsgemäß mit IAM Microsoft Entra ID Identity Center synchronisiert werden.

Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen können, müssen Sie zunächst Folgendes einrichten:

- Ein Microsoft Entra ID Mieter. Weitere Informationen finden Sie unter Schnellstart: Einen Mandanten einrichten auf der Microsoft-Website.
- Ein AWS IAM Identity Center -fähiges Konto. Weitere Informationen finden Sie unter Aktivieren von IAM Identity Center im AWS IAM Identity CenterBenutzerhandbuch.

Schritt 1: Bereiten Sie Ihren Microsoft-Mandanten vor

In diesem Schritt erfahren Sie, wie Sie Ihre AWS IAM Identity Center Unternehmensanwendung installieren und konfigurieren und einem neu erstellten Microsoft Entra ID Testbenutzer Zugriff zuweisen.

Step 1.1 >

Schritt 1.1: Richten Sie die AWS IAM Identity Center Unternehmensanwendung ein in Microsoft Entra ID

In diesem Verfahren installieren Sie die AWS IAM Identity Center Unternehmensanwendung inMicrosoft Entra ID. Sie benötigen diese Anwendung später, um Ihre SAML-Verbindung mit AWS zu konfigurieren.

1. Melden Sie sich mindestens als Cloud-Anwendungsadministrator im Microsoft Entra Admin Center an.
2. Navigieren Sie zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann Neue Anwendung aus.
3. Geben Sie auf der Seite Microsoft Entra Gallery durchsuchen **`AWS IAM Identity Center`**in das Suchfeld ein.

4. Wählen Sie AWS IAM Identity Centeraus dem Ergebnisbereich aus.
5. Wählen Sie Erstellen aus.

Step 1.2 >

Schritt 1.2: Erstellen Sie einen Testbenutzer in Microsoft Entra ID

Nikki Wolf ist der Name Ihres Microsoft Entra ID Testbenutzers, den Sie in diesem Verfahren erstellen werden.

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität > Benutzer > Alle Benutzer.
2. Wählen Sie Neuer Benutzer und dann oben auf dem Bildschirm Neuen Benutzer erstellen aus.
3. Geben Sie **`NikkiWolf`**im Feld Benutzerprinzipalname Ihre bevorzugte Domain und Erweiterung ein und wählen Sie sie aus. Zum Beispiel NikkiWolf@ *`example.org`*.
4. Geben **`NikkiWolf`**Sie im Feld Anzeigename den Wert ein.
5. Geben Sie unter Passwort ein sicheres Passwort ein oder klicken Sie auf das Augensymbol, um das automatisch generierte Passwort anzuzeigen, und kopieren Sie den angezeigten Wert entweder oder notieren Sie ihn.
6. Wählen Sie Eigenschaften und geben Sie im Feld Vorname den Text ein **`Nikki`**. Geben Sie im Feld Nachname den Wert ein **`Wolf`**.
7. Wählen Sie Überprüfen + Erstellen und dann Erstellen aus.

Step 1.3

Schritt 1.3: Testen Sie Nikkis Erfahrung, bevor Sie ihr die Berechtigungen zuweisen AWS IAM Identity Center

In diesem Verfahren überprüfen Sie, was Nikki erfolgreich in ihrem Microsoft My Account-Portal anmelden kann.

1. Öffnen Sie im selben Browser eine neue Registerkarte, rufen Sie die Anmeldeseite des Portals Mein Konto auf und geben Sie die vollständige E-Mail-Adresse von Nikki ein. Zum Beispiel NikkiWolf@ *`example.org`*.

2. Wenn Sie dazu aufgefordert werden, geben Sie Nikkis Passwort ein und wählen Sie dann Anmelden. Wenn es sich um ein automatisch generiertes Passwort handelt, werden Sie aufgefordert, das Passwort zu ändern.
3. Wählen Sie auf der Seite Aktion erforderlich die Option Später fragen aus, um die Aufforderung zur Angabe zusätzlicher Sicherheitsmethoden zu umgehen.
4. Wählen Sie auf der Seite Mein Konto in der linken Navigationsleiste Meine Apps aus. Beachten Sie, dass außer Add-ins derzeit keine Apps angezeigt werden. Sie werden eine AWS IAM Identity CenterApp hinzufügen, die in einem späteren Schritt hier angezeigt wird.

Step 1.4

Schritt 1.4: Weisen Sie Nikki Berechtigungen zu in Microsoft Entra ID

Nachdem Sie nun verifiziert haben, dass Nikki erfolgreich auf das Portal Mein Konto zugreifen kann, gehen Sie wie folgt vor, um ihren Benutzer der AWS IAM Identity CenterApp zuzuweisen.

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie dann AWS IAM Identity Centeraus der Liste aus.
2. Wählen Sie auf der linken Seite Benutzer und Gruppen aus.
3. Wählen Sie Add user/group (Benutzer/Gruppe hinzufügen) aus. Sie können die Meldung ignorieren, dass Gruppen nicht zugewiesen werden können. In diesem Tutorial werden keine Gruppen für Aufgaben verwendet.
4. Wählen Sie auf der Seite Zuweisung hinzufügen unter Benutzer die Option Keine ausgewählt aus.
5. Wählen Sie NikkiWolfund wählen Sie dann Auswählen.
6. Wählen Sie auf der Seite „Zuweisung hinzufügen“ die Option „Zuweisen“. NikkiWolf erscheint jetzt in der Liste der Benutzer, die der AWS IAM Identity CenterApp zugewiesen sind.

Schritt 2: Bereiten Sie Ihr AWS Konto vor

In diesem Schritt erfahren Sie, wie Sie IAM Identity CenterZugriffsberechtigungen (über einen Berechtigungssatz) konfigurieren, manuell einen entsprechenden Nikki Wolf-Benutzer erstellen und ihr die erforderlichen Berechtigungen für die Verwaltung von Ressourcen zuweisen. AWS

Step 2.1 >

Schritt 2.1: Erstellen Sie einen RegionalAdmin Berechtigungssatz in IAM Identity Center

Dieser Berechtigungssatz wird verwendet, um Nikki die erforderlichen AWS Kontoberechtigungen zu gewähren, die für die Verwaltung von Regionen auf der Kontoseite innerhalb von erforderlich sind. AWS Management Console Alle anderen Berechtigungen zum Anzeigen oder Verwalten anderer Informationen für Nikkis Konto sind standardmäßig verweigert.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
4. Wählen Sie auf der Seite Berechtigungssatztyp auswählen die Option Benutzerdefinierter Berechtigungssatz und dann Weiter aus.
5. Wählen Sie Inline-Richtlinie aus, um sie zu erweitern, und erstellen Sie dann mithilfe der folgenden Schritte eine Richtlinie für den Berechtigungssatz:

   a. Wählen Sie Neue Erklärung hinzufügen, um eine Richtlinienerklärung zu erstellen.

   b. Wählen Sie unter Kontoauszug bearbeiten die Option Konto aus der Liste aus und aktivieren Sie dann die folgenden Kontrollkästchen.

      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**

   c. Wählen Sie neben Eine Ressource hinzufügen die Option Hinzufügen aus.

   d. Wählen Sie auf der Seite Ressource hinzufügen unter Ressourcentyp die Option Alle Ressourcen und dann Ressource hinzufügen aus. Vergewissern Sie sich, dass Ihre Richtlinie wie folgt aussieht:

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
```

```
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Wählen Sie Weiter.
7. Geben Sie auf der Seite Details zum Berechtigungssatz angeben unter Name des Berechtigungssatzes die Eingabe ein **`RegionalAdmin`**, und wählen Sie dann Weiter aus.
8. Wählen Sie auf der Seite Überprüfen und erstellen die Option Erstellen aus. In der Liste der Berechtigungssätze sollte diese Option RegionalAdminangezeigt werden.

Step 2.2 >

Schritt 2.2: Erstellen Sie einen entsprechenden NikkiWolf Benutzer in IAM Identity Center

Da das SAML-Protokoll keinen Mechanismus bietet, um den IdP (Microsoft Entra ID) abzufragen und Benutzer hier in IAM Identity Center automatisch zu erstellen, gehen Sie wie folgt vor, um manuell einen Benutzer in IAM Identity Center zu erstellen, der die Kernattribute von Nikki Wolfs Benutzer in widerspiegelt. Microsoft Entra ID

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Benutzer und Benutzer hinzufügen aus, und geben Sie dann die folgenden Informationen ein:
   a. Sowohl für den Benutzernamen als auch für die E-Mail-Adresse — Geben Sie dieselbe **`NikkiWolf@`** ***`yourcompanydomain.extension`*** ein, die Sie bei der Erstellung Ihres Benutzers verwendet haben. Microsoft Entra ID *Zum Beispiel @ example.org. NikkiWolf*
   b. E-Mail-Adresse bestätigen — Geben Sie die E-Mail-Adresse aus dem vorherigen Schritt erneut ein
   c. Vorname — Geben Sie ein **`Nikki`**
   d. Nachname — Geben Sie ein **`Wolf`**

e. Anzeigename — Geben Sie ein **`Nikki Wolf`**

3. Wählen Sie zweimal Weiter und dann Benutzer hinzufügen.
4. Klicken Sie auf Close (Schließen).

Step 2.3

Schritt 2.3: Weisen Sie Nikki den in festgelegten RegionalAdmin Berechtigungen zu IAM Identity Center

Hier finden Sie die Regionen, AWS-Konto in denen Nikki die Regionen verwalten wird, und weisen ihr dann die erforderlichen Berechtigungen zu, damit sie erfolgreich auf das AWS Zugriffsportal zugreifen kann.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option. AWS-Konten
3. Aktiviere das Kontrollkästchen neben dem Kontonamen (zum Beispiel *`Sandbox`*), für den du Nikki Zugriff auf die Verwaltung von Regionen gewähren möchtest, und wähle dann Benutzer und Gruppen zuweisen aus.
4. Wähle auf der Seite „Benutzer und Gruppen zuweisen“ den Tab „Benutzer“, suche das Kästchen neben Nikki, markiere es und wähle dann Weiter aus.

Schritt 3: Konfigurieren und testen Sie Ihre SAML-Verbindung

In diesem Schritt konfigurieren Sie Ihre SAML-Verbindung mithilfe der AWS IAM Identity Center Unternehmensanwendung Microsoft Entra ID zusammen mit den externen IdP-Einstellungen in IAM Identity Center.

Step 3.1 >

Schritt 3.1: Sammeln Sie die erforderlichen Dienstanbieter-Metadaten aus dem IAM Identity Center

In diesem Schritt starten Sie den Assistenten zum Ändern der Identitätsquelle in der IAM Identity Center-Konsole und rufen die Metadatendatei und die AWS spezifische Anmelde-URL ab, die Sie bei der Konfiguration der Verbindung Microsoft Entra ID im nächsten Schritt eingeben müssen.

1. Wählen Sie in der IAM Identity Center-Konsole Einstellungen aus.

2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ **>** „Identitätsquelle ändern“.
3. Wählen Sie auf der Seite Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.
4. Wählen Sie auf der Seite Externen Identitätsanbieter konfigurieren unter Metadaten des Dienstanbieters die Option Metadatendatei herunterladen aus, um sie auf Ihr System herunterzuladen.
5. Suchen Sie im selben Abschnitt den Wert für die Anmelde-URL für das AWS Access Portal und kopieren Sie ihn. Sie müssen diesen Wert eingeben, wenn Sie im nächsten Schritt dazu aufgefordert werden.
6. Lassen Sie diese Seite geöffnet und fahren Sie mit dem nächsten Schritt (**`Step 3.2`**) fort, um die AWS IAM Identity Center Unternehmensanwendung zu konfigurierenMicrosoft Entra ID. Später kehren Sie zu dieser Seite zurück, um den Vorgang abzuschließen.

Step 3.2 **>**

Schritt 3.2: Konfigurieren Sie die AWS IAM Identity Center Unternehmensanwendung in Microsoft Entra ID

Dieses Verfahren stellt die Hälfte der SAML-Verbindung auf Microsoft-Seite mithilfe der Werte aus der Metadatendatei und der Anmelde-URL her, die Sie im letzten Schritt abgerufen haben.

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität **>** Anwendungen **>** Unternehmensanwendungen und wählen Sie AWS IAM Identity Centerdann.
2. Wählen Sie auf der linken Seite Single Sign-On aus.
3. Wählen Sie auf der Seite Single Sign-On mit SAML einrichten die Option Metadatendatei hochladen aus, klicken Sie auf das Ordnersymbol, wählen Sie die Metadatendatei des Dienstanbieters aus, die Sie im vorherigen Schritt heruntergeladen haben, und klicken Sie dann auf Hinzufügen.
4. Stellen Sie auf der Seite Basic SAML Configuration sicher, dass sowohl der Identifier - als auch der Antwort-URL-Wert jetzt auf Endpunkte verweisen, die mit beginnen. AWS `https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. Fügen Sie unter Anmelde-URL (optional) den Wert für die Anmelde-URL für das AWS Access Portal ein, den Sie im vorherigen Schritt kopiert haben (**`Step 3.1`**), wählen Sie Speichern und dann X aus, um das Fenster zu schließen.

6. Wenn Sie aufgefordert werden, Single Sign-On mit zu testenAWS IAM Identity Center, wählen Sie Nein, ich teste später. Sie werden diese Überprüfung in einem späteren Schritt durchführen.
7. Wählen Sie auf der Seite Single Sign-On mit SAML einrichten im Abschnitt SAML-Zertifikate neben Federation Metadata XML die Option Herunterladen aus, um die Metadatendatei auf Ihrem System zu speichern. Sie müssen diese Datei hochladen, wenn Sie im nächsten Schritt dazu aufgefordert werden.

Step 3.3 **>**

Schritt 3.3: Konfigurieren Sie den Microsoft Entra ID externen IdP in AWS IAM Identity Center

Hier kehren Sie zum Assistenten zum Ändern der Identitätsquelle in der IAM Identity Center-Konsole zurück, um die zweite Hälfte der SAML-Verbindung abzuschließen. AWS

1. Kehren Sie in der IAM Identity Center-Konsole zu der Browsersitzung zurück, die Sie geöffnet haben. **`Step 3.1`**
2. Klicken Sie auf der Seite Externen Identitätsanbieter konfigurieren im Abschnitt Identitätsanbieter-Metadaten unter IdP-SAML-Metadaten auf die Schaltfläche Datei auswählen, wählen Sie die Identitätsanbieter-Metadatendatei aus, aus der Sie Microsoft Entra ID im vorherigen Schritt heruntergeladen haben, und wählen Sie dann Öffnen aus.
3. Wählen Sie Weiter.
4. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ihn ein. **`ACCEPT`**
5. Wählen Sie Identitätsquelle ändern, um Ihre Änderungen zu übernehmen.

Step 3.4 **>**

Schritt 3.4: Testen Sie, ob Nikki zum AWS Zugangsportal weitergeleitet wird

In diesem Verfahren testen Sie die SAML-Verbindung, indem Sie sich mit den Anmeldeinformationen von Nikki beim My Account-Portal von Microsoft anmelden. Nach der Authentifizierung wählen Sie die AWS IAM Identity Center Anwendung aus, die Nikki zum Zugangsportal weiterleitet. AWS

1. Gehen Sie zur Anmeldeseite des Portals „Mein Konto“ und geben Sie die vollständige E-Mail-Adresse von Nikki ein. Zum Beispiel ***`NikkiWolf`***@ *`example.org`*.

2. Wenn Sie dazu aufgefordert werden, geben Sie Nikkis Passwort ein und wählen Sie dann Anmelden.
3. Wähle auf der Seite „Mein Konto“ in der linken Navigationsleiste „Meine Apps“ aus.
4. Wählen Sie auf der Seite Meine Apps die App mit dem Namen aus AWS IAM Identity Center. Dadurch sollten Sie zu einer zusätzlichen Authentifizierung aufgefordert werden.
5. Wählen Sie auf der Anmeldeseite von Microsoft Ihre NikkiWolf Anmeldeinformationen aus. Wenn Sie ein zweites Mal zur Authentifizierung aufgefordert werden, wählen Sie Ihre NikkiWolf Anmeldeinformationen erneut aus. Dadurch sollten Sie automatisch zum AWS Zugangsportal weitergeleitet werden.

   > **Tip**
   >
   > Wenn Sie nicht erfolgreich umgeleitet wurden, überprüfen Sie, ob der von Ihnen eingegebene Wert für die Anmelde-URL für das AWS Access Portal mit dem Wert **`Step 3.2`**übereinstimmt, von **`Step 3.1`**dem Sie kopiert haben.

6. Vergewissern Sie sich, dass ein AWSKontosymbol

   angezeigt wird.

   > **Tip**
   >
   > Wenn die Seite leer ist und kein AWSKontosymbol angezeigt wird, vergewissere dich, dass Nikki dem RegionalAdminBerechtigungssatz erfolgreich zugewiesen wurde (siehe **`Step 2.3`**).

Step 3.5

Schritt 3.5: Testen Sie Nikkis Zugriffsebene, um sie zu verwalten AWS-Konto

In diesem Schritt überprüfst du, ob Nikki Zugriffsrechte hat, um die Regionseinstellungen für sie zu verwalten. AWS-Konto Nikki sollte nur über ausreichende Administratorrechte verfügen, um Regionen von der Kontoseite aus zu verwalten.

1. Wählen Sie im AWS Zugangsportal das AWSKontosymbol,

um die Liste der Konten zu erweitern. Nachdem Sie das Symbol ausgewählt haben, werden die Kontonamen, Konto-IDs und E-Mail-Adressen aller Konten angezeigt, für die Sie Berechtigungssätze definiert haben.

2. Wählen Sie den Kontonamen (z. B. *Sandbox*), auf den Sie den Berechtigungssatz angewendet haben (siehe **Step 2.3**). Dadurch wird die Liste der Berechtigungssätze erweitert, aus denen Nikki für die Verwaltung ihres Kontos auswählen kann.
3. RegionalAdminWählen Sie als Nächstes die Verwaltungskonsole aus, um die Rolle anzunehmen, die Sie im RegionalAdminBerechtigungssatz definiert haben. Dadurch werden Sie zur AWS Management Console Startseite weitergeleitet.
4. Wählen Sie in der oberen rechten Ecke der Konsole Ihren Kontonamen und dann Konto aus. Dadurch gelangen Sie zur Kontoseite. Beachten Sie, dass in allen anderen Abschnitten auf dieser Seite eine Meldung angezeigt wird, dass Sie nicht über die erforderlichen Berechtigungen zum Anzeigen oder Ändern dieser Einstellungen verfügen.
5. Scrollen Sie auf der Kontoseite nach unten zum Abschnitt AWSRegionen. Wählen Sie ein Kontrollkästchen für jede verfügbare Region in der Tabelle aus. Beachten Sie, dass Nikki über die erforderlichen Berechtigungen verfügt, um die Liste der Regionen für ihr Konto wie vorgesehen zu aktivieren oder zu deaktivieren.

> Gut gemacht!
>
> Die Schritte 1 bis 3 haben Ihnen geholfen, Ihre SAML-Verbindung erfolgreich zu implementieren und zu testen. Um das Tutorial abzuschließen, empfehlen wir Ihnen, mit Schritt 4 fortzufahren, um die automatische Bereitstellung zu implementieren.

Schritt 4: Konfigurieren und testen Sie Ihre SCIM-Synchronisierung

In diesem Schritt richten Sie Microsoft Entra ID die automatische Bereitstellung (Synchronisation) von Benutzerinformationen aus dem IAM Identity Center mithilfe des SCIM v2.0-Protokolls ein. Sie konfigurieren diese Verbindung, Microsoft Entra ID indem Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Trägertoken verwenden, das automatisch von IAM Identity Center erstellt wird.

Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Microsoft Entra ID zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und überein. Microsoft Entra ID

In den folgenden Schritten erfahren Sie, wie Sie mithilfe der IAM Identity Center-App unter die automatische Bereitstellung von Benutzern aktivierenMicrosoft Entra ID, die hauptsächlich im IAM Identity Center ansässig sind. Microsoft Entra ID

Step 4.1 >

Schritt 4.1: Erstellen Sie einen zweiten Testbenutzer in Microsoft Entra ID

Zu Testzwecken erstellen Sie einen neuen Benutzer (Richard Roe) inMicrosoft Entra ID. Später, nachdem Sie die SCIM-Synchronisierung eingerichtet haben, werden Sie testen, ob dieser Benutzer und alle relevanten Attribute erfolgreich mit IAM Identity Center synchronisiert wurden.

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität > Benutzer > Alle Benutzer.
2. Wählen Sie Neuer Benutzer und dann oben auf dem Bildschirm Neuen Benutzer erstellen aus.
3. Geben Sie **`RichRoe`**im Feld Benutzerprinzipalname Ihre bevorzugte Domain und Erweiterung ein und wählen Sie sie aus. Zum Beispiel RichRoe@ *`example.org`*.
4. Geben **`RichRoe`**Sie im Feld Anzeigename den Wert ein.
5. Geben Sie unter Passwort ein sicheres Passwort ein oder klicken Sie auf das Augensymbol, um das automatisch generierte Passwort anzuzeigen, und kopieren Sie den angezeigten Wert entweder oder notieren Sie ihn.
6. Wählen Sie Eigenschaften und geben Sie dann die folgenden Werte ein:
   - Vorname — Geben Sie ein **`Richard`**
   - Nachname - Geben Sie ein **`Roe`**
   - Berufsbezeichnung - Geben Sie ein **`Marketing Lead`**
   - Abteilung — Geben Sie ein **`Sales`**
   - Mitarbeiter-ID — Geben Sie ein **`12345`**
7. Wählen Sie Überprüfen + Erstellen und dann Erstellen.

Step 4.2 >

Schritt 4.2: Aktivieren Sie die automatische Bereitstellung im IAM Identity Center

In diesem Verfahren verwenden Sie die IAM Identity Center-Konsole, um die automatische Bereitstellung von Benutzern und Gruppen zu aktivieren, die aus dem IAM Identity Center stammenMicrosoft Entra ID.

1. Öffnen Sie die IAM Identity Center-Konsole und wählen Sie im linken Navigationsbereich Einstellungen aus.
2. Beachten Sie auf der Seite Einstellungen unter dem Tab Identitätsquelle, dass die Bereitstellungsmethode auf Manuell eingestellt ist.
3. Suchen Sie das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird die automatische Bereitstellung im IAM Identity Center sofort aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten die einzelnen Werte für die folgenden Optionen. Sie müssen diese im nächsten Schritt einfügen, wenn Sie die Bereitstellung in konfigurieren. Microsoft Entra ID

   a. SCIM-Endpunkt — Zum Beispiel https://scim. *us-east-2 .amazonaws.com/ 111111111-2222-3333-4444-555555555555 /scim/v2/*

   b. Zugriffstoken — Wählen Sie Token anzeigen, um den Wert zu kopieren.
5. Klicken Sie auf Schließen.
6. Beachten Sie auf der Registerkarte Identitätsquelle, dass die Bereitstellungsmethode jetzt auf SCIM eingestellt ist.

Step 4.3 >

Schritt 4.3: Konfigurieren Sie die automatische Bereitstellung in Microsoft Entra ID

Nachdem Sie Ihren RichRoe Testbenutzer eingerichtet und SCIM im IAM Identity Center aktiviert haben, können Sie mit der Konfiguration der SCIM-Synchronisierungseinstellungen unter fortfahren. Microsoft Entra ID

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie AWS IAM Identity Centerdann.
2. Wählen Sie Provisioning und wählen Sie unter Verwalten erneut Provisioning aus.
3. Wählen Sie im Bereitstellungsmodus die Option Automatisch aus.

4. Fügen Sie unter Administratoranmeldedaten in das Feld Mandanten-URL den Wert für die SCIM-Endpunkt-URL ein, den Sie zuvor kopiert haben. **`Step 4.1`** Fügen Sie in Secret Token den Wert für das Zugriffstoken ein.
5. Wählen Sie Test Connection (Verbindung testen) aus. Es sollte eine Meldung angezeigt werden, die darauf hinweist, dass die getesteten Anmeldeinformationen erfolgreich autorisiert wurden, um die Bereitstellung zu aktivieren.
6. Wählen Sie Speichern aus.
7. Wählen Sie unter Verwalten die Option Benutzer und Gruppen und dann Benutzer/Gruppe hinzufügen aus.
8. Wählen Sie auf der Seite „Zuweisung hinzufügen“ unter Benutzer die Option Keine ausgewählt aus.
9. Wählen Sie RichRoeund wählen Sie dann Auswählen.
10. Wählen Sie auf der Seite Add Assignment (Zuweisung hinzufügen) Assign (Zuweisen) aus.
11. Wählen Sie Überblick und dann Bereitstellung starten aus.

Step 4.4

Schritt 4.4: Stellen Sie sicher, dass die Synchronisation stattgefunden hat

In diesem Abschnitt überprüfen Sie, ob Richards Benutzer erfolgreich bereitgestellt wurde und ob alle Attribute im IAM Identity Center angezeigt werden.

1. Wählen Sie in der IAM Identity Center-Konsole die Option Benutzer aus.
2. Auf der Seite „Benutzer“ sollte Ihr RichRoeBenutzer angezeigt werden. Beachten Sie, dass in der Spalte Erstellt von der Wert auf SCIM gesetzt ist.
3. Stellen Sie RichRoeunter Profil sicher, dass die folgenden Attribute von Microsoft Entra ID kopiert wurden.
   - Vorname - **`Richard`**
   - Nachname - **`Roe`**
   - Abteilung - **`Sales`**
   - Titel - **`Marketing Lead`**
   - Mitarbeiternummer - **`12345`**

Nachdem Richards Benutzer nun in IAM Identity Center erstellt wurde, können Sie ihn einem beliebigen Berechtigungssatz zuweisen, sodass Sie kontrollieren können, welche Zugriffsebene er auf Ihre AWS Ressourcen hat. Sie könnten beispielsweise dem **`RegionalAdmin`** Berechtigungssatz, den Sie zuvor verwendet haben, um Nikki die Berechtigungen zur Verwaltung von Regionen zu gewähren (siehe **`Step 2.3`**), zuweisen RichRoeund dann seine Zugriffsebene damit testen. **`Step 3.5`**

> **Herzlichen Glückwunsch!**
>
> Sie haben erfolgreich eine SAML-Verbindung zwischen Microsoft und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert, um alles synchron zu halten. Jetzt können Sie das Gelernte anwenden, um Ihre Produktionsumgebung reibungsloser einzurichten.

Überlegungen zur Verwendung von SCIM Microsoft Entra ID in einer Produktionsumgebung

Im Folgenden finden Sie wichtige ÜberlegungenMicrosoft Entra ID, die sich darauf auswirken können, wie Sie die automatische Bereitstellung mit IAM Identity Center in Ihrer Produktionsumgebung mithilfe des SCIM v2-Protokolls implementieren möchten.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, sich zunächst mit diesem Thema vertraut zu machen. Überlegungen zur Verwendung der automatischen Bereitstellung

Attribute für die Zugriffskontrolle

Attribute für die Zugriffskontrolle werden in Berechtigungsrichtlinien verwendet, die festlegen, wer in Ihrer Identitätsquelle auf Ihre AWS Ressourcen zugreifen kann. Wenn ein Attribut von einem Benutzer in entfernt wirdMicrosoft Entra ID, wird dieses Attribut nicht aus dem entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung inMicrosoft Entra ID. Wenn ein Attribut für einen Benutzer in einen anderen (nicht leeren) Wert geändert wird, wird diese Änderung mit IAM Identity Center synchronisiert.

Verschachtelte Gruppen

Der Microsoft Entra ID Benutzerbereitstellungsdienst kann Benutzer in verschachtelten Gruppen nicht lesen oder bereitstellen. Nur Benutzer, die unmittelbare Mitglieder einer explizit zugewiesenen Gruppe sind, können gelesen und Zugriffsberechtigungen zugewiesen werden. Microsoft Entra IDentpackt nicht rekursiv die Gruppenmitgliedschaften indirekt zugewiesener Benutzer oder Gruppen (Benutzer oder Gruppen, die Mitglieder einer direkt zugewiesenen Gruppe sind). Weitere Informationen finden Sie in der Dokumentation unter Zuweisungsbasiertes Scoping. Microsoft Entra ID

Dynamische Gruppen

Der Microsoft Entra ID Benutzerbereitstellungsdienst kann Benutzer in dynamischen Gruppen lesen und bereitstellen. Im Folgenden finden Sie ein Beispiel, das die Benutzer- und Gruppenstruktur bei der Verwendung dynamischer Gruppen und deren Anzeige im IAM Identity Center zeigt. Diese Benutzer und Gruppen wurden über SCIM aus dem Microsoft Entra ID IAM Identity Center bereitgestellt

Wenn die Microsoft Entra ID Struktur für dynamische Gruppen beispielsweise wie folgt aussieht:

1. Gruppe A mit den Mitgliedern ua1, ua2
2. Gruppe B mit Mitgliedern ub1
3. Gruppe C mit Mitgliedern uc1
4. Gruppe K mit der Regel, Mitglieder der Gruppe A, B, C einzubeziehen
5. Gruppe L mit einer Regel, die Mitglieder der Gruppen B und C einschließt

Nachdem die Benutzer- und Gruppeninformationen über SCIM aus dem Microsoft Entra ID IAM Identity Center bereitgestellt wurden, sieht die Struktur wie folgt aus:

1. Gruppe A mit den Mitgliedern ua1, ua2
2. Gruppe B mit Mitgliedern ub1
3. Gruppe C mit Mitgliedern uc1
4. Gruppe K mit den Mitgliedern ua1, ua2, ub1, uc1
5. Gruppe L mit den Mitgliedern ub1, uc1

Beachten Sie bei der Konfiguration der automatischen Bereitstellung mithilfe dynamischer Gruppen die folgenden Überlegungen.

- Eine dynamische Gruppe kann eine verschachtelte Gruppe enthalten. Der Microsoft Entra ID Provisioning Service reduziert die verschachtelte Gruppe jedoch nicht. Wenn Sie beispielsweise die folgende Microsoft Entra ID Struktur für dynamische Gruppen haben:
  - Gruppe A ist der Gruppe B übergeordnet.
  - Gruppe A hat ua1 als Mitglied.
  - Gruppe B hat ub1 als Mitglied.

Die dynamische Gruppe, zu der Gruppe A gehört, umfasst nur die direkten Mitglieder der Gruppe A (d. h. ua1). Sie schließt nicht rekursiv Mitglieder der Gruppe B ein.

- Dynamische Gruppen können keine anderen dynamischen Gruppen enthalten. Weitere Informationen finden Sie in der Microsoft Entra ID Dokumentation unter Einschränkungen der Vorschauversion.

Behebung von SCIM-Problemen mit Microsoft Entra ID

Wenn Sie Probleme mit Microsoft Entra ID Benutzern haben, die sich nicht mit IAM Identity Center synchronisieren, liegt das möglicherweise an einem Syntaxproblem, das IAM Identity Center gemeldet hat, wenn ein neuer Benutzer zu IAM Identity Center hinzugefügt wird. Sie können dies überprüfen, indem Sie in den Microsoft Entra ID Audit-Logs nach fehlgeschlagenen Ereignissen suchen, wie z. B. `'Export'` Der Statusgrund für dieses Ereignis lautet wie folgt:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Sie können auch AWS CloudTrail nach dem fehlgeschlagenen Ereignis suchen. Suchen Sie dazu in der Konsole „Event History“ oder CloudTrail verwenden Sie den folgenden Filter:

```
"eventName":"CreateUser"
```

Der Fehler in der CloudTrail Veranstaltung wird Folgendes bedeuten:

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

Letztlich bedeutet diese Ausnahme, dass einer der übergebenen Werte mehr Werte als erwartet Microsoft Entra ID enthielt. Die Lösung besteht darin, die Attribute des Benutzers zu überprüfen

und sicherzustellenMicrosoft Entra ID, dass keine doppelten Werte enthalten. Ein häufiges Beispiel für doppelte Werte ist das Vorhandensein mehrerer Werte für Kontaktnummern wie Handy -, Geschäfts - und Faxnummern. Obwohl sie separate Werte sind, werden sie alle unter dem einzigen übergeordneten Attribut PhoneNumbers an das IAM Identity Center übergeben.

Allgemeine Tipps zur SCIM-Fehlerbehebung finden Sie unter. Behebung von Problemen mit IAM Identity Center

Schritt 5: (Optional) ABAC konfigurieren

Nachdem Sie SAML und SCIM erfolgreich konfiguriert haben, können Sie optional die attributebasierte Zugriffskontrolle (ABAC) konfigurieren. ABAC ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert.

Mit können Sie eine der folgenden beiden Methoden verwendenMicrosoft Entra ID, um ABAC für die Verwendung mit IAM Identity Center zu konfigurieren.

Method 1

Methode 1: Konfigurieren Sie Benutzerattribute Microsoft Entra ID für die Zugriffskontrolle in IAM Identity Center

Im folgenden Verfahren legen Sie fest, welche Attribute von IAM Identity Center zur Verwaltung des Zugriffs auf Ihre AWS Ressourcen verwendet werden Microsoft Entra ID sollen. Nach der Definition werden diese Attribute über SAML-Assertionen an IAM Identity Center Microsoft Entra ID gesendet. Anschließend müssen Sie Berechtigungssatz erstellen im IAM Identity Center den Zugriff auf der Grundlage der Attribute verwalten, von denen Sie die Daten übergeben haben. Microsoft Entra ID

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zunächst die Attribute für Zugriffskontrolle Funktion aktivieren. Weitere Information dazu finden Sie unter Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle.

1. Navigieren Sie in der Microsoft Entra Admin Center-Konsole zu Identität > Anwendungen > Unternehmensanwendungen und wählen Sie AWS IAM Identity Centerdann.
2. Klicken Sie auf Single Sign-On.
3. Wählen Sie im Abschnitt Attribute und Ansprüche die Option Bearbeiten aus.
4. Gehen Sie auf der Seite „Attribute und Ansprüche“ wie folgt vor:

a. Wählen Sie Neuen Anspruch hinzufügen

b. Geben Sie unter Name `AccessControl:`*`AttributeName`* ein. *`AttributeName`*Ersetzen Sie es durch den Namen des Attributs, das Sie in IAM Identity Center erwarten. Zum Beispiel `AccessControl:`**`Department`**.

c. Geben Sie für Namespace **`https://aws.amazon.com/SAML/Attributes`** ein.

d. Wählen Sie unter Source (Quelle) die Option Attribute (Attribut) aus.

e. Verwenden Sie für das Quellattribut die Drop-down-Liste, um die Microsoft Entra ID Benutzerattribute auszuwählen. Zum Beispiel `user.`**`department`**.

5. Wiederholen Sie den vorherigen Schritt für jedes Attribut, das Sie in der SAML-Assertion an das IAM Identity Center senden müssen.
6. Wählen Sie Speichern aus.

Method 2

Methode 2: Konfigurieren Sie ABAC mithilfe von IAM Identity Center

Bei dieser Methode verwenden Sie die Attribute für Zugriffskontrolle Funktion in IAM Identity Center, um ein `Attribute` Element zu übergeben, dessen `Name` Attribut auf gesetzt ist. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Sie können dieses Element verwenden, um Attribute als Sitzungs-Tags in der SAML-Assertion zu übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Sitzungs-Tags übergeben AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben:

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates `Attribute` Element hinzu.

Konfiguration von SAML und SCIM mit einem IAM Okta Identity Center

Mithilfe des SCIM-Protokolls (System for Cross-Domain Identity Management) v2.0 Okta können Sie Benutzer- und Gruppeninformationen automatisch aus dem IAM Identity Center bereitstellen (synchronisieren). Um diese Verbindung zu konfigurierenOkta, verwenden Sie Ihren SCIM-Endpunkt für IAM Identity Center und ein Trägertoken, das automatisch von IAM Identity Center erstellt wird. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute Okta zu den benannten Attributen in IAM Identity Center. Diese Zuordnung entspricht den erwarteten Benutzerattributen zwischen IAM Identity Center und Ihren. Okta

Oktaunterstützt die folgenden Bereitstellungsfunktionen, wenn Sie über SCIM mit IAM Identity Center verbunden sind:

- Benutzer erstellen — Benutzer, die der IAM Identity Center-Anwendung in zugewiesen Okta sind, werden in IAM Identity Center bereitgestellt.
- Benutzerattribute aktualisieren — Attributänderungen für Benutzer, die der IAM Identity Center-Anwendung in zugewiesen sind, Okta werden in IAM Identity Center aktualisiert.
- Benutzer deaktivieren — Benutzer, denen die Zuweisung zur IAM Identity Center-Anwendung in aufgehoben wurde, Okta sind in IAM Identity Center deaktiviert.
- Gruppen-Push — Gruppen (und ihre Mitglieder) Okta werden mit IAM Identity Center synchronisiert.

> **Note**
>
> Um den Verwaltungsaufwand Okta sowohl in IAM Identity Center als auch in IAM Identity Center zu minimieren, empfehlen wir, Gruppen zuzuweisen und zu pushen, anstatt einzelne Benutzer zu verwenden.

Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter. Aktivieren AWS IAM Identity Center

Zielsetzung

In diesem Tutorial werden Sie Schritt für Schritt die Einrichtung einer SAML-Verbindung mit Okta IAM Identity Center beschrieben. Später werden Sie Benutzer mithilfe von Okta SCIM synchronisieren. In

diesem Szenario verwalten Sie alle Benutzer und Gruppen inOkta. Benutzer melden sich über das Okta Portal an. Um zu überprüfen, ob alles korrekt konfiguriert ist, melden Sie sich nach Abschluss der Konfigurationsschritte als Okta Benutzer an und verifizieren den Zugriff auf AWS Ressourcen.

> **Note**
>
> Sie können sich für ein Okta Konto (kostenlose Testversion) registrieren, auf dem die Okta's IAM Identity Center-Anwendung installiert ist. Bei kostenpflichtigen Okta Produkten müssen Sie möglicherweise bestätigen, dass Ihre Okta Lizenz das Lebenszyklusmanagement oder ähnliche Funktionen unterstützt, die die Bereitstellung ausgehender Daten ermöglichen. Diese Funktionen sind möglicherweise erforderlich, um SCIM von zu IAM Identity Center Okta zu konfigurieren.

Bevor Sie beginnen

Bevor Sie die SCIM-Bereitstellung zwischen Okta und IAM Identity Center konfigurieren, empfehlen wir Ihnen, dies zunächst zu überprüfen. Überlegungen zur Verwendung der automatischen Bereitstellung

Bestätigen Sie die folgenden Punkte, bevor Sie beginnen:

- Für jeden Okta Benutzer müssen die Werte Vorname, Nachname, Benutzername und Anzeigename angegeben werden.
- Jeder Okta Benutzer hat nur einen einzigen Wert pro Datenattribut, z. B. E-Mail-Adresse oder Telefonnummer. Alle Benutzer mit mehreren Werten können nicht synchronisiert werden. Wenn es Benutzer gibt, deren Attribute mehrere Werte enthalten, entfernen Sie die doppelten Attribute, bevor Sie versuchen, den Benutzer in IAM Identity Center bereitzustellen. Beispielsweise kann nur ein Telefonnummernattribut synchronisiert werden, da das Standard-Telefonnummernattribut „Geschäftstelefon“ ist. Verwenden Sie das Attribut „Geschäftstelefon“, um die Telefonnummer des Benutzers zu speichern, auch wenn es sich bei der Telefonnummer des Benutzers um ein Festnetz oder ein Mobiltelefon handelt.
- Wenn Sie die Adresse eines Benutzers aktualisieren, müssen Sie die Werte StreetAddress, City, State, ZipCode und CountryCode angeben. Wenn einer dieser Werte für den Okta Benutzer zum Zeitpunkt der Synchronisation nicht angegeben wurde, wird der Benutzer (oder Änderungen am Benutzer) nicht bereitgestellt.

> **Note**
>
> Berechtigungen und Rollenattribute werden nicht unterstützt und können nicht mit IAM Identity Center synchronisiert werden.
> Die Verwendung derselben Okta Gruppe für Aufgaben und Gruppen-Push wird derzeit nicht unterstützt. Um konsistente Gruppenmitgliedschaften zwischen Okta und IAM Identity Center aufrechtzuerhalten, erstellen Sie eine separate Gruppe und konfigurieren Sie sie so, dass Gruppen per Push an IAM Identity Center weitergeleitet werden.

Schritt 1: Rufen Sie die SAML-Metadaten von Ihrem Konto ab Okta

1. Melden Sie sich bei anOkta admin dashboard, erweitern Sie Anwendungen und wählen Sie dann Anwendungen aus.
2. Wählen Sie auf der Seite Applications (Anwendungen) die Option Browse App Catalog (App-Katalog durchsuchen) aus.
3. Geben Sie in das Suchfeld die App ein AWS IAM Identity Centerund wählen Sie sie aus, um die IAM Identity Center-App hinzuzufügen.
4. Wählen Sie den Tab Anmelden aus.
5. Wählen Sie unter SAML-Signaturzertifikate die Option Aktionen und dann IdP-Metadaten anzeigen aus. Ein neuer Browser-Tab mit der Dokumentenstruktur einer XML-Datei wird geöffnet. Wählen Sie das gesamte XML von `<md:EntityDescriptor>` bis aus `</md:EntityDescriptor>` und kopieren Sie es in eine Textdatei.
6. Speichern Sie die Textdatei unter`metadata.xml`.

Lassen Sie das Fenster Okta admin dashboard geöffnet, Sie werden diese Konsole in den späteren Schritten weiter verwenden.

Schritt 2: Okta Als Identitätsquelle für IAM Identity Center konfigurieren

1. Öffnen Sie die IAM Identity Center-Konsole als Benutzer mit Administratorrechten.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Wählen Sie auf der Seite Einstellungen die Option Aktionen und dann Identitätsquelle ändern aus.

4. Wählen Sie unter Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.
5. Gehen Sie unter Externen Identitätsanbieter konfigurieren wie folgt vor:

   a. Wählen Sie unter Metadaten des Dienstanbieters die Option Metadatendatei herunterladen aus, um die IAM Identity Center-Metadatendatei herunterzuladen und auf Ihrem System zu speichern. Sie werden die SAML-Metadatendatei für IAM Identity Center Okta später in diesem Tutorial bereitstellen.

      Kopieren Sie die folgenden Elemente in eine Textdatei, um den Zugriff zu erleichtern:

      - URL des IAM Identity Center Assertion Consumer Service (ACS)
      - URL des IAM Identity Center-Ausstellers

      Sie benötigen diese Werte später in diesem Tutorial.

   b. Wählen Sie unter Identitätsanbieter-Metadaten unter IdP SAML-Meta die Option Datei auswählen und wählen Sie dann die `metadata.xml` Datei aus, die Sie im vorherigen Schritt erstellt haben.

   c. Wählen Sie Weiter aus.
6. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
7. Wählen Sie Identitätsquelle ändern aus.

   Lassen Sie die AWS Konsole geöffnet, Sie werden diese Konsole im nächsten Schritt weiter verwenden.
8. Kehren Sie zur AWS IAM Identity Center App zurück Okta admin dashboard und wählen Sie die Registerkarte Anmelden aus. Klicken Sie dann auf Bearbeiten.
9. Geben Sie unter Erweiterte Anmeldeeinstellungen Folgendes ein:

   - Geben Sie für ACS-URL den Wert ein, den Sie für die IAM Identity Center Assertion Consumer Service (ACS) -URL kopiert haben
   - Geben Sie für Issuer URL den Wert ein, den Sie für IAM Identity Center Issuer URL kopiert haben
   - Wählen Sie für das Format des Anwendungsbenutzernamens eine der Optionen aus dem Drop-down-Menü aus.

Stellen Sie sicher, dass der von Ihnen gewählte Wert für jeden Benutzer einzigartig ist. Wählen Sie für dieses Tutorial den Okta-Benutzernamen

10. Wählen Sie Speichern.

Sie sind jetzt bereit, Benutzer vom IAM Identity Center aus Okta bereitzustellen. Lassen Sie das Okta admin dashboard Fenster geöffnet und kehren Sie für den nächsten Schritt zur IAM Identity Center-Konsole zurück.

Schritt 3: So stellen Sie Benutzer bereit von Okta

1. Suchen Sie in der IAM Identity Center-Konsole auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpunkt- und Zugriffstoken-Informationen angezeigt.
2. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten die einzelnen Werte für die folgenden Optionen:

   - SCIM-Endpunkt
   - Zugriffstoken

   Später in diesem Tutorial werden Sie diese Werte eingeben, um die Bereitstellung zu konfigurieren. Okta
3. Klicken Sie auf Schließen.
4. Kehren Sie zur IAM Identity Center App zurück Okta admin dashboard und navigieren Sie zur App.
5. Wählen Sie auf der Seite der IAM Identity Center-App den Tab Provisioning und wählen Sie dann in der linken Navigationsleiste unter Einstellungen die Option Integration aus.
6. Wählen Sie Bearbeiten und aktivieren Sie dann das Kontrollkästchen neben API-Integration aktivieren, um die Bereitstellung zu aktivieren.
7. Verwenden Sie für die Konfiguration Okta die SCIM-Bereitstellungswerte aus dem IAM Identity Center, die Sie zuvor in diesem Tutorial kopiert haben:

   a. Geben Sie im Feld Basis-URL den SCIM-Endpunktwert ein. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen.
   b. Geben Sie im Feld API-Token den Wert für das Zugriffstoken ein.

8. Wählen Sie API-Anmeldeinformationen testen, um zu überprüfen, ob die eingegebenen Anmeldeinformationen gültig sind.

   Die Nachricht AWS IAM Identity Center wurde erfolgreich verifiziert! zeigt an.

9. Wählen Sie Speichern. Sie werden zum Bereich Einstellungen weitergeleitet, in dem Integration ausgewählt ist.
10. Wählen Sie unter Einstellungen die Option Zur App aus und aktivieren Sie dann das Kontrollkästchen Aktivieren für jede der Funktionen von Provisioning to App, die Sie aktivieren möchten. Wählen Sie für dieses Tutorial alle Optionen aus.
11. Wählen Sie Speichern.

Sie sind jetzt bereit, Ihre Benutzer Okta mit IAM Identity Center zu synchronisieren.

Schritt 4: Synchronisieren Sie Benutzer Okta mit IAM Identity Center

Standardmäßig sind Ihrer Okta IAM Identity Center-App keine Gruppen oder Benutzer zugewiesen. Durch die Bereitstellung von Gruppen werden die Benutzer bereitgestellt, die Mitglieder der Gruppe sind. Gehen Sie wie folgt vor, um Gruppen und Benutzer mit IAM Identity Center zu synchronisieren.

1. Wählen Sie auf der Seite der OktaIAM Identity Center-App den Tab Zuweisungen aus. Sie können der IAM Identity Center-App sowohl Personen als auch Gruppen zuweisen.

   a. So weisen Sie Personen zu:

      - Wählen Sie auf der Seite „Aufgaben“ die Option „Zuweisen“ und dann „Personen zuweisen“ aus.
      - Wählen Sie die Okta Benutzer aus, die Zugriff auf die IAM Identity Center-App haben sollen. Wählen Sie „Zuweisen“, „Speichern und Zurück“ und anschließend „Fertig“.

      Dadurch wird der Prozess der Bereitstellung der Benutzer für IAM Identity Center gestartet.

   b. Um Gruppen zuzuweisen:

      - Wählen Sie auf der Seite „Zuweisungen“ die Option „Zuweisen“ und anschließend „Gruppen zuweisen“.
      - Wählen Sie die Okta Gruppen aus, für die Sie Zugriff auf die IAM Identity Center-App haben möchten. Wählen Sie „Zuweisen“, „Speichern und Zurück“ und anschließend „Fertig“.

Dadurch wird der Prozess der Bereitstellung der Benutzer in der Gruppe für IAM Identity Center gestartet.

> **Note**
>
> Möglicherweise müssen Sie zusätzliche Attribute für die Gruppe angeben, wenn diese nicht in allen Benutzerdatensätzen vorhanden sind. Die für die Gruppe angegebenen Attribute überschreiben alle individuellen Attributwerte.

2. Wählen Sie die Registerkarte Push-Gruppen. Wählen Sie die Okta Gruppe aus, die alle Gruppen enthält, die Sie der IAM Identity Center-App zugewiesen haben. Wählen Sie Speichern.

   Der Gruppenstatus ändert sich in Aktiv, nachdem die Gruppe und ihre Mitglieder per Push an das IAM Identity Center weitergeleitet wurden.

3. Kehren Sie zur Registerkarte „Zuweisungen“ zurück.

4. Wenn Sie Benutzer haben, die nicht Mitglieder der Gruppen sind, die Sie per Push an IAM Identity Center weitergeleitet haben, fügen Sie sie einzeln hinzu. Gehen Sie dazu wie folgt vor:

   Wählen Sie auf der Seite „Zuweisungen“ die Option „Zuweisen“ und anschließend „Personen zuweisen“.

5. Wählen Sie die Okta Benutzer aus, die Zugriff auf die IAM Identity Center-App haben sollen. Wählen Sie „Zuweisen“, „Speichern und Zurück“ und anschließend „Fertig“.

   Damit wird der Prozess der Bereitstellung der einzelnen Benutzer für IAM Identity Center gestartet.

   > **Note**
   >
   > Sie können der AWS IAM Identity Center App auch Benutzer und Gruppen zuweisen, und zwar auf der Anwendungsseite von. Okta admin dashboard Wählen Sie dazu das Einstellungssymbol aus und wählen Sie dann Benutzern zuweisen oder Zu Gruppen zuweisen und geben Sie dann den Benutzer oder die Gruppe an.

6. Kehren Sie zur IAM Identity Center-Konsole zurück. Wählen Sie in der linken Navigationsleiste Benutzer aus. Sie sollten die Benutzerliste mit Ihren Okta Benutzern sehen.

Herzlichen Glückwunsch!

Sie haben erfolgreich eine SAML-Verbindung zwischen Okta und eingerichtet AWS und sich vergewissert, dass die automatische Bereitstellung funktioniert. Sie können diese Benutzer jetzt Konten und Anwendungen in IAM Identity Center zuweisen. Für dieses Tutorial bestimmen wir im nächsten Schritt einen der Benutzer als IAM Identity Center-Administrator, indem wir ihm Administratorrechte für das Verwaltungskonto gewähren.

Schritt 5: Okta Benutzern Zugriff auf Konten gewähren

1. Wählen Sie im Navigationsbereich von IAM Identity Center unter Berechtigungen für mehrere Konten die Option. AWS-Konten
2. Auf der AWS-KontenSeite „Organisationsstruktur“ wird Ihr Organisationsstamm mit Ihren Konten darunter in der Hierarchie angezeigt. Markieren Sie das Kontrollkästchen für Ihr Verwaltungskonto und wählen Sie dann Benutzer oder Gruppen zuweisen aus.
3. Der Workflow „Benutzer und Gruppen zuweisen“ wird angezeigt. Er besteht aus drei Schritten:

    a. Wählen Sie für Schritt 1: Benutzer und Gruppen auswählen den Benutzer aus, der die Administratorfunktion ausführen soll. Wählen Sie anschließend Weiter.

    b. Wählen Sie für Schritt 2: Berechtigungssätze auswählen die Option Berechtigungssatz erstellen aus, um eine neue Registerkarte zu öffnen, die Sie durch die drei Teilschritte zur Erstellung eines Berechtigungssatzes führt.

        i. Gehen Sie für Schritt 1: Berechtigungssatztyp auswählen wie folgt vor:

            - Wählen Sie unter Typ des Berechtigungssatzes die Option Vordefinierter Berechtigungssatz aus.
            - Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz die Option aus AdministratorAccess.

            Wählen Sie Weiter aus.

        ii. Für Schritt 2: Geben Sie Details zum Berechtigungssatz an, behalten Sie die Standardeinstellungen bei und wählen Sie Weiter aus.

            Mit den Standardeinstellungen wird ein Berechtigungssatz *`AdministratorAccess`*mit einem Namen erstellt, dessen Sitzungsdauer auf eine Stunde festgelegt ist.

iii. Stellen Sie für Schritt 3: Überprüfen und erstellen sicher, dass der Typ Berechtigungssatz die AWS verwaltete Richtlinie verwendet AdministratorAccess. Wählen Sie Erstellen. Auf der Seite Berechtigungssätze wird eine Benachrichtigung angezeigt, die Sie darüber informiert, dass der Berechtigungssatz erstellt wurde. Sie können diese Registerkarte jetzt in Ihrem Webbrowser schließen.

Auf der Browser-Registerkarte Benutzer und Gruppen zuweisen befinden Sie sich immer noch in Schritt 2: Wählen Sie die Berechtigungssätze aus, von denen aus Sie den Workflow zum Erstellen von Berechtigungssätzen gestartet haben.

Wählen Sie im Bereich „Berechtigungssätze“ die Schaltfläche „Aktualisieren“. Der von Ihnen erstellte *`AdministratorAccess`*Berechtigungssatz wird in der Liste angezeigt. Aktivieren Sie das Kontrollkästchen für diesen Berechtigungssatz und wählen Sie dann Weiter.

c. Überprüfen Sie für Schritt 3: Überprüfen und Absenden den ausgewählten Benutzer und den ausgewählten Berechtigungssatz und wählen Sie dann Senden aus.

Die Seite wird mit der Meldung aktualisiert, dass Ihr AWS-Konto System gerade konfiguriert wird. Warten Sie, bis der Vorgang abgeschlossen ist.

Sie kehren zur AWS-Konten Seite zurück. In einer Benachrichtigung werden Sie darüber informiert, dass Ihr AWS-Konto Konto erneut bereitgestellt und der aktualisierte Berechtigungssatz angewendet wurde. Wenn sich der Benutzer anmeldet, hat er die Möglichkeit, die Rolle auszuwählen. *`AdministratorAccess`*

> **Note**
>
> Die automatische SCIM-Synchronisierung von unterstützt Okta nur die Bereitstellung von Benutzern. Gruppen werden nicht automatisch bereitgestellt. Mit dem können Sie keine Gruppen für Ihre Okta Benutzer erstellen. AWS Management Console Nach der Bereitstellung von Benutzern können Sie Gruppen mithilfe einer CLI- oder API-Operation erstellen

Schritt 6: Bestätigen Sie den Okta Benutzerzugriff auf Ressourcen AWS

1. Melden Sie sich Okta dashboard mit einem Testbenutzerkonto an.
2. Wählen Sie unter Meine Apps das AWS IAM Identity Center Symbol aus.

3. Sie sind im Portal angemeldet und können das AWS-Konto Symbol sehen. Erweitern Sie dieses Symbol, um die Liste der Symbole anzuzeigen AWS-Konten , auf die der Benutzer zugreifen kann. In diesem Tutorial haben Sie nur mit einem einzigen Konto gearbeitet, sodass beim Erweitern des Symbols nur ein Konto angezeigt wird.
4. Wählen Sie das Konto aus, um die für den Benutzer verfügbaren Berechtigungssätze anzuzeigen. In diesem Tutorial haben Sie den AdministratorAccessBerechtigungssatz erstellt.
5. Neben dem Berechtigungssatz befinden sich Links für den Zugriffstyp, der für diesen Berechtigungssatz verfügbar ist. Bei der Erstellung des Berechtigungssatzes haben Sie angegeben, dass sowohl die Verwaltungskonsole als auch der programmgesteuerte Zugriff aktiviert werden sollen, sodass diese beiden Optionen verfügbar sind. Wählen Sie Managementkonsole aus, um die zu öffnen. AWS Management Console
6. Der Benutzer ist an der Konsole angemeldet.

(Optional) Übergabe von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein `Attribute` Element zu übergeben, dessen `Name` Attribut auf `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` gesetzt ist. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie AWS STS im IAM-Benutzerhandbuch unter Sitzungs-Tags übergeben.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Verwenden Sie beispielsweise das folgende Attribut, um das Schlüssel-Wert-Paar `CostCenter = blue` für das Tag zu übergeben.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates `Attribute` Element hinzu.

Nächste Schritte

Nachdem Sie nun Okta als Identitätsanbieter konfiguriert und Benutzer in IAM Identity Center bereitgestellt haben, können Sie:

- Zugriff gewähren auf AWS-Konten, siehe. Weisen Sie Benutzerzugriff zu AWS-Konten
- Zugriff auf Cloud-Anwendungen gewähren, sieheWeisen Sie Benutzerzugriff auf Anwendungen in der IAM Identity Center-Konsole zu.
- Konfigurieren Sie Berechtigungen auf der Grundlage von Aufgabenfunktionen, siehe Einen Berechtigungssatz erstellen

Einrichten der SCIM-Bereitstellung zwischen OneLogin und IAM Identity Center

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisierung) von Benutzer- und Gruppeninformationen von OneLogin in IAM Identity Center mithilfe des Systems for Cross-Domain Identity Management (SCIM) v2.0-Protokolls. Sie konfigurieren diese Verbindung in unter OneLoginVerwendung Ihres SCIM-Endpunkts für IAM Identity Center und eines Bearer-Tokens, das automatisch von IAM Identity Center erstellt wird. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute in OneLogin zu den benannten Attributen in IAM Identity Center. Dies führt dazu, dass die erwarteten Attribute zwischen IAM Identity Center und übereinstimmenOneLogin.

Die folgenden Schritte führen Sie durch die Aktivierung der automatischen Bereitstellung von Benutzern und Gruppen von OneLogin an IAM Identity Center mithilfe des SCIM-Protokolls.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu überprüfenÜberlegungen zur Verwendung der automatischen Bereitstellung.

Themen

- (Optional) Schritt 3: Konfigurieren von Benutzerattributen in OneLogin für die Zugriffskontrolle in IAM Identity Center
- (Optional) Übergeben von Attributen für die Zugriffskontrolle
- Fehlerbehebung

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- Ein -OneLoginKonto. Wenn Sie noch kein -Konto haben, können Sie möglicherweise eine kostenlose Testversion oder ein Entwicklerkonto von der OneLogin Website erhalten.
- Ein IAM-Identity-Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Eine SAML-Verbindung von Ihrem OneLogin Konto zu IAM Identity Center. Weitere Informationen finden Sie unter Aktivieren von Single Sign-On zwischen OneLogin und AWS im -AWSPartnernetzwerk-Blog.

Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM-Identity-Center-Konsole, um die automatische Bereitstellung zu aktivieren.

So aktivieren Sie die automatische Bereitstellung in IAM Identity Center

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Feld Informationen zur automatischen Bereitstellung und wählen Sie dann Aktivieren aus. Dies aktiviert sofort die automatische Bereitstellung im IAM Identity Center und zeigt die erforderlichen SCIM-Endpunkt- und Zugriffstokeninformationen an.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehenden Datenverkehr jeden der Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
    a. SCIM-Endpunkt
    b. Zugriffstoken
5. Klicken Sie auf Schließen.

Sie haben jetzt die Bereitstellung in der IAM-Identity-Center-Konsole eingerichtet. Jetzt müssen Sie die verbleibenden Aufgaben mit der OneLogin Admin-Konsole ausführen, wie im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren der Bereitstellung in OneLogin

Gehen Sie wie folgt in der OneLogin Administratorkonsole vor, um die Integration zwischen IAM Identity Center und der IAM-Identity-Center-App zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die AWS Single-Sign-On-Anwendung bereits in OneLogin für die SAML-Authentifizierung konfiguriert haben. Wenn Sie diese SAML-Verbindung noch nicht erstellt haben, tun Sie dies, bevor Sie fortfahren, und kehren Sie dann hier zurück, um den SCIM-Bereitstellungsprozess abzuschließen. Weitere Informationen zur Konfiguration von SAML mit OneLoginfinden Sie unter Aktivieren von Single Sign-On zwischen OneLogin und AWS im -AWSPartnernetzwerk-Blog.

So konfigurieren Sie die Bereitstellung in OneLogin

1. Melden Sie sich bei an OneLoginund navigieren Sie dann zu Anwendungen > Anwendungen.
2. Suchen Sie auf der Seite Anwendungen nach der Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen. Wählen Sie es aus und wählen Sie dann in der linken Navigationsleiste Konfiguration aus.
3. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM-Basis-URL in einOneLogin. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen. Außerdem haben Sie im vorherigen Verfahren den Wert für das Zugriffstoken in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld SCIM Bearer Token in einOneLogin.
4. Klicken Sie neben API Connection auf Enable und anschließend auf Save, um die Konfiguration abzuschließen.
5. Wählen Sie in der linken Navigationsleiste Provisioning aus.
6. Aktivieren Sie die Kontrollkästchen für Bereitstellung aktivieren, Benutzer erstellen, Benutzer löschen und Benutzer aktualisieren und wählen Sie dann Speichern aus.
7. Wählen Sie in der linken Navigationsleiste Benutzer aus.
8. Klicken Sie auf Weitere Aktionen und wählen Sie Anmeldeinformationen synchronisieren aus. Sie sollten die Meldung Synchronisieren von Benutzern mit AWS Single Sign-On erhalten.
9. Klicken Sie erneut auf Weitere Aktionen und wählen Sie dann erneut Berechtigungszuordnungen anwenden aus. Sie sollten die Meldung Mappings werden erneut angewendet erhalten.

10. Zu diesem Zeitpunkt sollte der Bereitstellungsprozess beginnen. Um dies zu bestätigen, navigieren Sie zu Aktivität > Ereignisse und überwachen Sie den Fortschritt. Erfolgreiche Bereitstellungsereignisse sowie Fehler sollten im Ereignisstream angezeigt werden.
11. Um zu überprüfen, ob Ihre Benutzer und Gruppen alle erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM-Identity-Center-Konsole zurück und wählen Sie Benutzer aus. Ihre synchronisierten Benutzer von OneLogin werden auf der Seite Benutzer angezeigt. Sie können Ihre synchronisierten Gruppen auch auf der Seite Gruppen anzeigen.
12. Um Benutzeränderungen automatisch mit IAM Identity Center zu synchronisieren, navigieren Sie zur Seite Bereitstellung, suchen Sie den Abschnitt Administratorgenehmigung erforderlich, bevor diese Aktion ausgeführt wird, deaktivieren Sie Benutzer erstellen, Benutzer löschen und/oder Benutzer aktualisieren und klicken Sie auf Speichern.

(Optional) Schritt 3: Konfigurieren von Benutzerattributen in OneLogin für die Zugriffskontrolle in IAM Identity Center

Dies ist ein optionales Verfahren für , OneLogin wenn Sie Attribute konfigurieren möchten, die Sie in IAM Identity Center verwenden, um den Zugriff auf Ihre -AWSRessourcen zu verwalten. Die Attribute, die Sie in definieren, OneLogin werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie einen Berechtigungssatz in IAM Identity Center, um den Zugriff basierend auf den Attributen zu verwalten, die Sie von übergeben habenOneLogin.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die Attribute für Zugriffskontrolle Funktion aktivieren. Weitere Information dazu finden Sie unter Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle.

So konfigurieren Sie Benutzerattribute in OneLogin für die Zugriffskontrolle in IAM Identity Center

1. Melden Sie sich bei an OneLoginund navigieren Sie dann zu Anwendungen > Anwendungen.
2. Suchen Sie auf der Seite Anwendungen nach der Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen. Wählen Sie es aus und wählen Sie dann in der linken Navigationsleiste Parameter aus.
3. Gehen Sie im Abschnitt Erforderliche Parameter für jedes Attribut, das Sie in IAM Identity Center verwenden möchten, wie folgt vor:

    a. Wählen Sie + aus.

b. Geben Sie unter Feldname ein und ersetzen Sie **`AttributeName`** durch den Namen des Attributshttps://aws.amazon.com/SAML/Attributes/AccessControl:**`AttributeName`**, das Sie in IAM Identity Center erwarten. Beispiel: https://aws.amazon.com/SAML/Attributes/AccessControl:**`Department`**

c. Aktivieren Sie unter Flags das Kontrollkästchen neben In SAML-Assertion einschließen und wählen Sie Speichern aus.

d. Verwenden Sie im Feld Wert die Dropdown-Liste, um die OneLogin Benutzerattribute auszuwählen. Zum Beispiel Abteilung .

4. Wählen Sie Speichern.

(Optional) Übergeben von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein -AttributeElement mit dem -NameAttribut auf festzulegenhttps://aws.amazon.com/SAML/Attributes/AccessControl:**`{TagKey}`**. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das AttributeValue-Element ein, das den Wert des Tags angibt. Um beispielsweise das Tag-Schlüssel-Wert-Paar zu übergebenCostCenter = blue, verwenden Sie das folgende Attribut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates -AttributeElement hinzu.

Fehlerbehebung

Im Folgenden finden Sie Hinweise zur Behebung einiger häufiger Probleme, die beim Einrichten der automatischen Bereitstellung mit auftreten könnenOneLogin.

Gruppen werden nicht für IAM Identity Center bereitgestellt

Standardmäßig werden Gruppen nicht von OneLogin zu IAM Identity Center bereitgestellt. Stellen Sie sicher, dass Sie die Gruppenbereitstellung für Ihre IAM-Identity-Center-Anwendung in aktiviert habenOneLogin. Melden Sie sich dazu bei der OneLogin Administratorkonsole an und überprüfen Sie, ob die Option In Benutzerbereitstellung einschließen unter den Eigenschaften der IAM-Identity-Center-Anwendung ausgewählt ist (IAM-Identity-Center-Anwendung > Parameter > Gruppen). Weitere Informationen zum Erstellen von Gruppen in OneLogin, einschließlich zum Synchronisieren von OneLogin Rollen als Gruppen in SCIM, finden Sie auf der OneLogin Website .

Nichts wird von OneLogin zu IAM Identity Center synchronisiert, obwohl alle Einstellungen korrekt sind

Zusätzlich zum obigen Hinweis zur Administratorgenehmigung müssen Sie die Berechtigungszuordnungen erneut anwenden, damit viele Konfigurationsänderungen wirksam werden. Dies finden Sie unter Anwendungen > Anwendungen > IAM-Identity-Center-Anwendung > Weitere Aktionen. Details und Protokolle für die meisten Aktionen in OneLogin, einschließlich Synchronisationsereignissen, finden Sie unter Aktivität > Ereignisse.

Ich habe eine Gruppe in gelöscht oder deaktiviertOneLogin, sie wird aber weiterhin im IAM Identity Center angezeigt

OneLogin unterstützt derzeit nicht die SCIM DELETE-Operation für Gruppen, was bedeutet, dass die Gruppe weiterhin im IAM Identity Center existiert. Daher müssen Sie die Gruppe direkt aus dem IAM Identity Center entfernen, um sicherzustellen, dass alle entsprechenden Berechtigungen im IAM Identity Center für diese Gruppe entfernt werden.

Ich habe eine Gruppe in IAM Identity Center gelöscht, ohne sie zuerst aus zu löschen, OneLogin und jetzt habe ich Probleme mit der Benutzer-/Gruppensynchronisierung

Um diese Situation zu beheben, stellen Sie zunächst sicher, dass Sie keine redundanten Gruppenbereitstellungsregeln oder -konfigurationen in habenOneLogin. Zum Beispiel eine Gruppe, die direkt einer Anwendung zugewiesen ist, zusammen mit einer Regel, die in derselben Gruppe veröffentlicht. Löschen Sie als Nächstes alle unerwünschten Gruppen in IAM Identity Center. Aktualisieren OneLogin Sie schließlich in die Berechtigungen (IAM Identity Center App > Bereitstellung > Berechtigungen) und wenden Sie dann die Berechtigungszuordnungen erneut an (IAM Identity Center App > Weitere Aktionen). Um dieses Problem in Zukunft zu vermeiden, nehmen Sie zunächst die Änderung vor, um die Bereitstellung der Gruppe in zu beendenOneLogin, und löschen Sie dann die Gruppe aus IAM Identity Center.

Verwenden von -Ping IdentityProdukten mit IAM Identity Center

Die folgenden Ping Identity Produkte wurden mit IAM Identity Center getestet.

Themen

PingFederate

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisierung) von Benutzer- und Gruppeninformationen aus dem PingFederate Produkt bis Ping Identity (nachstehend „Ping“) in IAM Identity Center. Diese Bereitstellung verwendet das System for Cross-Domain Identity Management (SCIM) v2.0-Protokoll. Sie konfigurieren diese Verbindung in PingFederate mit Ihrem IAM-Identity-Center-SCIM-Endpunkt und Zugriffstoken. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute in PingFederate zu den benannten Attributen in IAM Identity Center. Dies führt dazu, dass die erwarteten Attribute zwischen IAM Identity Center und übereinstimmenPingFederate.

Dieses Handbuch basiert auf PingFederate Version 10.2. Die Schritte für andere Versionen können variieren. Weitere Informationen zum Konfigurieren der Bereitstellung für IAM Identity Center für andere Versionen von Ping erhalten Sie von PingFederate.

Die folgenden Schritte führen Sie durch die Aktivierung der automatischen Bereitstellung von Benutzern und Gruppen von PingFederate zu IAM Identity Center mithilfe des SCIM-Protokolls.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu überprüfenÜberlegungen zur Verwendung der automatischen Bereitstellung. Lesen Sie dann weitere Überlegungen im nächsten Abschnitt.

Themen

- Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center
- Schritt 2: Konfigurieren der Bereitstellung in PingFederate
- (Optional) Schritt 3: Konfigurieren von Benutzerattributen in PingFederate für die Zugriffskontrolle in IAM Identity Center
- (Optional) Übergeben von Attributen für die Zugriffskontrolle

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- Ein funktionierender PingFederate Server. Wenn Sie noch keinen PingFederate Server haben, können Sie möglicherweise eine kostenlose Testversion oder ein Entwicklerkonto von der Ping-Identity-Website erhalten. Die Testversion enthält Lizenzen und Software-Downloads sowie die zugehörige Dokumentation.
- Eine Kopie der auf Ihrem PingFederate Server installierten Software von PingFederate IAM Identity Center Connector. Weitere Informationen zum Abrufen dieser Software finden Sie unter IAM Identity Center Connector auf der Ping Identity-Website.
- Ein IAM-Identity-Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Eine SAML-Verbindung von Ihrer PingFederate Instance zu IAM Identity Center. Anweisungen zum Konfigurieren dieser Verbindung finden Sie in der -PingFederateDokumentation. Zusammenfassend lässt sich sagen, dass der empfohlene Pfad darin besteht, den IAM Identity Center Connector zu verwenden, um „Browser SSO“ in zu konfigurierenPingFederate, wobei die Metadatenfunktionen „Download“ und „Import“ an beiden Enden verwendet werden, um SAML-Metadaten zwischen PingFederate und IAM Identity Center auszutauschen.

Weitere Überlegungen

Im Folgenden finden Sie wichtige Überlegungen zu PingFederate, die sich auf die Implementierung der Bereitstellung mit IAM Identity Center auswirken können.

- Wenn ein Attribut (z. B. eine Telefonnummer) von einem Benutzer in dem in konfigurierten Datenspeicher entfernt wirdPingFederate, wird dieses Attribut nicht vom entsprechenden Benutzer in IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung bei der Implementierung von PingFederate’s -Provisionern. Wenn ein Attribut in einen anderen (nicht leeren) Wert eines Benutzers geändert wird, wird diese Änderung mit IAM Identity Center synchronisiert.

Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM-Identity-Center-Konsole, um die automatische Bereitstellung zu aktivieren.

So aktivieren Sie die automatische Bereitstellung in IAM Identity Center

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Feld Informationen zur automatischen Bereitstellung und wählen Sie dann Aktivieren aus. Dies aktiviert sofort die automatische Bereitstellung im IAM Identity Center und zeigt die erforderlichen SCIM-Endpunkt- und Zugriffstokeninformationen an.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehenden Datenverkehr jeden der Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
   a. SCIM-Endpunkt
   b. Zugriffstoken
5. Klicken Sie auf Schließen.

Nachdem Sie nun die Bereitstellung in der IAM-Identity-Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mit der PingFederate Administratorkonsole ausführen. Die Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren der Bereitstellung in PingFederate

Gehen Sie wie folgt in der PingFederate Administratorkonsole vor, um die Integration zwischen IAM Identity Center und dem IAM Identity Center Connector zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die Software IAM Identity Center Connector bereits installiert haben. Wenn Sie dies noch nicht getan haben, lesen Sie , und führen Sie dann dieses Verfahren ausVoraussetzungen, um die SCIM-Bereitstellung zu konfigurieren.

> **Important**
>
> Wenn Ihr PingFederate Server noch nicht für die ausgehende SCIM-Bereitstellung konfiguriert wurde, müssen Sie möglicherweise eine Änderung der Konfigurationsdatei vornehmen, um die Bereitstellung zu aktivieren. Weitere Informationen finden Sie

in der -PingDokumentation. Zusammenfassend lässt sich sagen, dass Sie die `-pf.provisioner.mode`Einstellung in der pingfederate-<version>/pingfederate/bin/run.properties Datei auf einen anderen Wert als ändern `OFF` (der Standard ist) und den Server neu starten müssen, wenn er derzeit ausgeführt wird. Sie können beispielsweise verwenden, `STANDALONE` wenn Sie derzeit keine Hochverfügbarkeitskonfiguration mit habenPingFederate.

So konfigurieren Sie die Bereitstellung in PingFederate

1. Melden Sie sich bei der PingFederate Administratorkonsole an.
2. Wählen Sie oben auf der Seite Anwendungen aus und klicken Sie dann auf SP Connections.
3. Suchen Sie die Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen, und klicken Sie auf den Verbindungsnamen.
4. Wählen Sie in den blauen Navigationsüberschriften oben auf der Seite Verbindungstyp aus. Sie sollten sehen, dass Browser SSO bereits aus Ihrer vorherigen Konfiguration von SAML ausgewählt wurde. Andernfalls müssen Sie diese Schritte zuerst ausführen, bevor Sie fortfahren können.
5. Aktivieren Sie das Kontrollkästchen Outbound Provisioning, wählen Sie IAM Identity Center Cloud Connector als Typ aus und klicken Sie auf Save . Wenn IAM Identity Center Cloud Connector nicht als Option angezeigt wird, stellen Sie sicher, dass Sie den IAM Identity Center Connector installiert und Ihren PingFederate Server neu gestartet haben.
6. Klicken Sie wiederholt auf Weiter, bis Sie auf der Seite Ausgehende Bereitstellung ankommen, und klicken Sie dann auf die Schaltfläche Bereitstellung konfigurieren.
7. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das SCIM-URL-Feld in der PingFederate Konsole ein. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen. Außerdem haben Sie im vorherigen Verfahren den Wert für das Zugriffstoken in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld Zugriffstoken in der PingFederate Konsole ein. Klicken Sie auf Speichern.
8. Klicken Sie auf der Seite Kanalkonfiguration (Kanäle konfigurieren) auf Erstellen.
9. Geben Sie einen Kanalnamen für diesen neuen Bereitstellungskanal ein (z. B. **`AWSIAMIdentityCenterchannel`**) und klicken Sie auf Weiter.
10. Wählen Sie auf der Seite Quelle den Active Data Store aus, den Sie für Ihre Verbindung mit IAM Identity Center verwenden möchten, und klicken Sie auf Weiter.

> **Note**
>
> Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Informationen zur Auswahl und Konfiguration einer Datenquelle in finden Sie in der Ping ProduktdokumentationPingFederate.

11. Bestätigen Sie auf der Seite Quelleinstellungen, dass alle Werte für Ihre Installation korrekt sind, und klicken Sie dann auf Weiter.
12. Geben Sie auf der Seite Quellspeicherort die für Ihre Datenquelle geeigneten Einstellungen ein und klicken Sie dann auf Weiter. Wenn Sie beispielsweise Active Directory als LDAP-Verzeichnis verwenden:
    a. Geben Sie den Basis-DN Ihrer AD-Gesamtstruktur ein (z. B. **`DC=myforest,DC=mydomain,DC=com`**).
    b. Geben Sie unter Benutzer > Gruppen-DN eine einzelne Gruppe an, die alle Benutzer enthält, die Sie für IAM Identity Center bereitstellen möchten. Wenn keine solche einzelne Gruppe vorhanden ist, erstellen Sie diese Gruppe in AD, kehren Sie zu dieser Einstellung zurück und geben Sie dann den entsprechenden DN ein.
    c. Geben Sie an, ob Untergruppen (verschachtelte Suche) und ein erforderlicher LDAP-Filter durchsucht werden sollen.
    d. Geben Sie unter Gruppen > Gruppen-DN eine einzelne Gruppe an, die alle Gruppen enthält, die Sie für IAM Identity Center bereitstellen möchten. In vielen Fällen kann es sich um denselben DN handeln, den Sie im Abschnitt Benutzer angegeben haben. Geben Sie bei Bedarf verschachtelte Such- und Filter werteein.
13. Stellen Sie auf der Seite Attributzuordnung Folgendes sicher und klicken Sie dann auf Weiter:
    a. Das Feld userName muss einem Attribut zugeordnet werden, das als E-Mail (user@domain.com) formatiert ist. Er muss auch mit dem Wert übereinstimmen, den der Benutzer für die Anmeldung bei Ping verwendet. Dieser Wert wird während der Verbundauthentifizierung wiederum im SAML-`nameId`Anspruch ausgefüllt und für den Abgleich mit dem Benutzer im IAM Identity Center verwendet. Wenn Sie beispielsweise Active Directory verwenden, können Sie die `UserPrincipalName` als userName angeben.
    b. Andere Felder mit dem Suffix * müssen Attributen zugeordnet werden, die für Ihre Benutzer ungleich Null sind.

14. Legen Sie auf der Seite Aktivierung und Zusammenfassung den Kanalstatus auf Aktiv fest, damit die Synchronisation sofort nach dem Speichern der Konfiguration gestartet wird.
15. Vergewissern Sie sich, dass alle Konfigurationswerte auf der Seite korrekt sind, und klicken Sie auf Fertig.
16. Klicken Sie auf der Seite Kanäle verwalten auf Speichern.
17. Zu diesem Zeitpunkt beginnt die Bereitstellung. Um die Aktivität zu bestätigen, können Sie die Datei provisioner.log anzeigen, die sich standardmäßig im pingfederate-<version>/pingfederate/log Verzeichnis auf Ihrem PingFederate Server befindet.
18. Um zu überprüfen, ob Benutzer und Gruppen erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM-Identity-Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von PingFederate werden auf der Seite Benutzer angezeigt. Sie können synchronisierte Gruppen auch auf der Seite Gruppen anzeigen.

(Optional) Schritt 3: Konfigurieren von Benutzerattributen in PingFederate für die Zugriffskontrolle in IAM Identity Center

Dies ist ein optionales Verfahren für , PingFederate wenn Sie Attribute konfigurieren möchten, die Sie in IAM Identity Center verwenden, um den Zugriff auf Ihre -AWSRessourcen zu verwalten. Die Attribute, die Sie in definieren, PingFederate werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie einen Berechtigungssatz in IAM Identity Center, um den Zugriff basierend auf den Attributen zu verwalten, die Sie von übergeben habenPingFederate.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die Attribute für Zugriffskontrolle Funktion aktivieren. Weitere Information dazu finden Sie unter Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle.

So konfigurieren Sie Benutzerattribute in PingFederate für die Zugriffskontrolle in IAM Identity Center

1. Melden Sie sich bei der PingFederate Administratorkonsole an.
2. Wählen Sie oben auf der Seite Anwendungen und dann SP Connections aus.
3. Suchen Sie die Anwendung, die Sie zuvor erstellt haben, um Ihre SAML-Verbindung mit IAM Identity Center herzustellen, und klicken Sie auf den Verbindungsnamen.
4. Wählen Sie in den blauen Navigationsüberschriften oben auf der Seite Browser SSO aus. Klicken Sie dann auf Browser SSO konfigurieren.
5. Wählen Sie auf der Seite Browser-SSO konfigurieren die Option Assertion Creation aus und klicken Sie dann auf Configure Assertion Creation .

6. Wählen Sie auf der Seite Assertionerstellung konfigurieren die Option Attributattribut aus.
7. Fügen Sie auf der Seite Attributvertrag im Abschnitt Verlängern des Rabatts ein neues Attribut hinzu, indem Sie die folgenden Schritte ausführen:

   a. Geben Sie in das Textfeld ein und ersetzen Sie **`AttributeName`** durch den Namen des Attributshttps://aws.amazon.com/SAML/Attributes/AccessControl:**`AttributeName`**, das Sie in IAM Identity Center erwarten. Beispiel: https://aws.amazon.com/SAML/Attributes/AccessControl:**`Department`**

   b. Wählen Sie für Attributnamenformat ausurn:oasis:names:tc:SAML:2.0:attrname-format:uri.

   c. Wählen Sie Hinzufügen und dann Weiter aus.
8. Wählen Sie auf der Seite Zuordnung von Authentifizierungsquellen die Adapter-Instance aus, die mit Ihrer Anwendung konfiguriert ist.
9. Wählen Sie auf der Seite Erfüllung des Attributvertrags die Optionen Quelle (Datenspeicher) und Wert (Datenspeicherattribut) für das Attributattribut aushttps://aws.amazon.com/SAML/Attributes/AccessControl:**`Department`**.

   > **Note**
   >
   > Wenn Sie noch keine Datenquelle konfiguriert haben, müssen Sie dies jetzt tun. Informationen zur Auswahl und Konfiguration einer Datenquelle in finden Sie in der Ping ProduktdokumentationPingFederate.
10. Klicken Sie wiederholt auf Weiter, bis Sie auf der Seite Aktivierung und Zusammenfassung ankommen, und klicken Sie dann auf Speichern.

(Optional) Übergeben von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein -AttributeElement mit dem -NameAttribut auf festzulegenhttps://aws.amazon.com/SAML/Attributes/AccessControl:**`{TagKey}`**. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Um beispielsweise das Tag-Schlüssel-Wert-Paar zu übergeben`CostCenter = blue`, verwenden Sie das folgende Attribut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates -`AttributeElement` hinzu.

PingOne

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisierung) von Benutzerinformationen aus dem PingOne Produkt bis Ping Identity (nachstehend „Ping“) in IAM Identity Center. Diese Bereitstellung verwendet das System for Cross-Domain Identity Management (SCIM) v2.0-Protokoll. Sie konfigurieren diese Verbindung in PingOne mit Ihrem IAM-Identity-Center-SCIM-Endpunkt und Zugriffstoken. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Benutzerattribute in PingOne zu den benannten Attributen in IAM Identity Center. Dies führt dazu, dass die erwarteten Attribute zwischen IAM Identity Center und übereinstimmenPingOne.

Dieses Handbuch basiert auf PingOne dem Stand Oktober 2020. Die Schritte für neuere Versionen können variieren. Weitere Ping Informationen zum Konfigurieren der Bereitstellung für IAM Identity Center für andere Versionen von erhalten Sie von PingOne. Dieses Handbuch enthält auch einige Hinweise zur Konfiguration der Benutzerauthentifizierung über SAML.

Die folgenden Schritte führen Sie durch die Aktivierung der automatischen Bereitstellung von Benutzern von PingOne an IAM Identity Center mithilfe des SCIM-Protokolls.

> **Note**
>
> Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die zu überprüfenÜberlegungen zur Verwendung der automatischen Bereitstellung. Lesen Sie dann weitere Überlegungen im nächsten Abschnitt.

Themen

- Voraussetzungen
- Weitere Überlegungen

- Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center
- Schritt 2: Konfigurieren der Bereitstellung in PingOne
- (Optional) Schritt 3: Konfigurieren von Benutzerattributen in PingOne für die Zugriffskontrolle in IAM Identity Center
- (Optional) Übergeben von Attributen für die Zugriffskontrolle

Voraussetzungen

Sie benötigen Folgendes, bevor Sie beginnen können:

- Ein PingOne Abonnement oder eine kostenlose Testversion mit Funktionen für Verbundauthentifizierung und Bereitstellung. Weitere Informationen zum Erhalten einer kostenlosen Testversion finden Sie auf der -Ping IdentityWebsite.
- Ein IAM-Identity-Center-fähiges Konto (kostenlos). Weitere Informationen finden Sie unter IAM Identity Center aktivieren.
- Die PingOne IAM-Identity-Center-Anwendung, die Ihrem PingOne Administratorportal hinzugefügt wurde. Sie können die PingOne IAM-Identity-Center-Anwendung aus dem PingOne Application Catalog abrufen. Allgemeine Informationen finden Sie unter Hinzufügen einer Anwendung aus dem Application Catalog auf der -Ping IdentityWebsite.
- Eine SAML-Verbindung von Ihrer PingOne Instance zu IAM Identity Center. Nachdem die PingOne IAM-Identity-Center-Anwendung zu Ihrem PingOne Administratorportal hinzugefügt wurde, müssen Sie sie verwenden, um eine SAML-Verbindung von Ihrer PingOne Instance zu IAM Identity Center zu konfigurieren. Verwenden Sie die Metadatenfunktion „Herunterladen“ und „Importieren“ an beiden Enden, um SAML-Metadaten zwischen PingOne und IAM Identity Center auszutauschen. Anweisungen zum Konfigurieren dieser Verbindung finden Sie in der -PingOneDokumentation.

Weitere Überlegungen

Im Folgenden finden Sie wichtige Überlegungen zu PingOne, die sich auf die Implementierung der Bereitstellung mit IAM Identity Center auswirken können.

- Seit Oktober 2020 unterstützt PingOne die Bereitstellung von Gruppen über SCIM nicht. Wenden Sie sich an Ping, um die neuesten Informationen zur Gruppenunterstützung in SCIM für zu erhaltenPingOne.
- Benutzer können PingOne auch nach der Deaktivierung der Bereitstellung im PingOne Administratorportal weiterhin von bereitgestellt werden. Wenn Sie die Bereitstellung sofort beenden

müssen, löschen Sie das entsprechende SCIM-Bearer-Token und/oder deaktivieren Sie es Automatische Bereitstellung im IAM Identity Center.

- Wenn ein Attribut für einen Benutzer aus dem in konfigurierten Datenspeicher entfernt wirdPingOne, wird dieses Attribut nicht aus dem entsprechenden Benutzer im IAM Identity Center entfernt. Dies ist eine bekannte Einschränkung bei der Implementierung von PingOne's -Provisionern. Wenn ein Attribut geändert wird, wird die Änderung mit IAM Identity Center synchronisiert.
- Im Folgenden finden Sie wichtige Hinweise zu Ihrer SAML-Konfiguration in PingOne:
  - IAM Identity Center unterstützt nur `emailaddress` als `NameId` Format. Das bedeutet, dass Sie ein Benutzerattribut auswählen müssen, das in Ihrem Verzeichnis in eindeutigPingOne, nicht null und als E-Mail/UPN (z. B. user@domain.com) für Ihre SAML_SUBJECT-Zuweisung in formatiert istPingOne. Email (Work) ist ein sinnvoller Wert, der für Testkonfigurationen mit dem PingOne integrierten Verzeichnis verwendet werden kann.
  - Benutzer, die sich PingOne mit einer E-Mail-Adresse anmelden, die ein + Zeichen enthält, können sich möglicherweise nicht beim IAM Identity Center anmelden, da Fehler wie `'SAML_215'` oder auftreten`'Invalid input'`. Um dies zu behebenPingOne, wählen Sie in die Option Erweitert für die SAML_SUBJECT-Zuweisung in Attributzuordnungen aus. Legen Sie dann urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress im Dropdown-Menü das Format der Namens-ID fest, das an SP gesendet werden soll: bis .

Schritt 1: Aktivieren der Bereitstellung in IAM Identity Center

In diesem ersten Schritt verwenden Sie die IAM-Identity-Center-Konsole, um die automatische Bereitstellung zu aktivieren.

So aktivieren Sie die automatische Bereitstellung in IAM Identity Center

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Feld Informationen zur automatischen Bereitstellung und wählen Sie dann Aktivieren aus. Dies aktiviert sofort die automatische Bereitstellung im IAM Identity Center und zeigt die erforderlichen SCIM-Endpunkt- und Zugriffstokeninformationen an.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehenden Datenverkehr jeden der Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.

a. SCIM-Endpunkt

b. Zugriffstoken

5. Klicken Sie auf Schließen.

Nachdem Sie nun die Bereitstellung in der IAM-Identity-Center-Konsole eingerichtet haben, müssen Sie die verbleibenden Aufgaben mit der PingOne IAM-Identity-Center-Anwendung abschließen. Diese Schritte werden im folgenden Verfahren beschrieben.

Schritt 2: Konfigurieren der Bereitstellung in PingOne

Gehen Sie wie folgt in der PingOne IAM-Identity-Center-Anwendung vor, um die Bereitstellung mit IAM Identity Center zu aktivieren. Bei diesem Verfahren wird davon ausgegangen, dass Sie die PingOne IAM-Identity-Center-Anwendung bereits zu Ihrem PingOne Administratorportal hinzugefügt haben. Wenn Sie dies noch nicht getan haben, lesen Sie , und führen Sie dann dieses Verfahren ausVoraussetzungen, um die SCIM-Bereitstellung zu konfigurieren.

So konfigurieren Sie die Bereitstellung in PingOne

1. Öffnen Sie die PingOne IAM-Identity-Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben PingOne (Anwendungen > Meine Anwendungen). Siehe Voraussetzungen.
2. Scrollen Sie nach unten auf der Seite. Wählen Sie unter Benutzerbereitstellung den vollständigen Link aus, um zur Konfiguration der Benutzerbereitstellung Ihrer Verbindung zu navigieren.
3. Wählen Sie auf der Seite Bereitstellungsanweisungen die Option Mit dem nächsten Schritt fortfahren aus.
4. Im vorherigen Verfahren haben Sie den SCIM-Endpunktwert in IAM Identity Center kopiert. Fügen Sie diesen Wert in das SCIM-URL-Feld in der PingOne IAM-Identity-Center-Anwendung ein. Stellen Sie sicher, dass Sie den abschließenden Schrägstrich am Ende der URL entfernen. Außerdem haben Sie im vorherigen Verfahren den Wert für das Zugriffstoken in IAM Identity Center kopiert. Fügen Sie diesen Wert in das Feld ACCESS_TOKEN in der PingOne IAM-Identity-Center-Anwendung ein.
5. Wählen Sie für REMOVE_ACTION entweder Deaktiviert oder Gelöscht aus (weitere Informationen finden Sie im Beschreibungstext auf der Seite).
6. Wählen Sie auf der Seite Attributzuordnung einen Wert aus, der für die SAML_SUBJECT (`NameId`)-Assertion verwendet werden soll, indem Sie den Anweisungen von Weitere

Überlegungen weiter oben auf dieser Seite folgen. Wählen Sie dann Weiter zum nächsten Schritt aus.

7. Nehmen Sie auf der Seite PingOne App Customization – IAM Identity Center alle gewünschten Anpassungsänderungen vor (optional) und klicken Sie auf Weiter zum nächsten Schritt .
8. Wählen Sie auf der Seite Gruppenzugriff die Gruppen aus, die die Benutzer enthalten, die Sie für die Bereitstellung und Single Sign-On beim IAM Identity Center aktivieren möchten. Wählen Sie Weiter zum nächsten Schritt aus.
9. Scrollen Sie zum Ende der Seite und wählen Sie Fertig stellen, um mit der Bereitstellung zu beginnen.
10. Um zu überprüfen, ob Benutzer erfolgreich mit IAM Identity Center synchronisiert wurden, kehren Sie zur IAM-Identity-Center-Konsole zurück und wählen Sie Benutzer aus. Synchronisierte Benutzer von PingOne werden auf der Seite Benutzer angezeigt. Diese Benutzer können jetzt Konten und Anwendungen im IAM Identity Center zugewiesen werden.

    Denken Sie daran, dass PingOne die Bereitstellung von Gruppen oder Gruppenmitgliedschaften über SCIM nicht unterstützt. Weitere Informationen erhalten Sie Ping von .

(Optional) Schritt 3: Konfigurieren von Benutzerattributen in PingOne für die Zugriffskontrolle in IAM Identity Center

Dies ist ein optionales Verfahren für , PingOne wenn Sie Attribute für IAM Identity Center konfigurieren möchten, um den Zugriff auf Ihre -AWSRessourcen zu verwalten. Die Attribute, die Sie in definieren, PingOne werden in einer SAML-Assertion an IAM Identity Center übergeben. Anschließend erstellen Sie einen Berechtigungssatz in IAM Identity Center, um den Zugriff basierend auf den Attributen zu verwalten, die Sie von übergeben habenPingOne.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie zuerst die Attribute für Zugriffskontrolle Funktion aktivieren. Weitere Information dazu finden Sie unter Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle.

So konfigurieren Sie Benutzerattribute in PingOne für die Zugriffskontrolle in IAM Identity Center

1. Öffnen Sie die PingOne IAM-Identity-Center-Anwendung, die Sie im Rahmen der Konfiguration von SAML für installiert haben PingOne (Anwendungen > Meine Anwendungen).
2. Wählen Sie Bearbeiten und dann Weiter zum nächsten Schritt, bis Sie zur Seite Attributzuordnungen gelangen.

3. Wählen Sie auf der Seite Attributzuordnungen die Option Neues Attribut hinzufügen aus und gehen Sie dann wie folgt vor. Sie müssen diese Schritte für jedes Attribut ausführen, das Sie zur Verwendung in IAM Identity Center für die Zugriffskontrolle hinzufügen.

   a. Geben Sie im Feld Application Attribute ein`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. Ersetzen Sie *`AttributeName`* durch den Namen des Attributs, das Sie in IAM Identity Center erwarten. Beispiel: `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**

   b. Wählen Sie im Feld Identity Bridge-Attribut oder Literalwert Benutzerattribute aus Ihrem PingOne Verzeichnis aus. Zum Beispiel E-Mail (Work).

4. Wählen Sie einige Male Weiter und dann Fertig stellen aus.

(Optional) Übergeben von Attributen für die Zugriffskontrolle

Sie können optional die Attribute für Zugriffskontrolle Funktion in IAM Identity Center verwenden, um ein -`AttributeElement` mit dem -`Name`Attribut auf festzulegen`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Mit diesem Element können Sie Attribute als Sitzungs-Tags in der SAML-Zusicherung übergeben. Weitere Informationen zu Sitzungs-Tags finden Sie unter Übergeben von Sitzungs-Tags in AWS STS im IAM-Benutzerhandbuch.

Um Attribute als Sitzungs-Tags zu übergeben, schließen Sie das `AttributeValue`-Element ein, das den Wert des Tags angibt. Um beispielsweise das Tag-Schlüssel-Wert-Paar zu übergeben`CostCenter = blue`, verwenden Sie das folgende Attribut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Wenn Sie mehrere Attribute hinzufügen müssen, fügen Sie für jedes Tag ein separates -`AttributeElement` hinzu.

Erste Schritte mit allgemeinen Aufgaben in IAM Identity Center

Wenn Sie ein neuer Benutzer von IAM Identity Center sind, lautet der grundlegende Arbeitsablauf für den Einstieg in die Nutzung des Dienstes wie folgt:

1. Melden Sie sich bei der Konsole Ihres Verwaltungskontos an, wenn Sie eine Organisationsinstanz von IAM Identity Center verwenden, oder bei Ihrer, AWS-Konto wenn Sie eine Kontoinstanz von IAM Identity Center verwenden, und navigieren Sie zur IAM Identity Center-Konsole.
2. Wählen Sie in der IAM Identity Center-Konsole das Verzeichnis aus, das Sie zum Speichern der Identitäten Ihrer Benutzer und Gruppen verwenden. IAM Identity Center stellt Ihnen standardmäßig ein Verzeichnis zur Verfügung, mit dem Sie den Benutzerzugriff konfigurieren können. Wenn Sie lieber eine andere Identitätsquelle verwenden möchten, können Sie Ihr Active Directory oder einen externen Identitätsanbieter verbinden.
3. Weisen Sie für Organisationsinstanzen Benutzerzugriff zu, AWS-Konten indem Sie die Konten in Ihrer Organisation auswählen und dann Benutzer oder Gruppen aus Ihrem Verzeichnis sowie die Berechtigungen auswählen, die Sie ihnen gewähren möchten.
4. Gewähren Sie Benutzern Zugriff auf Anwendungen, indem Sie:
   a. Richten Sie vom Kunden verwaltete SAML 2.0-Anwendungen ein, indem Sie entweder eine der vorintegrierten Anwendungen aus dem Anwendungskatalog auswählen oder Ihre eigene SAML 2.0-Anwendung hinzufügen.
   b. Konfigurieren Sie die Anwendungseigenschaften.
   c. Weisen Sie den Benutzern Zugriff auf die Anwendung zu. Es wird empfohlen, den Benutzerzugriff durch Gruppenmitgliedschaft zuzuweisen, anstatt einzelne Benutzerberechtigungen hinzuzufügen. Mit Gruppen können Sie Benutzergruppen Berechtigungen gewähren oder verweigern, anstatt diese Berechtigungen jedem einzelnen Benutzer zuzuweisen. Wenn ein Benutzer in eine andere Organisation wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe. Der Benutzer erhält dann automatisch die Berechtigungen, die für die neue Organisation erforderlich sind.
5. Wenn Sie das standardmäßige IAM Identity Center-Verzeichnis verwenden, teilen Sie Ihren Benutzern mit, wie sie sich beim AWS Access Portal anmelden sollen. Neue Benutzer in IAM Identity Center müssen ihre Benutzeranmeldedaten aktivieren, bevor sie für die Anmeldung am AWS Access Portal verwendet werden können. Weitere Informationen finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmelden beim AWS Access-Portal

Die Themen in diesem Abschnitt helfen Ihnen, sich mit den allgemeinen Aufgaben vertraut zu machen, die nach Abschluss der Erstkonfiguration von IAM Identity Center ausgeführt werden.

Wenn Sie IAM Identity Center noch nicht aktiviert haben, finden Sie weitere Informationen unter. Aktivieren AWS IAM Identity Center

Themen

Berechtigungssatz erstellen

Berechtigungssätze werden im IAM Identity Center gespeichert und definieren die Zugriffsebene, auf die Benutzer und Gruppen zugreifen können. AWS-Konto Der erste Berechtigungssatz, den Sie erstellen, ist der Administratorberechtigungssatz. Wenn Sie einen der Erste Schritte mit Tutorials bereits erstellten Administratorberechtigungssätze abgeschlossen haben. Gehen Sie wie folgt vor, um Berechtigungssätze zu erstellen, wie im Thema AWS Verwaltete Richtlinien für Jobfunktionen im IAM-Benutzerhandbuch beschrieben.

1. Führen Sie einen der folgenden Schritte aus, um sich bei der AWS Management Console anzumelden.

   - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
   - Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
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.

a. Wählen Sie auf der Seite Berechtigungssatztyp auswählen im Abschnitt Berechtigungssatztyp die Option Vordefinierter Berechtigungssatz aus.

b. Wählen Sie im Abschnitt Richtlinie für vordefinierten Berechtigungssatz eine der folgenden Optionen aus:

- AdministratorAccess
- Fakturierung
- DatabaseAdministrator
- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. 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.
6. Bestätigen Sie auf der Seite Überprüfen und erstellen Folgendes:

1. Unter Schritt 1: Typ des Berechtigungssatzes auswählen wird der Typ des ausgewählten Berechtigungssatzes angezeigt.
2. Für Schritt 2: Details zum Berechtigungssatz definieren wird der Name des ausgewählten Berechtigungssatzes angezeigt.
3. Wählen Sie Erstellen.

Erstellen Sie einen Berechtigungssatz, der Berechtigungen mit den geringsten Rechten anwendet

Um der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten zu folgen, erstellen Sie nach der Erstellung eines Administratorberechtigungssatzes einen restriktiveren Berechtigungssatz und weisen ihn einem oder mehreren Benutzern zu. Die im vorherigen Verfahren erstellten Berechtigungssätze bieten Ihnen einen Ausgangspunkt, um zu beurteilen, wie viel Zugriff

Ihre Benutzer auf Ressourcen benötigen. Um zu den Berechtigungen mit den geringsten Rechten zu wechseln, können Sie IAM Access Analyzer ausführen, um Prinzipale mit AWS verwalteten Richtlinien zu überwachen. Nachdem Sie erfahren haben, welche Berechtigungen sie verwenden, können Sie eine benutzerdefinierte Richtlinie schreiben oder eine Richtlinie generieren, die nur die erforderlichen Berechtigungen für Ihr Team enthält.

Mit IAM Identity Center können Sie demselben Benutzer mehrere Berechtigungssätze zuweisen. Ihrem Administratorbenutzer sollten außerdem zusätzliche, restriktivere Berechtigungssätze zugewiesen werden. Auf diese Weise können sie nur AWS-Konto mit den erforderlichen Berechtigungen auf Ihre zugreifen, anstatt immer ihre Administratorberechtigungen zu verwenden.

Wenn Sie beispielsweise Entwickler sind, können Sie nach der Erstellung Ihres Administratorbenutzers in IAM Identity Center einen neuen Berechtigungssatz erstellen, der `PowerUserAccess` Berechtigungen gewährt, und diesen Berechtigungssatz dann Ihnen selbst zuweisen. Im Gegensatz zum administrativen Berechtigungssatz, der `AdministratorAccess` Berechtigungen verwendet, ermöglicht der `PowerUserAccess` Berechtigungssatz keine Verwaltung von IAM-Benutzern und -Gruppen. Wenn Sie sich beim AWS Zugriffsportal anmelden, um auf Ihr AWS Konto zuzugreifen, können Sie `PowerUserAccess` wählen, ob Sie Entwicklungsaufgaben nicht im Konto ausführen `AdministratorAccess` möchten.

Beachten Sie folgende Überlegungen:

- Verwenden Sie einen vordefinierten Berechtigungssatz anstelle eines benutzerdefinierten Berechtigungssatzes, um schnell mit der Erstellung eines restriktiveren Berechtigungssatzes zu beginnen.

  Bei einem vordefinierten Berechtigungssatz, der vordefinierte Berechtigungen verwendet, wählen Sie eine einzelne AWS verwaltete Richtlinie aus einer Liste verfügbarer Richtlinien aus. Jede Richtlinie gewährt eine bestimmte Zugriffsebene auf AWS Dienste und Ressourcen oder Berechtigungen für eine allgemeine Aufgabenfunktion. Informationen zu jeder dieser Richtlinien finden Sie unter AWS Verwaltete Richtlinien für Berufsfunktionen.
- Sie können die Sitzungsdauer für einen Berechtigungssatz konfigurieren, um zu steuern, wie lange ein Benutzer angemeldet ist AWS-Konto.

  Wenn Benutzer sich mit ihnen verbinden AWS-Konto und die AWS Management Console oder die AWS Befehlszeilenschnittstelle (AWS CLI) verwenden, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Standardmäßig ist der Wert für die Sitzungsdauer, die bestimmt, wie lange ein Benutzer angemeldet werden kann und AWS-Konto bevor er sich von der Sitzung AWS abmeldet, auf eine

Stunde festgelegt. Sie können einen Höchstwert von 12 Stunden angeben. Weitere Informationen finden Sie unter Legen Sie die Sitzungsdauer fest.

- Sie können auch die Sitzungsdauer des AWS Access-Portals konfigurieren, um zu steuern, wie lange ein Workforce-Benutzer beim Portal angemeldet ist.

  Standardmäßig beträgt der Wert für Maximale Sitzungsdauer, der bestimmt, wie lange ein Workforce-Benutzer beim AWS Access-Portal angemeldet werden kann, bevor er sich erneut authentifizieren muss, acht Stunden. Sie können einen Höchstwert von 90 Tagen angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen.
- Wenn Sie sich beim AWS Zugriffsportal anmelden, wählen Sie die Rolle aus, die Berechtigungen mit den geringsten Rechten gewährt.

  Jeder Berechtigungssatz, den Sie erstellen und Ihrem Benutzer zuweisen, wird im Access-Portal als verfügbare Rolle angezeigt. AWS Wenn Sie sich als dieser Benutzer beim Portal anmelden, wählen Sie die Rolle aus, die dem restriktivsten Berechtigungssatz entspricht, den Sie für die Ausführung von Aufgaben im Konto verwenden können, und nicht`AdministratorAccess`.
- Sie können weitere Benutzer zu IAM Identity Center hinzufügen und diesen Benutzern bestehende oder neue Berechtigungssätze zuweisen.

  Weitere Informationen finden Sie unter. Weisen Sie Gruppen Zugriff zu AWS-Konto

Weisen Sie einem IAM Identity Center-Benutzer AWS-Konto Zugriff zu

Um den AWS-Konto Zugriff für einen IAM Identity Center-Benutzer einzurichten, müssen Sie den Benutzer dem AWS-Konto und -Berechtigungssatz zuweisen.

1. Führen Sie einen der folgenden Schritte aus, um sich bei der AWS Management Console anzumelden.

   - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
   - Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.

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 Zugriff zuweisen möchten. Wenn Sie Administratorzugriff für IAM Identity Center einrichten, aktivieren Sie das Kontrollkästchen neben dem Verwaltungskonto.
5. Wählen Sie Benutzer oder Gruppen zuweisen.
6. *Gehen Sie für **Schritt 1: Benutzer und Gruppen auswählen** auf der Seite **„AWS-Konto Benutzern und Gruppen zuordnen“** 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 dem ***AWS-Konto Namen*** zuweisen unter Berechtigungssätze einen Berechtigungssatz aus, um die Zugriffsebene zu definieren, die Benutzer und Gruppen darauf haben AWS-Konto.
8. Wählen Sie Weiter aus.
9. Gehen Sie für Schritt 3: Überprüfen und abschicken auf der Seite Aufgaben prüfen und abschicken an "***AWS-Konto Name***" wie folgt vor:

   1. Überprüfen Sie den ausgewählten Benutzer und den ausgewählten Berechtigungssatz.
   2. Nachdem Sie sich vergewissert haben, dass dem Berechtigungssatz 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, gehen Sie wie unter beschrieben vor, Benutzer zur MFA auffordern 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.

Melden Sie sich mit Ihren IAM Identity Center-Anmeldeinformationen beim AWS Zugriffsportal an

Das AWS Zugriffsportal bietet Benutzern von IAM Identity Center über ein Webportal Single Sign-On-Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen.

Gehen Sie wie folgt vor, um sicherzustellen, dass sich der IAM Identity Center-Benutzer beim AWS Zugriffsportal anmelden und auf das zugreifen kann. AWS-Konto

1. Führen Sie einen der folgenden Schritte aus, um sich bei der AWS Management Console anzumelden.
   - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
   - Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen an und wählen Sie eine Administratorrolle aus.
2. Öffnen Sie die IAM Identity Center-Konsole.

3. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
4. Wählen Sie auf der Dashboard-Seite unter Zusammenfassung der Einstellungen die URL des AWS Zugriffsportals aus.
5. 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.
   - Wenn Sie das standardmäßige 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.

1. Suchen Sie auf der Registerkarte Konten nach Ihrem Konto AWS-Konto und erweitern Sie es.
2. Die Rollen, die Ihnen zur Verfügung stehen, werden angezeigt. Wenn Ihnen beispielsweise sowohl der Berechtigungssatz als auch der AdministratorAccessBerechtigungssatz für die Abrechnung zugewiesen wurden, werden diese Rollen im AWS Zugriffsportal angezeigt. Wählen Sie den IAM-Rollennamen, den Sie für die Sitzung verwenden möchten.
3. Wenn Sie zur AWS Management Console weitergeleitet werden, haben Sie die Einrichtung des Zugriffs auf die AWS-Konto erfolgreich abgeschlossen.

> **Note**
>
> Wenn keine Rechte AWS-Kontenaufgeführt sind, wurde dem Benutzer wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Anweisungen zum Zuweisen von Benutzern zu einem Berechtigungssatz finden Sie unterWeisen Sie Benutzerzugriff zu AWS-Konten.

Nachdem Sie nun bestätigt haben, dass Sie sich mit Ihren IAM Identity Center-Anmeldeinformationen anmelden können, wechseln Sie zu dem Browser, mit dem Sie sich angemeldet haben, AWS Management Console und melden Sie sich von Ihren Root-Benutzer- oder IAM-Benutzeranmeldedaten ab.

> **Important**
>
> Wir empfehlen dringend, dass Sie bei der Anmeldung im AWS Access Portal die Anmeldeinformationen des IAM Identity Center-Administrators verwenden, um administrative Aufgaben auszuführen, anstatt die Anmeldeinformationen des IAM-Benutzers oder Root-Benutzers zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Um anderen Benutzern den Zugriff auf Ihre Konten und Anwendungen zu ermöglichen und IAM Identity Center zu verwalten, erstellen und weisen Sie Berechtigungssätze nur über IAM Identity Center zu.

Weisen Sie Gruppen Zugriff zu AWS-Konto

Nachdem Sie in IAM Identity Center einen Administratorbenutzer und zusätzliche Berechtigungssätze erstellt haben, mit denen Sie Aufgaben mit den geringsten Rechten ausführen können, können Sie Ihren beiden Benutzergruppen Zugriff gewähren. AWS-Konten

Wir empfehlen, den Zugriff direkt Gruppen und nicht einzelnen Benutzern zuzuweisen. Wenn Sie beispielsweise Gruppen und Berechtigungssätze auf der Grundlage von Organisationseinheiten erstellen und ein Benutzer zu einer anderen Organisationseinheit wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe und er erhält automatisch die Berechtigungen, die für die neue Organisationseinheit erforderlich sind, und verliert die Berechtigungen der vorherigen Organisationseinheit.

Um Benutzergruppenzugriff zuzuweisen AWS-Konten

1. Öffnen Sie die IAM Identity Center-Konsole.

   > **Note**
   >
   > Wenn Ihre Identitätsquelle ist, AWS Managed Microsoft AD stellen Sie sicher, dass die IAM Identity Center-Konsole die Region verwendet, in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie im Navigationsbereich unter Berechtigungen für mehrere Konten die Option. AWS-Konten

3. Auf der AWS-KontenSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren Kontrollkästchen AWS-Konten , denen Sie Single Sign-On-Zugriff zuweisen möchten.

   > **Note**
   >
   > Sie können bis zu 10 AWS-Konten pro Berechtigungssatz auswählen.

4. Wählen Sie Benutzer oder Gruppen zuweisen aus.
5. Schritt 1: Wählen Sie Benutzer und Gruppen aus. Wählen Sie auf der Seite Benutzer und Gruppen zu "***AWS-account-name***" zuweisen den Tab Gruppen und anschließend eine oder mehrere Gruppen aus.

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

   Um die ausgewählten Gruppen anzuzeigen, klicken Sie auf das seitliche Dreieck neben Ausgewählte Benutzer und Gruppen.

   Nachdem Sie bestätigt haben, dass die richtigen Gruppen ausgewählt sind, wählen Sie Weiter.
6. Für Schritt 2: Berechtigungssätze auswählen wählen Sie auf der Seite "***AWS-account-name***" Berechtigungssätze zuweisen einen oder mehrere Berechtigungssätze aus

   > **Note**
   >
   > Wenn Sie vor Beginn dieses Verfahrens nicht den gewünschten Berechtigungssatz erstellt haben, wählen Sie Berechtigungssatz erstellen aus und folgen Sie den Schritten unter. Berechtigungssatz erstellen Nachdem Sie die Berechtigungssätze erstellt haben, die Sie anwenden möchten, kehren Sie in der IAM Identity Center-Konsole zu AWS-Kontenund folgen Sie den Anweisungen, bis Sie zu Schritt 2: Berechtigungssätze auswählen gelangen. Wenn Sie diesen Schritt erreicht haben, wählen Sie die neuen Berechtigungssätze aus, die Sie erstellt haben, und fahren Sie mit dem nächsten Schritt in diesem Verfahren fort.

   Nachdem Sie bestätigt haben, dass die richtigen Berechtigungssätze ausgewählt wurden, wählen Sie Weiter.

7. Gehen Sie für Schritt 3: Überprüfen und abschicken auf der Seite Aufgaben überprüfen und an "***AWS-account-name***" senden wie folgt vor:

   1. Überprüfen Sie die ausgewählten Gruppen und Berechtigungssätze.
   2. Nachdem Sie sich vergewissert haben, dass die richtigen Gruppen und Berechtigungssätze ausgewählt sind, wählen Sie Senden aus.

   > **Important**
   >
   > Der Vorgang der Gruppenzuweisung kann einige Minuten dauern. Lassen Sie diese Seite geöffnet, bis der Vorgang erfolgreich abgeschlossen ist.

   > **Note**
   >
   > Möglicherweise müssen Sie Benutzern oder Gruppen Berechtigungen gewähren, um mit dem AWS Organizations Verwaltungskonto arbeiten zu können. Da es sich um ein Konto mit hohen Rechten handelt, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen über die FullAccessIAM-Richtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

Alternativ können Sie sie verwenden, AWS CloudFormationum Berechtigungssätze zu erstellen und zuzuweisen und diesen Berechtigungssätzen Benutzer zuzuweisen. Benutzer können sich dann beim AWS Zugriffsportal anmelden oder die Befehle AWS Command Line Interface (AWS CLI) verwenden.

Richten Sie Single Sign-On-Zugriff auf Ihre Anwendungen ein

IAM Identity Center unterstützt zwei Anwendungstypen: AWS verwaltete Anwendungen und vom Kunden verwaltete Anwendungen.

AWS verwaltete Anwendungen werden direkt in den entsprechenden Anwendungskonsolen oder über die Anwendungs-APIs konfiguriert.

Vom Kunden verwaltete Anwendungen müssen der IAM Identity Center-Konsole hinzugefügt und mit den entsprechenden Metadaten sowohl für IAM Identity Center als auch für den Service Provider

konfiguriert werden. Sie können aus einem Katalog häufig verwendeter Anwendungen wählen, die SAML 2.0 unterstützen, oder Sie können Ihre eigenen SAML 2.0-Anwendungen oder OAuth 2.0-Anwendungen einrichten.

Die Konfigurationsschritte für die Einrichtung des Single Sign-On-Zugriffs auf Anwendungen variieren je nach Anwendungstyp.

Richten Sie eine AWS verwaltete Anwendung ein

AWS verwaltete Anwendungen wie Amazon Managed Grafana und Amazon Monitron lassen sich in IAM Identity Center integrieren und können es für Authentifizierungs- und Verzeichnisdienste verwenden. Um eine AWS verwaltete Anwendung für die Zusammenarbeit mit IAM Identity Center einzurichten, müssen Sie die Anwendung direkt von der Konsole aus für den entsprechenden Dienst konfigurieren, oder Sie müssen die Anwendungs-APIs verwenden.

Richten Sie eine Anwendung aus dem Anwendungskatalog ein

Sie können eine SAML 2.0-Anwendung aus einem Katalog häufig verwendeter Anwendungen in der IAM Identity Center-Konsole auswählen. Gehen Sie wie folgt vor, um eine SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer Anwendung einzurichten.

So richten Sie eine Anwendung aus dem Anwendungskatalog ein

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte Vom Kunden verwaltet.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Einstellungen die Option Ich möchte eine Anwendung aus dem Katalog auswählen aus.
6. Geben Sie unter Anwendungskatalog den Namen der Anwendung, die Sie hinzufügen möchten, in das Suchfeld ein.
7. Wählen Sie den Namen der Anwendung aus der Liste aus, wenn er in den Suchergebnissen angezeigt wird, und klicken Sie dann auf Weiter.
8. Auf der Seite „Anwendung konfigurieren“ sind die Felder Anzeigename und Beschreibung bereits mit relevanten Details für die Anwendung gefüllt. Sie können diese Informationen bearbeiten.

9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:

    a. Wählen Sie unter IAM Identity Center SAML-Metadatendatei die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.

    b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Zertifikat herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

    > **Note**
    >
    > Sie benötigen diese Dateien später, wenn Sie die Anwendung auf der Website des Dienstanbieters einrichten. Befolgen Sie die Anweisungen des Anbieters.

10. (Optional) Unter Anwendungseigenschaften können Sie die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendungseigenschaften in der IAM Identity Center-Konsole.
11. Führen Sie unter Anwendungsmetadaten einen der folgenden Schritte aus:

    a. Wenn Sie über eine Metadatendatei verfügen, wählen Sie SAML-Metadatendatei für die Anwendung hochladen aus. Wählen Sie dann Datei auswählen, nach der die Metadatendatei gesucht werden soll, und wählen Sie sie aus.

    b. Wenn Sie keine Metadatendatei haben, wählen Sie Manuelles Eingeben Ihrer Metadatenwerte und geben Sie dann die ACS-URL der Anwendung und die SAML-Zielgruppenwerte für die Anwendung an.

12. Wählen Sie Absenden aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Richten Sie Ihre eigene SAML 2.0-Anwendung ein

Gehen Sie wie folgt vor, um Ihre eigene SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer eigenen SAML 2.0-Anwendung einzurichten. Bevor Sie damit beginnen, stellen Sie sicher, dass Sie die Zertifikatsdatei sowie die Austauschdatei mit den Metadaten des Service-Anbieters haben, damit Sie die Einrichtung der Vertrauensstellung abschließen können.

So richten Sie Ihre eigene SAML 2.0-Anwendung ein

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).

3. Wählen Sie die Registerkarte Vom Kunden verwaltet.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Einstellungen die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
6. Wählen Sie unter Anwendungstyp die Option SAML 2.0 aus.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Anwendung konfigurieren unter Anwendung konfigurieren einen Anzeigenamen für die Anwendung ein, z. B. **`MyApp`** Geben Sie dann eine Beschreibung ein.
9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:

    a. Wählen Sie unter IAM Identity Center SAML-Metadatendatei die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.

    b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

    > **Note**
    >
    > Sie benötigen diese Dateien später, wenn Sie die benutzerdefinierte Anwendung über die Website des Service-Anbieters einrichten.

10. (Optional) Unter Anwendungseigenschaften können Sie auch die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendungseigenschaften in der IAM Identity Center-Konsole.
11. Wählen Sie unter Anwendungsmetadaten die Option Manuelles Eingeben Ihrer Metadatenwerte aus. Geben Sie dann die ACS-URL der Anwendung und die Zielgruppenwerte für die SAML-Anwendung ein.
12. Wählen Sie Absenden aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Nachdem Sie Ihre Anwendungen eingerichtet haben, können Ihre Benutzer von ihrem Zugriffsportal aus auf Ihre Anwendungen AWS zugreifen, basierend auf den von Ihnen zugewiesenen Berechtigungen.

Wenn Sie vom Kunden verwaltete Anwendungen haben, die OAuth 2.0 unterstützen, und Ihre Benutzer Zugriff von diesen Anwendungen auf AWS Dienste benötigen, können Sie Trusted

Identity Propagation verwenden. Mit Trusted Identity Propagation kann sich ein Benutzer bei einer Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Zugriff auf Daten in AWS Diensten weitergeben. Weitere Informationen finden Sie unter Verwendung von Trusted Identity Propagation mit vom Kunden verwalteten Anwendungen.

Weitere Informationen zu unterstützten Anwendungstypen finden Sie unter Zugriff auf Anwendungen verwalten.

Benutzer- und Gruppenzuweisungen anzeigen

Auf den Seiten Benutzer und Gruppen können Sie sehen, wer Zugriff auf was in IAM Identity Center hat. Gehen Sie wie folgt vor, um die Zugriffsebene anzuzeigen, die Benutzer auf AWS Konten, Berechtigungssätze, Anwendungen und Gruppen haben.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Benutzer oder Gruppen, je nachdem, ob Sie eine Benutzergruppe oder einen Benutzer bearbeiten möchten, der einzeln zugewiesen wurde.
3. Wählen Sie einen Benutzer oder eine Gruppe aus der Liste aus.
4. Wählen Sie aus, ob Sie Kontenzuordnungen, Anwendungszuordnungen oder Gruppenzuweisungen anzeigen möchten:

   - AWS Zuweisungen von Konten und Berechtigungssätzen
     1. Wählen Sie die Registerkarte Accounts.
     2. Wählen Sie ein Konto aus der Liste aus, um die Zuweisungen von Berechtigungssätzen für Benutzer und Gruppen anzuzeigen.
     3. Wählen Sie einen Berechtigungssatz aus, um die Richtlinien- und Zuweisungsdetails anzuzeigen.
   - Anwendungszuweisungen
     1. Wählen Sie die Registerkarte Anwendungen, um zu sehen, welche Anwendungen einem Benutzer oder einer Gruppe zugewiesen sind.
     2. Wählen Sie eine Anwendung aus der Liste aus, um die Zuweisungsdetails anzuzeigen.
   - Gruppenzuweisungen
     1. Wählen Sie auf der Seite Benutzer die Registerkarte Gruppen aus.
     2. Wählen Sie eine Gruppe aus, um die Gruppenzuweisungen für einen Benutzer anzuzeigen.

Organisations- und Kontoinstanzen von IAM Identity Center verwalten

Eine Instanz ist eine einzelne Bereitstellung von IAM Identity Center. Für IAM Identity Center sind zwei Arten von Instanzen verfügbar: Organisationsinstanzen und Kontoinstanzen.

AWS-Konto Typen, die IAM Identity Center aktivieren können

Um IAM Identity Center zu aktivieren, melden Sie sich je nach Instanztyp, den Sie erstellen möchten, mit einem der folgenden Anmeldeinformationen an: AWS Management Console

- Ihr AWS Organizations Verwaltungskonto (empfohlen) — Erforderlich, um eine Organisationsinstanz von IAM Identity Center zu erstellen. Verwenden Sie eine Organisationsinstanz für Berechtigungen für mehrere Konten und Anwendungszuweisungen im gesamten Unternehmen.
- Ihr AWS Organizations Mitgliedskonto — Wird verwendet, um eine Kontoinstanz von IAM Identity Center zu erstellen, um Anwendungszuweisungen innerhalb dieses Mitgliedskontos zu ermöglichen. In einer Organisation können ein oder mehrere Konten mit einer Instanz auf Mitgliedsebene existieren.
- Eigenständig AWS-Konto — Wird verwendet, um eine Organisations- oder Kontoinstanz von IAM Identity Center zu erstellen. Die Standalone-Version wird AWS-Konto nicht von AWS Organizations verwaltet. Nur eine Instanz von IAM Identity Center kann einer eigenständigen Instanz zugeordnet werden, AWS-Konto und Sie können die Instanz für Anwendungszuweisungen innerhalb dieser eigenständigen AWS-Konto Instanz verwenden.

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Instanz AWS-Konto
Benutzer verwalten	 Ja	 Ja	 Ja

Funktion	Instanz im AWS Organizations Verwaltungskonto (empfohlen)	Instanz in einem Mitgliedskonto	Instanz in einer eigenständigen Instanz AWS-Konto
AWS Zugriffsportal für Single-Sign-On-Zugriff auf Ihre AWS verwalteten Anwendungen	 Ja	 Ja	 Ja
Vom Kunden verwaltete OAuth 2.0 (OIDC) -Anwendungen	 Ja	 Ja	 Ja
Berechtigungen für mehrere Konten	 Ja	 N	 Nein
AWS Zugangsportal für Single-Sign-On-Zugriff auf Ihre AWS-Konten	 Ja	 N	 Nein
Von Kunden verwaltete SAML 2.0-Anwendungen	 Ja	 N	 Nein
Ein delegierter Administrator kann die Instanz verwalten	 Ja	 N	 Nein

Themen

- Organisationsinstanzen von IAM Identity Center
- Kontoinstanzen von IAM Identity Center

- Aktivieren Sie Kontoinstanzen in der IAM Identity Center-Konsole
- Steuern Sie die Erstellung von Kontoinstanzen mit Services Control-Richtlinien
- Erstellen Sie eine Kontoinstanz von IAM Identity Center

Organisationsinstanzen von IAM Identity Center

Wenn Sie IAM Identity Center in Verbindung mit aktivieren AWS Organizations, erstellen Sie eine Organisationsinstanz von IAM Identity Center. Ihre Organisationsinstanz muss in Ihrem Verwaltungskonto aktiviert sein und Sie können den Zugriff von Benutzern und Gruppen mit einer einzigen Organisationsinstanz zentral verwalten. Sie können nur eine Organisationsinstanz für jedes Verwaltungskonto in haben AWS Organizations.

Wenn Sie IAM Identity Center vor dem 15. November 2023 aktiviert haben, verfügen Sie über eine Organisationsinstanz von IAM Identity Center.

Wann sollte eine Organisationsinstanz verwendet werden

Eine Organisationsinstanz ist die primäre Methode zur Aktivierung von IAM Identity Center. In den meisten Fällen wird eine Organisationsinstanz empfohlen. Organisationsinstanzen bieten die folgenden Vorteile:

- Support für alle Funktionen von IAM Identity Center — einschließlich der Verwaltung von Berechtigungen für mehrere Personen AWS-Konten in Ihrem Unternehmen und der Zuweisung von Zugriff auf vom Kunden verwaltete Anwendungen.
- Reduzieren Sie die Anzahl der Verwaltungspunkte — Eine Organisationsinstanz hat einen einzigen Verwaltungspunkt, das Verwaltungskonto. Wir empfehlen, eine Organisationsinstanz anstelle einer Kontoinstanz zu aktivieren, um die Anzahl der Verwaltungspunkte zu reduzieren.
- Steuern Sie die Erstellung von Kontoinstanzen — Sie können steuern, ob Kontoinstanzen von Mitgliedskonten in Ihrer Organisation erstellt werden können, solange Sie Ihrer Organisation keine Instanz von IAM Identity Center in einer Opt-in-Region bereitgestellt haben (AWS-Region die standardmäßig deaktiviert ist).

Kontoinstanzen von IAM Identity Center

Mit einer Kontoinstanz von IAM Identity Center können Sie unterstützte AWS verwaltete Anwendungen und OIDC-basierte, vom Kunden verwaltete Anwendungen bereitstellen.

Kontoinstanzen unterstützen die isolierte Bereitstellung von Anwendungen in einer einzigen AWS-Konto Lösung und nutzen dabei die Funktionen des IAM Identity Center für Personalidentität und Zugriff auf das IAM Identity Center.

Kontoinstanzen sind an ein einzelnes Konto gebunden AWS-Konto und werden nur zur Verwaltung des Benutzer- und Gruppenzugriffs auf unterstützte Anwendungen im selben Konto und verwendet. AWS-Region Sie sind auf eine Kontoinstanz pro Konto beschränkt AWS-Konto. Sie können eine Kontoinstanz aus einer der folgenden Optionen erstellen:

- Ein Mitgliedskonto in AWS Organizations.
- Ein eigenständiges AWS-Konto Gerät, das nicht von verwaltet wird AWS Organizations.

Verfügbarkeitsbeschränkungen für Mitgliedskonten

Sie können eine Kontoinstanz in einem Mitgliedskonto einer Organisation bereitstellen, wenn Folgendes zutrifft:

- Vor dem 15. November 2023 wurde in Ihrer Organisation keine Instanz von IAM Identity Center bereitgestellt.
- Sie haben bereits vor dem 15. November 2023 eine Instanz von IAM Identity Center in Ihrer Organisation bereitgestellt, und Ihr Administrator hat Mitgliedskonten aktiviert, um Kontoinstanzen von IAM Identity Center zu erstellen.
- Ihr Administrator hat keine Service Control-Richtlinie erstellt, die verhindert, dass Mitgliedskonten Kontoinstanzen erstellen.
- Sie haben noch keine Instanz von IAM Identity Center in demselben Konto, unabhängig davon AWS-Region.
- Sie arbeiten in einem Land, in AWS-Region dem IAM Identity Center nicht verfügbar ist. Informationen zu Regionen finden Sie unterAWS IAM Identity Center Verfügbarkeit in der Region.

Themen

Wann sollten Kontoinstanzen verwendet werden

In den meisten Fällen wird eine Organisationsinstanz empfohlen. Kontoinstanzen sollten nur verwendet werden, wenn eines der folgenden Szenarien zutrifft:

- Sie möchten eine temporäre Testversion einer unterstützten AWS verwalteten Anwendung ausführen, um festzustellen, ob die Anwendung Ihren Geschäftsanforderungen entspricht.
- Sie haben nicht vor, IAM Identity Center in Ihrem Unternehmen einzuführen, möchten aber eine oder mehrere AWS verwaltete Anwendungen unterstützen.
- Sie haben eine Organisationsinstanz von IAM Identity Center, möchten aber eine unterstützte AWS verwaltete Anwendung für eine isolierte Gruppe von Benutzern bereitstellen, die sich von den Benutzern in Ihrer Organisationsinstanz unterscheiden.

> **Important**
>
> Wenn Sie planen, IAM Identity Center zur Unterstützung von Anwendungen in mehreren Konten zu verwenden, erstellen Sie eine Organisationsinstanz und verwenden Sie keine Kontoinstanzen.

Überlegungen zu Kontoinstanzen

Eine Kontoinstanz ist für spezielle Anwendungsfälle konzipiert und bietet eine Teilmenge der Funktionen, die einer Organisationsinstanz zur Verfügung stehen. Beachten Sie Folgendes, bevor Sie eine Kontoinstanz erstellen:

- Kontoinstanzen unterstützen keine Berechtigungssätze und unterstützen daher auch keinen Zugriff auf AWS-Konten.
- Sie können eine Kontoinstanz nicht in eine Organisationsinstanz konvertieren.
- Sie können eine Kontoinstanz nicht mit einer Organisationsinstanz zusammenführen.
- Nur ausgewählte AWS verwaltete Anwendungen Support-Kontoinstanzen.
- Verwenden Sie Kontoinstanzen für isolierte Benutzer, die Anwendungen nur in einem einzigen Konto und für die gesamte Lebensdauer der verwendeten Anwendungen verwenden.
- Anwendungen, die mit einer Kontoinstanz verknüpft sind, müssen an die Kontoinstanz angehängt bleiben, bis Sie die Anwendung und ihre Ressourcen löschen.

- Eine Kontoinstanz muss dort verbleiben AWS-Konto , wo sie erstellt wurde.

AWS verwaltete Anwendungen, die Kontoinstanzen unterstützen

Erfahren AWS verwaltete Anwendungen Sie, welche AWS verwalteten Anwendungen Kontoinstanzen von IAM Identity Center unterstützen. Überprüfen Sie die Verfügbarkeit der Kontoinstanzerstellung mit Ihrer AWS verwalteten Anwendung.

Aktivieren Sie Kontoinstanzen in der IAM Identity Center-Konsole

Wenn Sie IAM Identity Center vor dem 15. November 2023 aktiviert haben, verfügen Sie über eine Organisationsinstanz von IAM Identity Center und die Möglichkeit, dass Mitgliedskonten Kontoinstanzen erstellen können, ist standardmäßig deaktiviert. Sie können wählen, ob Ihre Mitgliedskonten Kontoinstanzen erstellen können, indem Sie die Kontoinstanzfunktion in der aktivieren. AWS Management Console

> **Note**
>
> Mitgliedskonten können unabhängig vom Bereitstellungsdatum eine Kontoinstanz erstellen, sofern Sie in Ihrer Organisation keine Instanz von IAM Identity Center in einer Region bereitgestellt haben (AWS-Region die standardmäßig deaktiviert ist). Jede Organisationsinstanz von IAM Identity Center, die in einem Opt-In bereitgestellt AWS-Region wird, verhindert die Erstellung von Kontoinstanzen. Informationen zu Regionen finden Sie unter. AWS IAM Identity Center Verfügbarkeit in der Region

So ermöglichen Sie die Erstellung von Kontoinstanzen durch Mitgliedskonten in Ihrer Organisation

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Einstellungen und dann die Registerkarte Verwaltung.
3. Wählen Sie im Abschnitt Kontoinstanzen von IAM Identity Center die Option Kontoinstanzen von IAM Identity Center aktivieren aus.
4. Bestätigen Sie im Dialogfeld Kontoinstanzen von IAM Identity Center aktivieren, dass Sie Mitgliedskonten in Ihrer Organisation die Erstellung von Kontoinstanzen ermöglichen möchten, indem Sie Aktivieren wählen.

> **Important**
>
> Das Aktivieren von Kontoinstanzen von IAM Identity Center für Mitgliedskonten ist ein einmaliger Vorgang. Das bedeutet, dass dieser Vorgang nicht rückgängig gemacht werden kann. Nach der Aktivierung können Sie die Erstellung von Kontoinstanzen einschränken, indem Sie eine Service Control Policy (SCP) erstellen. Anweisungen finden Sie unter Steuern der Erstellung von Kontoinstanzen mit Services Control-Richtlinien.

Steuern Sie die Erstellung von Kontoinstanzen mit Services Control-Richtlinien

Benutzer können eine Instanz von IAM Identity Center erstellen, die an eine einzelne Instanz gebunden ist AWS-Konto, die als Kontoinstanz von IAM Identity Center bezeichnet wird. Sie können die Erstellung von Kontoinstanzen mit Service Control Policies (SCP) steuern.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie auf dem Dashboard im Bereich Zentrale Verwaltung die Schaltfläche Kontoinstanzen verhindern.
3. Im Dialogfeld SCP anhängen, um die Erstellung neuer Kontoinstanzen zu verhindern, wird ein SCP für Sie bereitgestellt. Kopieren Sie das SCP und wählen Sie die Dashboard-Schaltfläche Gehe zu SCP. Sie werden zur AWS Organizations Konsole weitergeleitet, um das SCP zu erstellen oder es als Statement an ein bestehendes SCP anzuhängen.

   Richtlinien zur Servicesteuerung sind ein Feature von. AWS OrganizationsAnweisungen zum Anhängen eines SCP finden Sie im Benutzerhandbuch unter Dienststeuerungsrichtlinien anhängen und trennen.AWS Organizations

Anstatt die Erstellung von Kontoinstanzen zu verhindern, können Sie die Erstellung von Kontoinstanzen auf eine bestimmte AWS-Konto Instanz innerhalb Ihrer Organisation beschränken:

Example : SCP zur Steuerung der Instanzerstellung

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

```
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

Erstellen Sie eine Kontoinstanz von IAM Identity Center

Eine Organisationsinstanz ist die primäre und empfohlene Methode zur Aktivierung von IAM Identity Center. Stellen Sie sicher, dass Ihr Anwendungsfall die Erstellung einer Kontoinstanz unterstützt und dass Sie sich der Überlegungen bewusst sind.

Erstellen Sie eine Kontoinstanz über ein Mitgliedskonto einer Organisation oder über ein eigenständiges Konto AWS-Konto

1. Führen Sie einen der folgenden Schritte aus, um sich bei der anzumelden AWS Management Console.
   - Neu bei AWS (Root-Benutzer) — Melden Sie sich als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.
   - Verwenden Sie bereits AWS (IAM-Anmeldeinformationen) — Melden Sie sich mit Ihren IAM-Anmeldeinformationen mit Administratorrechten an.
2. Öffnen Sie die IAM Identity Center-Konsole.
3. Wählen Sie unter IAM Identity Center aktivieren die Option Aktivieren aus.
4. Wählen Sie Mit der Erstellung der Kontoinstanz fortfahren und dann Weiter aus.

> **Note**
>
> Wenn eine Organisationsinstanz von IAM Identity Center vorhanden ist, stellen Sie sicher, dass Ihr Anwendungsfall eine eigene Kontoinstanz von IAM Identity Center erfordert. Ist dies nicht der Fall, wählen Sie Abbrechen und verwenden Sie die Organisationsinstanz.

5. Optional. Fügen Sie Tags hinzu, die Sie dieser Kontoinstanz zuordnen möchten.

Eine Benachrichtigung in der Konsole weist darauf hin, dass eine erfolgreiche Kontoinstanz erstellt wurde, und enthält die Instanz-ID. Sie können Ihrer Instanz in der Zusammenfassung der Einstellungen einen Namen geben.

> **Note**
>
> Die Multi-Faktor-Authentifizierung (MFA) ist standardmäßig für Kontoinstanzen aktiviert. Benutzer werden aufgefordert, sich mit MFA anzumelden, wenn sich ihr Gerät, ihr Browser oder ihr Standort ändert. Als bewährte Sicherheitsmethode empfehlen wir dringend MFA für Ihre Mitarbeiteridentitäten. Erfahren Sie mehr über MFA-Geräte im IAM Identity Center verwalten.

Verwaltungsfunktionen wie die Bestätigung Ihrer Identitätsquelle, die Anpassung der Einstellungen für die Multi-Faktor-Authentifizierung und das Hinzufügen AWS verwalteter Anwendungen müssen in der IAM Identity Center-Konsole abgeschlossen werden.

Authentifizierung

Ein Benutzer meldet sich mit seinem Benutzernamen beim AWS Access Portal an. In diesem Fall leitet IAM Identity Center die Anfrage auf der Grundlage des mit der Benutzer-E-Mail-Adresse verknüpften Verzeichnisses an den IAM Identity Center-Authentifizierungsdienst weiter. Nach der Authentifizierung haben Benutzer Single Sign-On-Zugriff auf alle AWS Konten und Drittanbieteranwendungen software-as-a-service (SaaS), die im Portal angezeigt werden, ohne dass zusätzliche Anmeldeaufforderungen erforderlich sind. Das bedeutet, dass Benutzer nicht mehr mehrere Kontoanmeldeinformationen für die verschiedenen zugewiesenen AWS Anwendungen nachverfolgen müssen, die sie täglich verwenden.

Authentifizationssitzungen

Es gibt zwei Arten von Authentifizierungssitzungen, die von IAM Identity Center verwaltet werden: eine, die die Anmeldung der Benutzer bei IAM Identity Center darstellt, und eine andere, die den Zugriff der Benutzer auf AWS verwaltete Anwendungen wie Amazon SageMaker Studio oder Amazon Managed Grafana darstellt. Jedes Mal, wenn sich ein Benutzer bei IAM Identity Center anmeldet, wird eine Anmeldesitzung für die in IAM Identity Center konfigurierte Dauer erstellt, die bis zu 90 Tage betragen kann. Weitere Informationen finden Sie unter Verwalten Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen. Jedes Mal, wenn der Benutzer auf eine Anwendung zugreift, wird die IAM Identity Center-Anmeldesitzung verwendet, um eine IAM Identity Center-Anwendungssitzung für diese Anwendung zu erhalten. IAM Identity Center-Anwendungssitzungen haben eine aktualisierbare Nutzungsdauer von einer Stunde. Das heißt, IAM Identity Center-Anwendungssitzungen werden automatisch jede Stunde aktualisiert, solange die IAM Identity Center-Anmeldesitzung, aus der sie abgerufen wurden, noch gültig ist. Wenn der Benutzer IAM Identity Center verwendet, um auf die AWS Management Console oder CLI zuzugreifen, wird die IAM Identity Center-Anmeldesitzung verwendet, um eine IAM-Sitzung zu erhalten, wie im entsprechenden IAM Identity Center-Berechtigungssatz angegeben (genauer gesagt, IAM Identity Center nimmt eine IAM-Rolle an, die IAM Identity Center im Zielkonto verwaltet).

Wenn Sie einen Benutzer in IAM Identity Center deaktivieren oder löschen, wird dieser Benutzer sofort daran gehindert, sich anzumelden, um neue IAM Identity Center-Anmeldesitzungen zu erstellen. IAM Identity Center-Anmeldesitzungen werden für eine Stunde zwischengespeichert. Wenn Sie also einen Benutzer deaktivieren oder löschen, während er eine aktive IAM Identity Center-Anmeldesitzung hat, wird seine bestehende IAM Identity Center-Anmeldesitzung bis zu einer Stunde

fortgesetzt, je nachdem, wann die Anmeldesitzung zuletzt aktualisiert wurde. Während dieser Zeit kann der Benutzer neue IAM Identity Center-Anwendungs- und IAM-Rollensitzungen initiieren.

Nach Ablauf der IAM Identity Center-Anmeldesitzung kann der Benutzer keine neuen IAM Identity Center-Anwendungs- oder IAM-Rollensitzungen mehr initiieren. IAM Identity Center-Anwendungssitzungen können jedoch auch bis zu einer Stunde zwischengespeichert werden, sodass der Benutzer nach Ablauf der IAM Identity Center-Anmeldesitzung bis zu einer Stunde Zugriff auf eine Anwendung behalten kann. Alle bestehenden IAM-Rollensitzungen werden auf der Grundlage der Dauer fortgesetzt, die im IAM Identity Center-Berechtigungssatz konfiguriert ist (vom Administrator konfigurierbar, bis zu 12 Stunden).

In der folgenden Tabelle sind diese Verhaltensweisen zusammengefasst:

Benutzererfahrung/Systemverhalten	Zeit nach dem Deaktivieren/Löschen des Benutzers
Der Benutzer kann sich nicht mehr bei IAM Identity Center anmelden; der Benutzer kann keine neue IAM Identity Center-Anmeldesitzung abrufen	Keine (mit sofortiger Wirkung)
Der Benutzer kann keine neuen Anwendung s- oder IAM-Rollensitzungen mehr über IAM Identity Center starten	Bis zu 1 Stunde
Der Benutzer kann nicht mehr auf Anwendung en zugreifen (alle Anwendungssitzungen werden beendet)	Bis zu 2 Stunden (bis zu 1 Stunde für den Ablauf der IAM Identity Center-Anmeldesitzung plus bis zu 1 Stunde für den Ablauf der IAM Identity Center-Anwendungssitzung)
Der Benutzer kann AWS-Konten über IAM Identity Center nicht mehr auf diese zugreifen	Bis zu 13 Stunden (bis zu 1 Stunde für den Ablauf der IAM Identity Center-Anmeldesitz ung plus bis zu 12 Stunden für den vom Administrator konfigurierten Ablauf der IAM-Rollensitzung gemäß den Einstellungen für die Dauer der IAM Identity Center-Sitzung für den Berechtigungssatz)

Weitere Informationen zu Sitzungen finden Sie unter Legen Sie die Sitzungsdauer fest.

Personalidentitäten verwalten

AWS Identity and Access Management(IAM) hilft Ihnen dabei, Identitäten und den Zugriff auf AWS Dienste und Ressourcen sicher zu verwalten. Als IAM-Service können Sie die Identitäten Ihrer Mitarbeiter auf AWS einmal erstellen oder verbinden und den Zugriff auf Ihre Anwendungen zentral verwalten. AWS IAM Identity Center AWS-Konten

Für Kunden von IAM Identity Center ändert sich nichts daran, wie Sie den Zugriff auf mehrere AWS-Konten Anwendungen zentral verwalten. Für Neukunden von IAM Identity Center können Sie IAM Identity Center flexibel so konfigurieren, dass es parallel zur AWS-Konto Einzelzugriffsverwaltung mit IAM läuft oder diese ersetzt.

Themen

Anwendungsfälle

Im Folgenden finden Sie Anwendungsfälle, die zeigen, wie Sie IAM Identity Center verwenden können, um unterschiedliche Geschäftsanforderungen zu erfüllen.

Themen

Aktivieren Sie den Single Sign-On-Zugriff auf Ihre AWS Anwendungen (Anwendungsadministratorrolle)

Dieser Anwendungsfall bietet Hilfestellung, wenn Sie ein Anwendungsadministrator sind, der AWS verwaltete Anwendungen beispielsweise Amazon SageMaker oder verwaltetAWS IoT SiteWise, und Sie Ihren Benutzern Single Sign-On-Zugriff gewähren müssen.

Bevor Sie beginnen, sollten Sie Folgendes beachten:

- Möchten Sie eine Test- oder Produktionsumgebung in einer separaten Organisation in erstellenAWS Organizations?
- Ist IAM Identity Center in Ihrer Organisation bereits aktiviert? Haben Sie die Berechtigung, IAM Identity Center im Verwaltungskonto von zu aktivieren? AWS Organizations

Lesen Sie sich die folgenden Hinweise durch, um die nächsten Schritte auf der Grundlage Ihrer Geschäftsanforderungen festzulegen.

Meine AWS Anwendung als eigenständige Anwendung konfigurieren AWS-Konto

Wenn Sie Single Sign-On-Zugriff auf eine AWS Anwendung gewähren müssen und wissen, dass Ihre IT-Abteilung IAM Identity Center noch nicht verwendet, müssen Sie zunächst möglicherweise eine eigenständige AWS-Konto Anwendung erstellen. Wenn Sie Ihre eigene Organisation erstellenAWS-Konto, verfügen Sie standardmäßig über die erforderlichen Berechtigungen, um Ihre eigene AWS Organisation zu erstellen und zu verwalten. Um IAM Identity Center zu aktivieren, benötigen Sie Root-Benutzer des AWS-Kontos Berechtigungen.

IAM Identity Center und AWS Organizations kann bei der Einrichtung für einige AWS Anwendungen (z. B. Amazon Managed Grafana) automatisch aktiviert werden. Wenn Ihre AWS Anwendung keine Option zur Aktivierung dieser Dienste bietet, müssen Sie ein IAM Identity Center einrichtenAWS Organizations, bevor Sie Single Sign-On-Zugriff auf Ihre Anwendung gewähren können.

IAM Identity Center ist in meiner Organisation nicht konfiguriert

In Ihrer Rolle als Anwendungsadministrator können Sie IAM Identity Center je nach Ihren Berechtigungen möglicherweise nicht aktivieren. Für IAM Identity Center sind bestimmte Berechtigungen im AWS Organizations Verwaltungskonto erforderlich. Wenden Sie sich in diesem Fall an den entsprechenden Administrator, damit IAM Identity Center im Verwaltungskonto der Organizations aktiviert wird.

Wenn Sie über ausreichende Berechtigungen verfügen, um IAM Identity Center zu aktivieren, tun Sie dies zuerst und fahren Sie dann mit der Einrichtung der Anwendung fort. Weitere Informationen finden Sie unter Erste Schritte mit allgemeinen Aufgaben in IAM Identity Center.

IAM Identity Center ist derzeit in meiner Organisation konfiguriert

In diesem Szenario können Sie Ihre AWS Anwendung weiter bereitstellen, ohne weitere Maßnahmen ergreifen zu müssen.

> **Note**
>
> Wenn Ihre Organisation IAM Identity Center vor dem 25. November 2019 im Verwaltungskonto aktiviert hat, müssen Sie AWS verwaltete Anwendungen auch im Verwaltungskonto und optional in den Mitgliedskonten aktivieren. Wenn Sie sie nur im Verwaltungskonto aktivieren, können Sie sie später in Mitgliedskonten aktivieren. Um diese Anwendungen zu aktivieren, wählen Sie auf der Einstellungsseite der IAM Identity Center-Konsole im Abschnitt AWS Verwaltete Anwendungen die Option Zugriff aktivieren. Weitere Informationen finden Sie unter Konfiguration von IAM Identity Center für die gemeinsame Nutzung von Identitätsinformationen .

Aktivieren Sie den Single Sign-On-Zugriff auf Ihre Amazon EC2 EC2-Windows-Instances

Sie können den Single Sign-On-Zugriff auf Ihre Amazon EC2 Windows-Instances aktivieren, wenn Sie ein Anwendungsadministrator sind, der Benutzer im Identity Center-Verzeichnis (der Standard-Identitätsquelle für IAM Identity Center) verwaltet, oder ein unterstützter externer Identitätsanbieter (IdP), und Sie müssen IAM Identity Center-Zugriff auf Ihre Amazon EC2 EC2-Windows-Desktops von der Fleet Manager-Konsole aus gewähren. AWS

Mit dieser Konfiguration können Sie mit vorhandenen Unternehmensanmeldedaten sicher auf Ihre Amazon EC2 Windows-Instances zugreifen. Sie müssen Administratoranmeldedaten und Zugangsdaten nicht mehrfach weitergeben oder die Client-Software für den Fernzugriff konfigurieren. Sie können den Zugriff auf Ihre Amazon EC2 Windows-Instances zentral gewähren und entziehen, und zwar in großem Umfang für mehrereAWS-Konten. Wenn Sie beispielsweise einen Mitarbeiter aus Ihrer integrierten Identitätsquelle im IAM Identity Center entfernen, verliert dieser automatisch den Zugriff auf alle AWS Ressourcen, einschließlich Amazon EC2 EC2-Windows-Instances.

Weitere Informationen finden Sie unter So aktivieren Sie sicheres, nahtloses Single Sign-On für Amazon EC2 EC2-Windows-Instances mit IAM Identity Center.

Eine Demonstration der Konfiguration von IAM Identity Center zur Aktivierung dieser Funktion finden Sie unter Aktivieren von Single Sign-On für Amazon EC2 Windows mit IAM Identity Center.

Benutzer, Gruppen und Bereitstellung

Beachten Sie bei der Arbeit mit Benutzern und Gruppen in IAM Identity Center die folgenden Überlegungen.

Eindeutigkeit von Benutzername und E-Mail-Adresse

Benutzer in IAM Identity Center müssen eindeutig identifizierbar sein. IAM Identity Center implementiert einen Benutzernamen, der die primäre Kennung für Ihre Benutzer ist. Obwohl die meisten Benutzer den Benutzernamen mit der E-Mail-Adresse eines Benutzers gleichsetzen, ist dies bei IAM Identity Center und dem SAML 2.0-Standard nicht erforderlich. Viele SAML 2.0-basierte Anwendungen verwenden jedoch eine E-Mail-Adresse als eindeutige Kennung für Benutzer. Diese Anwendungen beziehen diese Informationen aus Assertions, die ein SAML 2.0-Identitätsanbieter während der Authentifizierung sendet. Solche Anwendungen hängen von der Einzigartigkeit der E-Mail-Adressen für jeden Benutzer ab. Aus diesem Grund können Sie in IAM Identity Center für die Benutzeranmeldung etwas anderes als eine E-Mail-Adresse angeben. IAM Identity Center erfordert, dass alle Benutzernamen und E-Mail-Adressen Ihrer Benutzer ungleich NULL und eindeutig sind.

Gruppen

Gruppen sind eine logische Kombination von Benutzern, die Sie definieren. Sie können Gruppen erstellen und Benutzer zu den Gruppen hinzufügen. IAM Identity Center unterstützt nicht das Hinzufügen einer Gruppe zu einer Gruppe (verschachtelte Gruppen). Gruppen sind nützlich, wenn Sie Zugriff auf Anwendungen zuweisen möchtenAWS-Konten. Anstatt jeden Benutzer einzeln zuzuweisen, erteilen Sie einer Gruppe Berechtigungen. Wenn Sie später Benutzer zu einer Gruppe hinzufügen oder daraus entfernen, erhält oder verliert der Benutzer dynamisch Zugriff auf Konten und Anwendungen, die Sie der Gruppe zugewiesen haben.

Bereitstellung von Benutzern und Gruppen

Bei der Bereitstellung werden Benutzer- und Gruppeninformationen für die Verwendung durch IAM Identity Center und AWS verwaltete Anwendungen oder kundenverwaltete Anwendungen zur Verfügung gestellt. Sie können Benutzer und Gruppen direkt in IAM Identity Center erstellen oder mit Benutzern und Gruppen arbeiten, die Sie in Active Directory oder einem externen Identitätsanbieter haben. Bevor Sie IAM Identity Center verwenden können, um Benutzern und Gruppen Zugriffsberechtigungen in einem zuzuweisenAWS-Konto, muss IAM Identity Center die Benutzer und Gruppen kennen. Ebenso können AWS verwaltete Anwendungen und vom Kunden

verwaltete Anwendungen mit Benutzern und Gruppen funktionieren, die IAM Identity Center bekannt sind.

Die Bereitstellung in IAM Identity Center hängt von der verwendeten Identitätsquelle ab. Weitere Informationen finden Sie unter Verwalte deine Identitätsquelle.

Verwalte deine Identitätsquelle

Ihre Identitätsquelle in IAM Identity Center definiert, wo Ihre Benutzer und Gruppen verwaltet werden. Nachdem Sie Ihre Identitätsquelle konfiguriert haben, können Sie nach Benutzern oder Gruppen suchen, um ihnen Single Sign-On-Zugriff auf AWS-Konten Anwendungen oder beides zu gewähren.

Sie können pro Organisation nur eine Identitätsquelle haben. AWS Organizations Sie können eine der folgenden Optionen als Identitätsquelle wählen:

- Identity Center-Verzeichnis — Wenn Sie IAM Identity Center zum ersten Mal aktivieren, wird es automatisch mit einem Identity Center-Verzeichnis als Standard-Identitätsquelle konfiguriert. Hier erstellen Sie Ihre Benutzer und Gruppen und weisen deren Zugriffsebene Ihren Anwendungen AWS-Konten zu.
- Active Directory — Wählen Sie diese Option, wenn Sie weiterhin Benutzer in Ihrem AWS Managed Microsoft AD Verzeichnis AWS Directory Service oder in Active Directory (AD) Ihrem selbst verwalteten Verzeichnis verwalten möchten.
- Externer Identitätsanbieter — Wählen Sie diese Option, wenn Sie Benutzer in einem externen Identitätsanbieter (IdP) wie Okta oder Microsoft Entra ID verwalten möchten.

> **Note**
>
> IAM Identity Center unterstützt SAMBA4-basiertes Simple AD nicht als Identitätsquelle.

Themen

- Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis
- Stellen Sie eine Connect zu einem externen Identitätsanbieter her

Überlegungen zum Ändern Ihrer Identitätsquelle

Obwohl Sie Ihre Identitätsquelle jederzeit ändern können, empfehlen wir Ihnen, zu überlegen, wie sich diese Änderung auf Ihre aktuelle Bereitstellung auswirken kann.

Wenn Sie bereits Benutzer und Gruppen in einer Identitätsquelle verwalten, entfernt ein Wechsel zu einer anderen Identitätsquelle möglicherweise alle Benutzer- und Gruppenzuweisungen, die Sie in IAM Identity Center konfiguriert haben. In diesem Fall verlieren alle Benutzer, einschließlich des Administratorbenutzers im IAM Identity Center, den Single-Sign-On-Zugriff auf ihre AWS-Konten und Anwendungen.

Bevor Sie die Identitätsquelle für IAM Identity Center ändern, lesen Sie die folgenden Überlegungen, bevor Sie fortfahren. Wenn Sie mit dem Ändern Ihrer Identitätsquelle fortfahren möchten, finden Sie weitere Informationen unter Ändern Sie Ihre Identitätsquelle .

Wechseln zwischen IAM Identity Center und Active Directory

Wenn Sie bereits Benutzer und Gruppen in Active Directory verwalten, empfehlen wir Ihnen, Ihr Verzeichnis zu verbinden, wenn Sie IAM Identity Center aktivieren und Ihre Identitätsquelle auswählen. Tun Sie dies, bevor Sie Benutzer und Gruppen im Standardverzeichnis von Identity Center erstellen und Zuweisungen vornehmen.

Wenn Sie bereits Benutzer und Gruppen im Standardverzeichnis von Identity Center verwalten, sollten Sie Folgendes berücksichtigen:

- Zuweisungen entfernt und Benutzer und Gruppen gelöscht – Wenn Sie Ihre Identitätsquelle in Active Directory ändern, werden Ihre Benutzer und Gruppen aus dem Identity-Center-Verzeichnis gelöscht. Durch diese Änderung werden auch Ihre Zuweisungen entfernt. In diesem Fall müssen Sie nach dem Wechsel zu Active Directory Ihre Benutzer und Gruppen von Active Directory in das Identity-Center-Verzeichnis synchronisieren und dann ihre Zuweisungen erneut anwenden.

  Wenn Sie Active Directory nicht verwenden möchten, müssen Sie Ihre Benutzer und Gruppen im Identity-Center-Verzeichnis erstellen und dann Zuweisungen vornehmen.
- Zuweisungen werden nicht gelöscht, wenn Identitäten gelöscht werden – Wenn Identitäten im Identity-Center-Verzeichnis gelöscht werden, werden entsprechende Zuweisungen auch im IAM

Identity Center gelöscht. Wenn jedoch Identitäten in Active Directory gelöscht werden (entweder in Active Directory oder den synchronisierten Identitäten), werden entsprechende Zuweisungen nicht gelöscht.

- Keine ausgehende Synchronisation für APIs – Wenn Sie Active Directory als Identitätsquelle verwenden, empfehlen wir Ihnen, die APIs zum Erstellen, Aktualisieren und Löschen mit Vorsicht zu verwenden. IAM Identity Center unterstützt keine ausgehende Synchronisation, sodass Ihre Identitätsquelle nicht automatisch mit den Änderungen aktualisiert wird, die Sie mit diesen APIs an Benutzern oder Gruppen vornehmen.
- Die URL des Zugriffsportals ändert sich – Das Ändern Ihrer Identitätsquelle zwischen IAM Identity Center und Active Directory ändert auch die URL für das AWS Zugriffsportal.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis.

Wechseln von IAM Identity Center zu einem externen IdP

Wenn Sie Ihre Identitätsquelle von IAM Identity Center zu einem externen Identitätsanbieter (IdP) ändern, sollten Sie Folgendes berücksichtigen:

- Zuweisungen und Mitgliedschaften funktionieren mit korrekten Aussagen – Ihre Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Aussagen sendet (z. B. SAML-nameIDs Diese Aussagen müssen mit den Benutzernamen und Gruppen im IAM Identity Center übereinstimmen.
- Keine ausgehende Synchronisation – IAM Identity Center unterstützt keine ausgehende Synchronisation, sodass Ihr externer IdP nicht automatisch mit Änderungen an Benutzern und Gruppen aktualisiert wird, die Sie in IAM Identity Center vornehmen.
- SCIM-Bereitstellung – Wenn Sie die SCIM-Bereitstellung verwenden, werden Änderungen an Benutzern und Gruppen in Ihrem Identitätsanbieter erst in IAM Identity Center wiedergegeben, nachdem Ihr Identitätsanbieter diese Änderungen an IAM Identity Center gesendet hat. Siehe Überlegungen zur Verwendung der automatischen Bereitstellung.
- Rollback – Sie können Ihre Identitätsquelle jederzeit wieder mit IAM Identity Center verwenden. Siehe Wechseln von einem externen IdP zu IAM Identity Center.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter Stellen Sie eine Connect zu einem externen Identitätsanbieter her.

Wechseln von einem externen IdP zu IAM Identity Center

Wenn Sie Ihre Identitätsquelle von einem externen Identitätsanbieter (IdP) in IAM Identity Center ändern, sollten Sie Folgendes berücksichtigen:

- IAM Identity Center behält alle Ihre Zuweisungen bei.
- Zurücksetzen des Passworts erzwingen – Benutzer, die Passwörter im IAM Identity Center hatten, können sich weiterhin mit ihren alten Passwörtern anmelden. Für Benutzer, die sich im externen IdP befanden und sich nicht im IAM Identity Center befanden, muss ein Administrator das Zurücksetzen des Passworts erzwingen.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter Identitäten im IAM Identity Center verwalten.

Wechseln von einem externen IdP zu einem anderen externen IdP

Wenn Sie bereits einen externen IdP als Identitätsquelle für IAM Identity Center verwenden und zu einem anderen externen IdP wechseln, sollten Sie Folgendes berücksichtigen:

- Zuweisungen und Mitgliedschaften funktionieren mit korrekten Aussagen – IAM Identity Center behält alle Ihre Zuweisungen bei. Die Benutzerzuweisungen, Gruppenzuweisungen und Gruppenmitgliedschaften funktionieren weiterhin, solange der neue IdP die richtigen Assertionen sendet (z. B. SAMLnameIDs).

  Diese Aussagen müssen mit den Benutzernamen im IAM Identity Center übereinstimmen, wenn sich Ihre Benutzer über den neuen externen IdP authentifizieren.
- SCIM-Bereitstellung – Wenn Sie SCIM für die Bereitstellung in IAM Identity Center verwenden, empfehlen wir Ihnen, die IdP spezifischen Informationen in diesem Handbuch und in der vom IdP bereitgestellten Dokumentation zu lesen, um sicherzustellen, dass der neue Anbieter Benutzer und Gruppen korrekt zuordnet, wenn SCIM aktiviert ist.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter Stellen Sie eine Connect zu einem externen Identitätsanbieter her.

Wechseln zwischen Active Directory und einem externen IdP

Wenn Sie Ihre Identitätsquelle von einem externen IdP in Active Directory oder von Active Directory in einen externen IdP ändern, sollten Sie Folgendes berücksichtigen:

- Benutzer, Gruppen und Zuweisungen werden gelöscht – Alle Benutzer, Gruppen und Zuweisungen werden aus dem IAM Identity Center gelöscht. Benutzer- oder Gruppeninformationen sind weder im externen IdP noch im Active Directory betroffen.
- Bereitstellen von Benutzern – Wenn Sie zu einem externen IdP wechseln, müssen Sie IAM Identity Center für die Bereitstellung Ihrer Benutzer konfigurieren. Alternativ müssen Sie die Benutzer und Gruppen für den externen IdP manuell bereitstellen, bevor Sie Zuweisungen konfigurieren können.
- Zuweisungen und Gruppen erstellen – Wenn Sie zu Active Directory wechseln, müssen Sie Zuweisungen mit den Benutzern und Gruppen erstellen, die sich in Ihrem Verzeichnis in Active Directory befinden.

Informationen darüber, wie IAM Identity Center Benutzer und Gruppen bereitstellt, finden Sie unter Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis.

Ändern Sie Ihre Identitätsquelle

Im folgenden Verfahren wird beschrieben, wie Sie von einem von IAM Identity Center bereitgestellten Verzeichnis (dem standardmäßigen Identity Center-Verzeichnis) zu Active Directory oder einem externen Identitätsanbieter wechseln oder umgekehrt. Bevor Sie fortfahren, werden jedoch die folgenden Informationen unterÜberlegungen zum Ändern Ihrer Identitätsquelle. Abhängig von Ihrer aktuellen Bereitstellung werden durch diese Änderung möglicherweise alle Benutzer- und Gruppenzuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben. In diesem Fall verlieren alle Benutzer, einschließlich des administrativen Benutzers im IAM Identity Center, den Single Sign-On-Zugriff auf ihreAWS-Kontenund Anwendungen.

So ändern Sie Ihre Identitätsquelle

1. Öffne dasIAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Auf derEinstellungenSeite, wählen Sie dieIdentitätsquelleTabulator. WählenAktionenund dann wählenIdentitätsquelle ändern.
4. UnterWählen der Identitätsquelle, wählen Sie die Quelle aus, zu der Sie wechseln möchten, und wählen SieWeiter.

   Wenn Sie zu Active Directory wechseln, wählen Sie das verfügbare Verzeichnis aus dem Menü auf der nächsten Seite aus.

> **Important**
>
> Wenn Sie Ihre Identitätsquelle in oder aus Active Directory ändern, werden Benutzer und Gruppen aus dem Identity Center-Verzeichnis gelöscht. Durch diese Änderung werden auch alle Zuweisungen entfernt, die Sie in IAM Identity Center konfiguriert haben.

Wenn Sie zu einem externen Identitätsanbieter wechseln, werden jedoch die folgenden Schritte empfohlen, die unterWie stelle ich eine Verbindung zu einem externen Identitätsanbieter her.

5. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben SieAKZEPTIEREN.
6. WählenIdentitätsquelle ändern. Wenn Sie Ihre Identitätsquelle auf Active Directory ändern, fahren Sie mit dem nächsten Schritt fort.
7. Wenn Sie Ihre Identitätsquelle in Active Directory ändern, gelangen Sie zumEinstellungenSeite. Auf derEinstellungen. Führen Sie eine der folgenden Aufgaben aus:

   - WählenStarten der geführten Einrichtung. Weitere Informationen, wie Sie den geführten Einrichtungsvorgang durchführen können, finden Sie unterGeführte Einrichtung.
   - In derIdentitätsquelleAbschnitt, wählenAktionenund dann wählenVerwalten der Synchronisierungum IhreSynchronisierungsbereich, die Liste der zu synchronisierenden Benutzer und Gruppen.

Verwalten Sie die Anmeldung und die Verwendung von Attributen für alle Identitätsquellentypen

IAM Identity Center bietet die folgenden Funktionen, mit denen Administratoren die Nutzung des AWS Zugriffsportals steuern, die Sitzungsdauer für Benutzer im AWS Zugriffsportal und in Ihren Anwendungen festlegen und Attribute für die Zugriffskontrolle verwenden können. Diese Funktionen funktionieren mit einem Identity Center-Verzeichnis oder einem externen Identitätsanbieter als Identitätsquelle.

> **Note**
>
> Wenn Sie Active Directory als Identitätsquelle für IAM Identity Center verwenden, wird die Sitzungsverwaltung nicht unterstützt.

Themen

Verwalten Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen

Der IAM Identity Center-Administrator kann die Sitzungsdauer sowohl für in IAM Identity Center integrierte Anwendungen als auch für die konfigurieren. AWS-Zugangsportal Die Konfiguration der Sitzungsdauer bestimmt, wie oft sich Benutzer erneut authentifizieren müssen. Der IAM Identity Center-Administrator kann eine Active AWS Access-Portal-Sitzung beenden und damit auch die Sitzungen integrierter Anwendungen beenden.

Weitere Informationen finden Sie unter Konfigurieren Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen. Weitere Informationen zum Verwalten und Beenden von Benutzersitzungen finden Sie unterLöschen Sie Sitzungen für das AWS Access Portal und die AWS integrierten Anwendungen.

> **Note**
>
> Das Ändern der Sitzungsdauer des AWS Access-Portals und das Beenden der AWS Access-Portal-Sitzungen haben keine Auswirkungen auf die Sitzungsdauer der AWS Management Console, die Sie in Ihren Berechtigungssätzen definieren.

Konfigurieren Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen

Die Sitzungsdauer der Authentifizierung in den integrierten Anwendungen AWS-Zugangsportal und in IAM Identity Center entspricht der Höchstdauer, für die ein Benutzer angemeldet werden kann, ohne sich erneut zu authentifizieren. Die Standardsitzungsdauer beträgt 8 Stunden. Der IAM Identity Center-Administrator kann eine andere Dauer angeben, von mindestens 15 Minuten bis maximal 90

Tagen. Weitere Informationen zur Dauer der Authentifizierungssitzung und zum Benutzerverhalten finden Sie unterAuthentifizierung.

Die folgenden Themen enthalten Informationen zur Konfiguration der Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen.

Themen

- Voraussetzungen und Überlegungen
- Wie konfiguriert man die Sitzungsdauer

Voraussetzungen und Überlegungen

Im Folgenden werden die Voraussetzungen und Überlegungen für die Konfiguration der Sitzungsdauer für das AWS Zugriffsportal und die integrierten IAM Identity Center-Anwendungen beschrieben.

Externe Identitätsanbieter

IAM Identity Center verwendet `SessionNotOnOrAfter` Attribute aus SAML-Assertionen, um zu bestimmen, wie lange die Sitzung gültig sein kann.

- Wenn keine SAML-Assertion übergeben `SessionNotOnOrAfter` wird, wird die Dauer einer AWS Access-Portal-Sitzung nicht von der Dauer Ihrer externen IdP-Sitzung beeinflusst. Wenn Ihre IdP-Sitzung beispielsweise 24 Stunden dauert und Sie im IAM Identity Center eine Sitzungsdauer von 18 Stunden festlegen, müssen sich Ihre Benutzer nach 18 Stunden erneut im AWS Zugriffsportal authentifizieren.
- Wenn eine SAML-Assertion übergeben `SessionNotOnOrAfter` wird, wird der Wert für die Sitzungsdauer auf den kürzeren Wert der AWS Access-Portal-Sitzungsdauer und Ihrer SAML-IdP-Sitzungsdauer gesetzt. Wenn Sie in IAM Identity Center eine Sitzungsdauer von 72 Stunden festlegen und Ihr IdP eine Sitzungsdauer von 18 Stunden hat, haben Ihre Benutzer für die in Ihrem IdP definierten 18 Stunden Zugriff auf AWS Ressourcen.
- Wenn die Sitzungsdauer Ihres IdP länger ist als die in IAM Identity Center festgelegte, können Ihre Benutzer eine neue IAM Identity Center-Sitzung starten, ohne ihre Anmeldeinformationen erneut eingeben zu müssen, basierend auf ihrer noch gültigen Anmeldesitzung mit Ihrem IdP.

> **Note**
>
> Wenn Sie Active Directory als Identitätsquelle für IAM Identity Center verwenden, wird die Sitzungsverwaltung nicht unterstützt.

AWS CLI und SDK-Sitzungen

Wenn Sie AWS Software Development Kits (SDKs) oder andere AWS Entwicklungstools verwenden, um programmgesteuert auf AWS Dienste zuzugreifen, müssen die folgenden Voraussetzungen erfüllt sein, um die Sitzungsdauer für das AWS Access Portal und die integrierten IAM Identity Center-Anwendungen festzulegen. AWS Command Line Interface

- Sie müssen die Sitzungsdauer des AWS Zugriffsportals in der IAM Identity Center-Konsole konfigurieren.
- Sie müssen in Ihrer gemeinsam genutzten AWS Konfigurationsdatei ein Profil für Single Sign-On-Einstellungen definieren. Dieses Profil wird verwendet, um eine Verbindung zum AWS Zugriffsportal herzustellen. Wir empfehlen, die Konfiguration des SSO-Token-Anbieters zu verwenden. Mit dieser Konfiguration kann Ihr AWS SDK oder Tool automatisch aktualisierte Authentifizierungstoken abrufen. Weitere Informationen finden Sie unter Konfiguration des SSO-Token-Anbieters im AWS SDK- und Tools-Referenzhandbuch.
- Benutzer müssen eine Version des AWS CLI oder eines SDK ausführen, das die Sitzungsverwaltung unterstützt.

Mindestversionen von AWS CLI , die die Sitzungsverwaltung unterstützen

Im Folgenden sind die Mindestversionen von aufgeführt AWS CLI , die die Sitzungsverwaltung unterstützen.

- AWS CLI V2 2.9 oder höher
- AWS CLI V1 1.27.10 oder später

Informationen zur Installation oder Aktualisierung der neuesten AWS CLI Version finden Sie unter Installation oder Aktualisierung der neuesten Version von. AWS CLI

Wenn Ihre Benutzer das AWS CLI ausführen und Sie Ihren Berechtigungssatz kurz vor Ablauf der IAM Identity Center-Sitzung aktualisieren und die Sitzungsdauer auf 20 Stunden und die Dauer des

Berechtigungssatzes auf 12 Stunden festgelegt ist, läuft die AWS CLI Sitzung maximal 20 Stunden plus 12 Stunden insgesamt 32 Stunden. Weitere Informationen zur IAM Identity Center CLI finden Sie unter AWS CLI Befehlsreferenz.

Mindestversionen von SDKs, die das IAM Identity Center-Sitzungsmanagement unterstützen

Im Folgenden sind die Mindestversionen der SDKs aufgeführt, die die IAM Identity Center-Sitzungsverwaltung unterstützen.

SDK	Mindestversion
Python	1.26.10
PHP	3,245,0
Ruby	aws-sdk-core 3,167,0
Java V2	AWS SDK for Java v2 (2.18.13)
Gehe zu V2	Gesamtes SDK: Release-2022-11-11 und spezifische Go-Module: Credentials/v1.13.0, config/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Wie konfiguriert man die Sitzungsdauer

Gehen Sie wie folgt vor, um die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen zu konfigurieren.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.

4. Wählen Sie unter Authentifizierung neben Sitzungseinstellungen die Option Konfigurieren aus. Das Dialogfeld „Sitzungseinstellungen konfigurieren“ wird angezeigt.
5. Wählen Sie im Dialogfeld Sitzungseinstellungen konfigurieren die maximale Sitzungsdauer in Minuten, Stunden und Tagen für Ihre Benutzer aus, indem Sie auf den Dropdownpfeil klicken. Wählen Sie die Länge für die Sitzung aus und klicken Sie dann auf Speichern. Sie kehren zur Seite mit den Einstellungen zurück.

Löschen Sie Sitzungen für das AWS Access Portal und die AWS integrierten Anwendungen

Gehen Sie wie folgt vor, um aktive Sitzungen für einen IAM Identity Center-Benutzer anzuzeigen und zu löschen.

Um eine aktive Sitzung des AWS Access Portals und der integrierten IAM Identity Center-Anwendungen zu löschen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie auf der Seite Benutzer den Benutzernamen des Benutzers aus, dessen Sitzungen Sie verwalten möchten. Dadurch gelangen Sie zu einer Seite mit den Benutzerinformationen.
4. Wählen Sie auf der Seite des Benutzers die Registerkarte Aktive Sitzungen aus. Die Zahl in Klammern neben Aktive Sitzungen gibt die Anzahl der aktuell aktiven Sitzungen für diesen Benutzer an.
5. Aktivieren Sie die Kontrollkästchen neben den Sitzungen, die Sie löschen möchten, und wählen Sie dann Sitzung löschen aus. Es wird ein Dialogfeld angezeigt, das bestätigt, dass Sie aktive Sitzungen für diesen Benutzer löschen. Lesen Sie die Informationen im Dialogfeld, und wenn Sie fortfahren möchten, wählen Sie Sitzung löschen.
6. Sie kehren zur Seite des Benutzers zurück. Eine grüne Flash-Leiste zeigt an, dass die ausgewählten Sitzungen erfolgreich gelöscht wurden.

Weitere Informationen zum Verhalten widerrufener Authentifizierungssitzungen finden Sie unterAuthentifizationssitzungen.

Unterstützte Benutzer- und Gruppenattribute

Attribute sind Informationen, die Ihnen helfen, einzelne Benutzer- oder Gruppenobjekte wie `name`, `email`, oder zu definieren und zu identifizieren`members`. IAM Identity Center unterstützt die am häufigsten verwendeten Attribute, unabhängig davon, ob sie bei der Benutzererstellung manuell eingegeben oder automatisch mithilfe einer Synchronisierungs-Engine bereitgestellt werden, wie sie in der SCIM-Spezifikation (System for Cross-Domain Identity Management) definiert ist. Weitere Informationen zu dieser Spezifikation finden Sie unter https://tools.ietf.org/html/rfc7642. Weitere Informationen zur manuellen und automatischen Bereitstellung finden Sie unterBereitstellung, wenn Benutzer von einem externen IdP kommen.

Da IAM Identity Center SCIM für Anwendungsfälle der automatischen Bereitstellung unterstützt, unterstützt das Identity Center-Verzeichnis mit einigen Ausnahmen dieselben Benutzer- und Gruppenattribute, die in der SCIM-Spezifikation aufgeführt sind. In den folgenden Abschnitten wird beschrieben, welche Attribute von IAM Identity Center nicht unterstützt werden.

Benutzerobjekte

Alle Attribute aus dem SCIM-Benutzerschema (https://tools.ietf.org/html/rfc7643#section-8.3) werden im IAM Identity Center-Identitätsspeicher unterstützt, mit Ausnahme der folgenden:

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Alle Unterattribute für Benutzer werden unterstützt, mit Ausnahme der folgenden:

- `'display'`Unterattribut eines beliebigen Attributs mit mehreren Werten (z. B. oder) `emails` `phoneNumbers`
- `'version'`Unterattribut eines Attributs `'meta'`

Objekte gruppieren

Alle Attribute aus dem SCIM-Gruppenschema (https://tools.ietf.org/html/rfc7643#section-8.4) werden unterstützt.

Alle Unterattribute für Gruppen werden unterstützt, mit Ausnahme der folgenden:

- `'display'` Unterattribut eines beliebigen Attributs mit mehreren Werten (z. B. Mitglieder).

Identitäten im IAM Identity Center verwalten

IAM Identity Center bietet die folgenden Funktionen für Ihre Benutzer und Gruppen:

- Erstellen Sie Ihre Benutzer und Gruppen.
- Fügen Sie Ihre Benutzer den Gruppen als Mitglieder hinzu.
- Weisen Sie den Gruppen die gewünschte Zugriffsebene für Ihre Anwendungen AWS-Konten zu.

AWS Unterstützt die unter Identity Center-Aktionen aufgeführten API-Operationen zur Verwaltung von Benutzern und Gruppen im IAM Identity Center Store.

Bereitstellung, wenn sich Benutzer im IAM Identity Center befinden

Wenn Sie Benutzer und Gruppen direkt in IAM Identity Center erstellen, erfolgt die Bereitstellung automatisch. Diese Identitäten sind sofort für die Zuweisung von Aufgaben und für Anwendungen verfügbar. Weitere Informationen finden Sie unter Bereitstellung von Benutzern und Gruppen.

Ändern Sie Ihre Identitätsquelle

Wenn Sie es vorziehen, Benutzer in zu verwalten AWS Managed Microsoft AD, können Sie die Verwendung Ihres Identity Center-Verzeichnisses jederzeit beenden und stattdessen IAM Identity Center mit Ihrem Verzeichnis in Microsoft AD verbinden, indem AWS Directory Service Sie. Weitere Informationen finden Sie unter Überlegungen zuWechseln zwischen IAM Identity Center und Active Directory.

Wenn Sie es vorziehen, Benutzer in einem externen Identitätsanbieter (IdP) zu verwalten, können Sie IAM Identity Center mit Ihrem IdP verbinden und die automatische Bereitstellung aktivieren. Weitere Informationen finden Sie unter Überlegungen zu. Wechseln von IAM Identity Center zu einem externen IdP

Themen

- Hinzufügen von Benutzern
- Fügen Sie Gruppen hinzu
- Fügen Sie Benutzer zu Gruppen hinzu

- Löschen Sie Gruppen im IAM Identity Center
- Löschen Sie Benutzer im IAM Identity Center
- Deaktivieren Sie den Benutzerzugriff im IAM Identity Center
- Benutzereigenschaften bearbeiten
- Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück
- Senden Sie ein E-Mail-OTP für Benutzer, die über die API erstellt wurden
- Passwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center

Hinzufügen von Benutzern

Benutzer und Gruppen, die Sie in Ihrem Identity Center-Verzeichnis erstellen, sind nur in IAM Identity Center verfügbar. Gehen Sie wie folgt vor, um Benutzer mithilfe der IAM Identity Center-Konsole zu Ihrem Identity Center-Verzeichnis hinzuzufügen. Alternativ können Sie den AWS API-Vorgang aufrufen CreateUser, um Benutzer hinzuzufügen.

So fügen Sie einen Benutzer hinzu

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie Benutzer hinzufügen und geben Sie die folgenden erforderlichen Informationen ein:

    a. Benutzername — Dieser Benutzername ist für die Anmeldung am AWS Access Portal erforderlich und kann später nicht geändert werden. Er muss zwischen 1 und 100 Zeichen lang sein.

    b. Passwort — Sie können entweder eine E-Mail mit den Anweisungen zur Einrichtung des Passworts senden (dies ist die Standardoption) oder ein Einmalpasswort generieren. Wenn Sie einen Administratorbenutzer erstellen und sich dafür entscheiden, eine E-Mail zu senden, stellen Sie sicher, dass Sie eine E-Mail-Adresse angeben, auf die Sie zugreifen können.

        i. Senden Sie diesem Benutzer eine E-Mail mit Anweisungen zur Einrichtung des Passworts. — Diese Option sendet dem Benutzer automatisch eine von Amazon Web Services adressierte E-Mail mit der Betreffzeile Einladung zum Beitritt AWS IAM Identity Center (Nachfolger von AWS Single Sign-On). In der E-Mail wird der Benutzer im Namen Ihres Unternehmens aufgefordert, auf das Zugriffsportal für das IAM Identity Center AWS zuzugreifen.

> **Note**
>
> In bestimmten Regionen sendet IAM Identity Center E-Mails an Benutzer, die Amazon Simple Email Service von einer anderen AWS-Region Region aus verwenden. Informationen darüber, wie E-Mails gesendet werden, finden Sie unterRegionsübergreifende Anrufe.
> Alle vom IAM Identity Center-Dienst gesendeten E-Mails stammen entweder von der Adresse `no-reply@signin.aws.com` oderno-reply@login.awsapps.com. Wir empfehlen Ihnen, Ihr E-Mail-System so zu konfigurieren, dass es E-Mails von diesen Absender-E-Mail-Adressen akzeptiert und sie nicht als Junk oder Spam behandelt.

ii. Generieren Sie ein Einmalpasswort, das Sie mit diesem Benutzer teilen können. — Mit dieser Option erhalten Sie die URL und das Passwort des AWS Zugriffsportals, die Sie manuell von Ihrer E-Mail-Adresse aus an den Benutzer senden können.

c. E-Mail-Adresse — Die E-Mail-Adresse muss eindeutig sein.

d. Bestätigen Sie die E-Mail-Adresse

e. Vorname — Sie müssen hier einen Namen eingeben, damit die automatische Bereitstellung funktioniert. Weitere Informationen finden Sie unter Automatische Bereitstellung.

f. Nachname — Sie müssen hier einen Namen eingeben, damit die automatische Bereitstellung funktioniert.

g. Anzeigename

> **Note**
>
> (Optional) Falls zutreffend, können Sie Werte für zusätzliche Attribute wie die unveränderliche Microsoft 365-ID des Benutzers angeben, um dem Benutzer Single Sign-On-Zugriff auf bestimmte Geschäftsanwendungen zu ermöglichen.

4. Wählen Sie Weiter aus.
5. Wählen Sie gegebenenfalls eine oder mehrere Gruppen aus, zu denen Sie den Benutzer hinzufügen möchten, und klicken Sie auf Weiter.
6. Überprüfen Sie die Informationen, die Sie für Schritt 1: Benutzerdetails angeben und Schritt 2: Benutzer zu Gruppen hinzufügen — optional angegeben haben. Wählen Sie in einem der beiden Schritte die Option Bearbeiten aus, um Änderungen vorzunehmen. Nachdem Sie bestätigt

haben, dass die richtigen Informationen für beide Schritte angegeben wurden, wählen Sie Benutzer hinzufügen.

Fügen Sie Gruppen hinzu

Gehen Sie wie folgt vor, um mithilfe der IAM Identity Center-Konsole Gruppen zu Ihrem Identity Center-Verzeichnis hinzuzufügen. Alternativ können Sie den AWS API-Vorgang aufrufen CreateGroup, um Gruppen hinzuzufügen.

So fügen Sie eine Gruppe hinzu

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Klicken Sie auf Groups (Gruppen).
3. Wählen Sie Create group (Gruppe erstellen) aus.
4. Geben Sie einen Gruppennamen und eine Beschreibung ein — optional. Die Beschreibung sollte Angaben darüber enthalten, welche Berechtigungen der Gruppe zugewiesen wurden oder werden. Suchen Sie unter Benutzer zur Gruppe hinzufügen — optional nach den Benutzern, die Sie als Mitglieder hinzufügen möchten. Aktivieren Sie dann das Kontrollkästchen neben jedem von ihnen.
5. Wählen Sie Create group (Gruppe erstellen) aus.

Nachdem Sie diese Gruppe zu Ihrem Identity Center-Verzeichnis hinzugefügt haben, können Sie dieser Gruppe Single Sign-On-Zugriff zuweisen. Weitere Informationen finden Sie unter Weisen Sie Benutzerzugriff zu AWS-Konten.

Fügen Sie Benutzer zu Gruppen hinzu

Gehen Sie wie folgt vor, um Benutzer als Mitglieder einer Gruppe hinzuzufügen, die Sie zuvor mit der IAM Identity Center-Konsole in Ihrem Identity Center-Verzeichnis erstellt haben. Alternativ können Sie den AWS API-Vorgang aufrufen CreateGroupMembership, um einen Benutzer als Mitglied einer Gruppe hinzuzufügen.

So fügen Sie einen Benutzer einer Gruppe als Mitglied hinzu

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Klicken Sie auf Groups (Gruppen).
3. Wählen Sie den Gruppennamen, den Sie aktualisieren möchten.

4. Wählen Sie auf der Seite mit den Gruppendetails unter Benutzer in dieser Gruppe die Option Benutzer zur Gruppe hinzufügen aus.
5. Suchen Sie auf der Seite Benutzer zur Gruppe hinzufügen unter Andere Benutzer nach den Benutzern, die Sie als Mitglieder hinzufügen möchten. Aktivieren Sie dann das Kontrollkästchen neben jedem von ihnen.
6. Wählen Sie Add Users (Benutzer hinzufügen).

Löschen Sie Gruppen im IAM Identity Center

Wenn Sie eine Gruppe in Ihrem IAM Identity Center-Verzeichnis löschen, werden dadurch der Zugriff auf AWS-Konten und die Anwendungen für alle Benutzer, die Mitglieder dieser Gruppe sind, entfernt. Nachdem eine Gruppe gelöscht wurde, kann sie nicht mehr rückgängig gemacht werden. Gehen Sie wie folgt vor, um eine Gruppe in Ihrem Identity Center-Verzeichnis mithilfe der IAM Identity Center-Konsole zu löschen.

Um eine Gruppe in IAM Identity Center zu löschen

> **Important**
>
> Die Anweisungen auf dieser Seite gelten für. AWS IAM Identity Center Sie gelten nicht für AWS Identity and Access Management(IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Löschen von Gruppen in IAM finden Sie unter Löschen einer IAM-Benutzergruppe im Benutzerhandbuch.AWS Identity and Access Management

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Klicken Sie auf Groups (Gruppen).
3. Es gibt zwei Möglichkeiten, eine Gruppe zu löschen:
   - Auf der Seite Gruppen können Sie mehrere Gruppen zum Löschen auswählen. Wählen Sie den Gruppennamen aus, den Sie löschen möchten, und wählen Sie Gruppe löschen.
   - Wählen Sie den Gruppennamen, den Sie löschen möchten. Wählen Sie auf der Seite mit den Gruppendetails die Option Gruppe löschen aus.
4. Möglicherweise werden Sie aufgefordert, Ihre Absicht zu bestätigen, die Gruppe zu löschen.

- Wenn Sie mehrere Gruppen gleichzeitig löschen, bestätigen Sie Ihre Absicht, indem Sie **`Delete`** im Dialogfeld Gruppe löschen etwas eingeben.
- Wenn Sie eine einzelne Gruppe löschen, die Benutzer enthält, bestätigen Sie Ihre Absicht, indem Sie den Namen der Gruppe, die Sie löschen möchten, in das Dialogfeld Gruppe löschen eingeben.

5. Wählen Sie Delete group (Gruppe löschen) aus. Wenn Sie mehrere Gruppen zum Löschen ausgewählt haben, wählen Sie „# Gruppen löschen“.

Löschen Sie Benutzer im IAM Identity Center

Wenn Sie einen Benutzer in Ihrem IAM Identity Center-Verzeichnis löschen, wird ihm dadurch der Zugriff auf AWS-Konten und die Anwendungen entzogen. Nachdem ein Benutzer gelöscht wurde, kann er nicht mehr rückgängig gemacht werden. Gehen Sie wie folgt vor, um einen Benutzer in Ihrem Identity Center-Verzeichnis mithilfe der IAM Identity Center-Konsole zu löschen.

> **Note**
>
> Wenn Sie den Benutzerzugriff deaktivieren oder einen Benutzer in IAM Identity Center löschen, wird dieser Benutzer sofort daran gehindert, sich beim AWS Zugriffsportal anzumelden, und er kann keine neuen Anmeldesitzungen erstellen. Weitere Informationen finden Sie unter Authentifizationssitzungen.

Um einen Benutzer in IAM Identity Center zu löschen

> **Important**
>
> Die Anweisungen auf dieser Seite gelten für. AWS IAM Identity Center Sie gelten nicht für AWS Identity and Access Management(IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Löschen von Benutzern in IAM finden Sie unter Löschen eines IAM-Benutzers im Benutzerhandbuch.AWS Identity and Access Management

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.

3. Es gibt zwei Möglichkeiten, einen Benutzer zu löschen:

   - Auf der Seite Benutzer können Sie mehrere Benutzer zum Löschen auswählen. Wählen Sie den Benutzernamen aus, den Sie löschen möchten, und wählen Sie Benutzer löschen.
   - Wählen Sie den Benutzernamen, den Sie löschen möchten. Wählen Sie auf der Seite mit den Benutzerdetails die Option Benutzer löschen aus.

4. Wenn Sie mehrere Benutzer gleichzeitig löschen, bestätigen Sie Ihre Absicht, indem Sie etwas **`Delete`** in das Dialogfeld „Benutzer löschen“ eingeben.
5. Wählen Sie Benutzer löschen. Wenn Sie mehrere Benutzer zum Löschen ausgewählt haben, wählen Sie Anzahl Benutzer löschen.

Deaktivieren Sie den Benutzerzugriff im IAM Identity Center

Wenn Sie den Benutzerzugriff in Ihrem IAM Identity Center-Verzeichnis deaktivieren, können Sie deren Benutzerdetails nicht bearbeiten, ihr Passwort nicht zurücksetzen, den Benutzer zu einer Gruppe hinzufügen oder seine Gruppenmitgliedschaft anzeigen. Gehen Sie wie folgt vor, um den Benutzerzugriff in Ihrem Identity Center-Verzeichnis mithilfe der IAM Identity Center-Konsole zu deaktivieren.

> **Note**
>
> Wenn Sie den Benutzerzugriff deaktivieren oder einen Benutzer in IAM Identity Center löschen, wird dieser Benutzer sofort daran gehindert, sich beim AWS Zugriffsportal anzumelden, und er kann keine neuen Anmeldesitzungen erstellen. Weitere Informationen finden Sie unter Authentifizationssitzungen.

Um den Benutzerzugriff im IAM Identity Center zu deaktivieren

1. Öffnen Sie die IAM Identity Center-Konsole.

> **Important**
>
> Die Anweisungen auf dieser Seite gelten für. AWS IAM Identity Center Sie gelten nicht für AWS Identity and Access Management(IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zur Deaktivierung von Benutzern in IAM finden Sie

im Benutzerhandbuch unter Verwaltung von IAM-Benutzern.AWS Identity and Access Management

2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie den Benutzernamen des Benutzers aus, dessen Zugriff Sie deaktivieren möchten.
4. Wählen Sie unter dem Benutzernamen des Benutzers, dessen Zugriff Sie deaktivieren möchten, im Abschnitt Allgemeine Informationen die Option Benutzerzugriff deaktivieren aus.
5. Wählen Sie im Dialogfeld Benutzerzugriff deaktivieren die Option Benutzerzugriff deaktivieren aus.

Benutzereigenschaften bearbeiten

Gehen Sie wie folgt vor, um die Eigenschaften eines Benutzers in Ihrem Identity Center-Verzeichnis mithilfe der IAM Identity Center-Konsole zu bearbeiten. Alternativ können Sie den AWS API-Vorgang aufrufen, um die Benutzereigenschaften UpdateUserzu aktualisieren.

Um Benutzereigenschaften im IAM Identity Center zu bearbeiten

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.
3. Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.
4. Wählen Sie auf der Benutzerprofilseite neben Profildetails die Option Bearbeiten aus.
5. Aktualisieren Sie auf der Seite Profildetails bearbeiten die Eigenschaften nach Bedarf. Dann wählen Sie Save changes (Änderungen speichern) aus.

> **Note**
>
> (Optional) Sie können zusätzliche Attribute wie die Mitarbeiternummer und die unveränderliche Office 365-ID ändern, um die Identität des Benutzers in IAM Identity Center bestimmten Geschäftsanwendungen zuzuordnen, die Benutzer verwenden müssen.

> **Note**
>
> Das E-Mail-Adressattribut ist ein bearbeitbares Feld, und der von Ihnen angegebene Wert muss eindeutig sein.

Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück

Dieses Verfahren richtet sich an Administratoren, die das Passwort für einen Benutzer in Ihrem IAM Identity Center-Verzeichnis zurücksetzen müssen. Sie verwenden die IAM Identity Center-Konsole, um Passwörter zurückzusetzen.

Überlegungen zu Identitätsanbietern und Benutzertypen

- MicrosoftActive Directory oder externer Anbieter — Wenn Sie IAM Identity Center mit Microsoft Active Directory oder einem externen Anbieter verbinden, müssen Benutzerkennwörter von Active Directory oder dem externen Anbieter aus zurückgesetzt werden. Das bedeutet, dass Passwörter für diese Benutzer nicht über die IAM Identity Center-Konsole zurückgesetzt werden können.
- Benutzer im IAM Identity Center-Verzeichnis — Wenn Sie ein IAM Identity Center-Benutzer sind, können Sie Ihr eigenes IAM Identity Center-Passwort zurücksetzen, siehe. Ihr IAM Identity Center-Benutzerkennwort zurücksetzen

So setzen Sie ein Passwort für einen IAM Identity Center-Endbenutzer zurück

> **Important**
>
> Die Anweisungen auf dieser Seite gelten für. AWS IAM Identity Center Sie gelten nicht für AWS Identity and Access Management(IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zum Ändern von Passwörtern für IAM-Benutzer finden Sie im Benutzerhandbuch unter Passwörter für IAM-Benutzer verwalten.AWS Identity and Access Management

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Users (Benutzer) aus.

3. Wählen Sie den Benutzernamen des Benutzers aus, dessen Passwort Sie zurücksetzen möchten.
4. Wählen Sie auf der Seite mit den Benutzerdetails die Option Passwort zurücksetzen aus.
5. Wählen Sie im Dialogfeld „Passwort zurücksetzen“ eine der folgenden Optionen und dann „Passwort zurücksetzen“ aus:

   a. Dem Benutzer eine E-Mail mit Anweisungen zum Zurücksetzen des Passworts senden — Diese Option sendet dem Benutzer automatisch eine von Amazon Web Services adressierte E-Mail, in der er erklärt, wie er sein Passwort zurücksetzen kann.

   > **Warning**
   >
   > Aus Sicherheitsgründen sollten Sie überprüfen, ob die E-Mail-Adresse für diesen Benutzer korrekt ist, bevor Sie diese Option auswählen. Wenn diese E-Mail zum Zurücksetzen des Kennworts an eine falsche oder falsch konfigurierte E-Mail-Adresse gesendet würde, könnte sich ein böswilliger Empfänger damit unbefugten Zugriff auf Ihre AWS Umgebung verschaffen.

   b. Generieren Sie ein Einmalpasswort und teilen Sie das Passwort mit dem Benutzer — Mit dieser Option erhalten Sie die Kennwortdetails, die Sie dem Benutzer manuell von Ihrer E-Mail-Adresse aus senden können.

Senden Sie ein E-Mail-OTP für Benutzer, die über die API erstellt wurden

Wenn Sie Benutzer mit der CreateUserAPI-Operation erstellen, haben diese keine Passwörter. Sie können dies ändern, indem Sie festlegen, dass Benutzern ein Einmalpasswort (OTP) per E-Mail gesendet wird, wenn sie mit der API erstellt werden. Benutzer erhalten das E-Mail-OTP, wenn sie zum ersten Mal versuchen, sich anzumelden. Wenn sich ein Benutzer nach Erhalt des E-Mail-OTP anmeldet, muss er ein neues Passwort festlegen. Wenn Sie diese Einstellung nicht aktivieren, müssen Sie OTP generieren und mit den Benutzern teilen, die Sie mithilfe der CreateUserAPI erstellen.

Um E-Mail-OTP an Benutzer zu senden, die mit der API erstellt wurden CreateUser

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.

4. Wählen Sie im Abschnitt Standardauthentifizierung die Option Konfigurieren aus.
5. Ein Dialogfeld wird angezeigt. Markieren Sie das Kästchen neben E-Mail-OTP senden. Wählen Sie dann Save (Speichern) aus. Der Status wird von Deaktiviert auf Aktiviert aktualisiert.

Passwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center

> **Note**
>
> Diese Anforderungen gelten nur für Benutzer, die im Identity Center-Verzeichnis erstellt wurden. Wenn Sie eine andere Identitätsquelle als IAM Identity Center für die Authentifizierung konfiguriert haben, z. B. Active Directoryoder einen externen Identitätsanbieter, werden die Passwortrichtlinien für Ihre Benutzer in diesen Systemen definiert und durchgesetzt, nicht in IAM Identity Center. Wenn Ihre Identitätsquelle dies ist AWS Managed Microsoft AD, finden Sie weitere Informationen unter Passwortrichtlinien verwalten. AWS Managed Microsoft AD

Wenn Sie IAM Identity Center als Identitätsquelle verwenden, müssen Benutzer die folgenden Kennwortanforderungen einhalten, um ihr Passwort festzulegen oder zu ändern:

- Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden.
- Passwörter müssen zwischen 8 und 64 Zeichen lang sein.
- Passwörter müssen mindestens ein Zeichen aus jeder der folgenden vier Kategorien enthalten:
  - Kleinbuchstaben (a – z)
  - Großbuchstaben (A – Z)
  - Zahlen (0 – 9)
  - Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- Die letzten drei Passwörter können nicht wiederverwendet werden.
- Passwörter, die aufgrund eines von Dritten durchgesickerten Datensatzes öffentlich bekannt sind, können nicht verwendet werden.

Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis

Mit können AWS IAM Identity CenterSie ein selbstverwaltetes Verzeichnis in Active Directory (AD) oder ein Verzeichnis in mithilfe AWS Managed Microsoft AD von verbinden AWS Directory

Service. Dieses Microsoft-AD-Verzeichnis definiert den Identitätspool, aus dem Administratoren abrufen können, wenn sie die IAM-Identity-Center-Konsole verwenden, um Single-Sign-On-Zugriff zuzuweisen. Nachdem Sie Ihr Unternehmensverzeichnis mit IAM Identity Center verbunden haben, können Sie Ihren AD-Benutzern oder -Gruppen Zugriff auf AWS-Konten, Anwendungen oder beides gewähren.

AWS Directory Service hilft Ihnen, ein eigenständiges AWS Managed Microsoft AD Verzeichnis einzurichten und auszuführen, das in der - AWS Cloud gehostet wird. Sie können auch verwenden AWS Directory Service , um Ihre - AWS Ressourcen mit einem vorhandenen selbstverwalteten AD zu verbinden. Um AWS Directory Service für die Arbeit mit Ihrem selbstverwalteten AD zu konfigurieren, müssen Sie zunächst Vertrauensstellungen einrichten, um die Authentifizierung auf die Cloud auszuweiten.

IAM Identity Center verwendet die von bereitgestellte Verbindung AWS Directory Service , um die Pass-Through-Authentifizierung für die AD-Quell-Instance durchzuführen. Wenn Sie AWS Managed Microsoft AD als Identitätsquelle verwenden, kann IAM Identity Center mit Benutzern aus AWS Managed Microsoft AD oder von jeder Domain zusammenarbeiten, die über eine AD-Vertrauensstellung verbunden ist. Wenn Sie Ihre Benutzer in vier oder mehr Domänen finden möchten, müssen Benutzer die `DOMAIN\user` Syntax als Benutzernamen verwenden, wenn sie sich bei IAM Identity Center anmelden.

Hinweise

- Stellen Sie als Voraussetzung sicher, dass sich Ihr AD Connector oder Verzeichnis AWS Managed Microsoft AD in in Ihrem AWS Organizations Verwaltungskonto AWS Directory Service befindet. Weitere Informationen finden Sie unter Bestätigen Sie Ihre Identitätsquellen im IAM Identity Center.
- IAM Identity Center unterstützt kein SAMBA-4-basiertes Simple AD als verbundenes Verzeichnis.

Überlegungen zur Verwendung von Active Directory

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

- Wenn Sie verwenden AWS Managed Microsoft AD, müssen Sie IAM Identity Center in derselben aktivieren AWS-Region , in der 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 im Verwaltungskonto:

  Sie müssen einen vorhandenen AD Connector oder ein AWS Managed Microsoft AD Verzeichnis in eingerichtet haben AWS Directory Serviceund dieser muss sich in Ihrem AWS Organizations Verwaltungskonto befinden. Sie können jeweils nur ein AD-Connector-Verzeichnis oder ein Verzeichnis in verbinden AWS Managed Microsoft AD . Wenn Sie mehrere Domains oder Gesamtstrukturen unterstützen müssen, verwenden Sie AWS Managed Microsoft AD. Weitere Informationen finden Sie hier:

  - Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center
  - Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center
- Verwenden Sie ein Active Directory, das sich im delegierten Administratorkonto befindet:

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

  Wenn Sie sich entscheiden, die Identitätsquelle von einer anderen Quelle in Active Directory oder von Active Directory in eine andere Quelle zu ändern, muss sich das Verzeichnis im delegierten Administratorkonto von IAM Identity Center befinden (im Besitz von sein), falls vorhanden. Andernfalls muss es sich im Verwaltungskonto befinden.

Verbinden von Active Directory und Angeben eines Benutzers

Wenn Sie bereits Active Directory verwenden, helfen Ihnen die folgenden Themen bei der Vorbereitung der Verbindung Ihres Verzeichnisses mit IAM Identity Center.

Sie können ein - AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory mit IAM Identity Center verbinden. Wenn Sie ein - AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory verbinden möchten, stellen Sie sicher, dass Ihre Active-Directory-Konfiguration die Voraussetzungen unter erfülltBestätigen Sie Ihre Identitätsquellen im IAM Identity Center.

> **Note**
>
> Als bewährte Sicherheitsmethode empfehlen wir dringend, die Multi-Faktor-Authentifizierung zu aktivieren. Wenn Sie ein - AWS Managed Microsoft AD Verzeichnis oder ein selbstverwaltetes Verzeichnis in Active Directory verbinden möchten und RADIUS MFA nicht mit verwenden AWS Directory Service, aktivieren Sie MFA in IAM Identity Center.

AWS Managed Microsoft AD

1. Lesen Sie die Anleitungen unter Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis.
2. Führen Sie die Schritte unter Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center aus.
3. Konfigurieren Sie Active Directory, um den Benutzer zu synchronisieren, dem Sie Administratorberechtigungen für IAM Identity Center erteilen möchten. Weitere Informationen finden Sie unter Synchronisieren eines Administratorbenutzers mit IAM Identity Center.

Selbstverwaltetes Verzeichnis in Active Directory

1. Lesen Sie die Anleitungen unter Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis.
2. Führen Sie die Schritte unter Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center aus.
3. Konfigurieren Sie Active Directory, um den Benutzer zu synchronisieren, dem Sie Administratorberechtigungen für IAM Identity Center erteilen möchten. Weitere Informationen finden Sie unter Synchronisieren eines Administratorbenutzers mit IAM Identity Center.

Externer IdP

1. Lesen Sie die Anleitungen unter Stellen Sie eine Connect zu einem externen Identitätsanbieter her.
2. Führen Sie die Schritte unter Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her aus.
3. Konfigurieren Sie Ihren IdP für die Bereitstellung von Benutzern in IAM Identity Center.

> **Note**
>
> Bevor Sie die automatische, gruppenbasierte Bereitstellung aller Ihrer Mitarbeiteridentitäten von Ihrem IdP in IAM Identity Center einrichten, empfehlen wir Ihnen, den einen Benutzer zu synchronisieren, dem Sie Administratorberechtigungen für IAM Identity Center erteilen möchten.

Synchronisieren eines Administratorbenutzers mit IAM Identity Center

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

1. Öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Sync verwalten aus.
4. Wählen Sie auf der Seite Sync 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 Benutzer und Gruppen hinzugefügt wie folgt vor:
   a. Vergewissern Sie sich, dass der Benutzer angegeben ist, dem Sie Administratorberechtigungen erteilen möchten.
   b. Aktivieren Sie das Kontrollkästchen links neben dem Benutzernamen.
   c. Wählen Sie Absenden aus.
7. Auf der Seite Synchronisierung verwalten wird der von Ihnen angegebene Benutzer in der Liste Benutzer im Synchronisierungsbereich 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 angezeigt wird. Wählen Sie das Aktualisierungssymbol, um die Liste der Benutzer zu aktualisieren.

Zu diesem Zeitpunkt hat Ihr Benutzer keinen Zugriff auf das Verwaltungskonto. Sie richten den administrativen Zugriff auf dieses Konto ein, indem Sie einen administrativen Berechtigungssatz erstellen und den Benutzer diesem Berechtigungssatz zuweisen. Weitere Informationen finden Sie unter Berechtigungssatz erstellen.

Bereitstellung, wenn Benutzer aus Active Directory stammen

IAM Identity Center verwendet die von bereitgestellte Verbindung, AWS Directory Service um Benutzer-, Gruppen- und Mitgliedschaftsinformationen aus Ihrem Quellverzeichnis in Active Directory mit dem IAM-Identity-Center-Identitätsspeicher zu synchronisieren. Es werden keine Passwortinformationen mit IAM Identity Center synchronisiert, da die Benutzerauthentifizierung direkt aus dem Quellverzeichnis in Active Directory erfolgt. Diese Identitätsdaten werden von Anwendungen verwendet, um In-App-Lookup-, Autorisierungs- und Zusammenarbeitsszenarien zu erleichtern, ohne LDAP-Aktivitäten zurück an das Quellverzeichnis in Active Directory zu übergeben.

Weitere Informationen über die Bereitstellung finden Sie unter Bereitstellung von Benutzern und Gruppen.

Themen

- Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center
- Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center
- Attributzuordnungen für AWS Managed Microsoft AD das Verzeichnis
- Bereitstellen von Benutzern und Gruppen aus Active Directory

Verbinden eines Verzeichnisses in AWS Managed Microsoft AD mit IAM Identity Center

Gehen Sie wie folgt vor, um ein Verzeichnis in AWS Managed Microsoft AD , das von verwaltet wird, mit IAM Identity Center AWS Directory Service zu verbinden.

So stellen Sie eine Verbindung AWS Managed Microsoft AD mit IAM Identity Center her

1. Öffnen Sie die IAM-Identity-Center-Konsole .

> **Note**
>
> Stellen Sie sicher, dass die IAM-Identity-Center-Konsole eine der Regionen verwendet, in denen sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle und dann Aktionen > Identitätsquelle ändern aus.
4. Wählen Sie unter Identitätsquelle auswählen die Option Active Directory und dann Weiter aus.
5. Wählen Sie unter Aktives Verzeichnis verbinden ein Verzeichnis in AWS Managed Microsoft AD aus der Liste und dann Weiter aus.
6. Überprüfen Sie unter Änderung bestätigen die Informationen und wenn bereit, Typ ACCEPT und wählen Sie dann Identitätsquelle ändern aus.

> **Important**
>
> Um einen Benutzer in Active Directory als Administratorbenutzer in IAM Identity Center anzugeben, müssen Sie zunächst den Benutzer synchronisieren, dem Sie Administratorberechtigungen von Active Directory in IAM Identity Center erteilen möchten. Eine Schritt-für-Schritt-Anleitung hierzu finden Sie unter Synchronisieren eines Administratorbenutzers mit IAM Identity Center.

Verbinden eines selbstverwalteten Verzeichnisses in Active Directory mit IAM Identity Center

Benutzer in Ihrem selbstverwalteten Verzeichnis in Active Directory (AD) können auch Single-Sign-On-Zugriff auf AWS-Konten und Anwendungen im - AWS Zugriffsportal haben. Um den Single-Sign-On-Zugriff für diese Benutzer zu konfigurieren, können Sie einen der folgenden Schritte ausführen:

- Erstellen einer bidirektionalen Vertrauensstellung – Wenn bidirektionale Vertrauensstellungen zwischen AWS Managed Microsoft AD und einem selbstverwalteten Verzeichnis in AD erstellt werden, können sich Benutzer in Ihrem selbstverwalteten Verzeichnis in AD mit ihren Unternehmensanmeldeinformationen bei verschiedenen - AWS Services und

Geschäftsanwendungen anmelden. Einseitige Vertrauensstellungen funktionieren nicht mit IAM Identity Center.

AWS IAM Identity Center erfordert eine bidirektionale Vertrauensstellung, damit Benutzer- und Gruppeninformationen aus Ihrer Domain gelesen werden können, um Benutzer- und Gruppenmetadaten zu synchronisieren. IAM Identity Center verwendet diese Metadaten, wenn Zugriff auf Berechtigungssätze oder Anwendungen zugewiesen wird. Benutzer- und Gruppenmetadaten werden auch von Anwendungen für die Zusammenarbeit verwendet, z. B. wenn Sie ein Dashboard für einen anderen Benutzer oder eine andere Gruppe freigeben. Die Vertrauensstellung von AWS Directory Service für Microsoft Active Directory zu Ihrer Domain ermöglicht es IAM Identity Center, Ihrer Domain zur Authentifizierung zu vertrauen. Die Vertrauensstellung in die entgegengesetzte Richtung gewährt AWS Berechtigungen zum Lesen von Benutzer- und Gruppenmetadaten.

Weitere Informationen zum Einrichten einer bidirektionalen Vertrauensstellung finden Sie unter Zeitpunkt zum Erstellen einer Vertrauensstellung im AWS Directory Service - Administratorhandbuch.

- Erstellen eines AD Connectors – AD Connector ist ein Verzeichnis-Gateway, das Verzeichnisanforderungen an Ihr selbstverwaltetes AD umleiten kann, ohne Informationen in der Cloud zwischenspeichern zu müssen. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem Verzeichnis im AWS Directory Service -Administratorhandbuch.

> **Note**
>
> Wenn Sie IAM Identity Center mit einem AD-Connector-Verzeichnis verbinden, müssen alle zukünftigen Benutzerpasswörter in AD zurückgesetzt werden. Das bedeutet, dass Benutzer ihre Passwörter nicht über das - AWS Zugriffsportal zurücksetzen können.
> Wenn Sie AD Connector verwenden, um Ihren Active Directory Domain Service mit IAM Identity Center zu verbinden, hat IAM Identity Center nur Zugriff auf die Benutzer und Gruppen der einzelnen Domain, an die AD Connector anhängt. Wenn Sie mehrere Domains oder Gesamtstrukturen unterstützen müssen, verwenden AWS Directory Service Sie für Microsoft Active Directory.

> **Note**
>
> IAM Identity Center funktioniert nicht mit SAMBA4-based Simple-AD-Verzeichnissen.

Attributzuordnungen für AWS Managed Microsoft AD das Verzeichnis

Attributzuordnungen werden verwendet, um Attributtypen, die in IAM Identity Center vorhanden sind, mit ähnlichen Attributen in einem - AWS Managed Microsoft AD Verzeichnis zuzuordnen. IAM Identity Center ruft Benutzerattribute aus Ihrem Microsoft-AD-Verzeichnis ab und ordnet sie IAM-Identity-Center-Benutzerattributen zu. Diese IAM-Identity-Center-Benutzerattributzuordnungen werden auch zum Generieren von SAML-2.0-Assertionen für Ihre Anwendungen verwendet. Jede Anwendung bestimmt die Liste der SAML-2.0-Attribute, die sie für ein erfolgreiches Single Sign-On benötigt.

IAM Identity Center füllt eine Reihe von Attributen für Sie auf der Registerkarte Attributzuordnungen auf der Konfigurationsseite Ihrer Anwendung aus. IAM Identity Center verwendet diese Benutzerattribute, um SAML-Assertions (als SAML-Attribute) auszufüllen, die an die Anwendung gesendet werden. Diese Benutzerattribute werden wiederum von Ihrem Mircosoft AD-Verzeichnis abgerufen. Weitere Informationen finden Sie unter Ordnen Sie Attribute in Ihrer Anwendung den IAM Identity Center-Attributen zu.

IAM Identity Center verwaltet auch eine Reihe von Attributen für Sie im Abschnitt Attributzuordnungen Ihrer Verzeichniskonfigurationsseite. Weitere Informationen finden Sie unter Zuordnen von Attributen in IAM Identity Center zu Attributen in Ihrem AWS Managed Microsoft AD Verzeichnis.

Unterstützte Verzeichnisattribute

In der folgenden Tabelle sind alle unterstützten AWS Managed Microsoft AD Verzeichnisattribute aufgeführt, die Benutzerattributen in IAM Identity Center zugeordnet werden können.

Unterstützte Attribute in Ihrem Microsoft AD-Verzeichnis
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`

Unterstützte Attribute in Ihrem Microsoft AD-Verzeichnis
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Sie können eine beliebige Kombination unterstützter Microsoft AD-Verzeichnisattribute angeben, die einem einzelnen veränderbaren Attribut in IAM Identity Center zugeordnet werden sollen. Sie können beispielsweise das `subject` Attribut unter dem Benutzerattribut in der Spalte IAM Identity Center auswählen. Ordnen Sie sie dann entweder `${dir:displayname}` `${dir:lastname}${dir:firstname }` oder einem beliebigen unterstützten Attribut oder einer beliebigen Kombination unterstützter Attribute zu. Eine Liste der Standardzuordnungen für Benutzerattribute in IAM Identity Center finden Sie unter Standardzuordnungen.

> **Warning**
>
> Bestimmte IAM-Identity-Center-Attribute können nicht geändert werden, da sie unveränderlich sind und standardmäßig bestimmten Microsoft-AD-Verzeichnisattributen zugeordnet sind. Beispielsweise ist „Benutzername“ ein obligatorisches Attribut im IAM Identity Center. Wenn Sie einem AD-Verzeichnisattribut mit einem leeren Wert „Benutzername“ zuordnen, betrachtet IAM Identity Center den `windowsUpn` Wert als Standardwert für „Benutzername“. Wenn Sie die Attributzuordnung für „Benutzername“ aus Ihrer aktuellen Zuordnung ändern möchten, vergewissern Sie sich, dass IAM-Identity-Center-Flows mit Abhängigkeit von „Benutzername“ weiterhin wie erwartet funktionieren, bevor Sie die Änderung vornehmen.

Wenn Sie die - ListUsers oder ListGroups-API-Aktionen oder die - list-users und list-groups AWS - CLI-Befehle verwenden, um Benutzern und Gruppen Zugriff auf AWS-Konten und auf Anwendungen zuzuweisen, müssen Sie den Wert für `AttributeValue` als FQDN angeben. Dieser Wert muss das folgende Format haben: user@example.com. Im folgenden Beispiel `AttributeValue` ist auf festgelegt`janedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Unterstützte IAM-Identity-Center-Attribute

In der folgenden Tabelle sind alle unterstützten IAM-Identity-Center-Attribute aufgeführt, die Benutzerattributen in Ihrem AWS Managed Microsoft AD Verzeichnis zugeordnet werden können. Nachdem Sie Ihre Anwendungsattributzuordnungen eingerichtet haben, können Sie dieselben IAM-Identity-Center-Attribute verwenden, um tatsächlichen Attributen zuzuordnen, die von dieser Anwendung verwendet werden.

Unterstützte Attribute in IAM Identity Center
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Unterstützte externe Identitätsanbieterattribute

In der folgenden Tabelle sind alle unterstützten Attribute des externen Identitätsanbieters (IdP) aufgeführt, die Attributen zugeordnet werden können, die Sie bei der Konfiguration von Attribute für Zugriffskontrolle in IAM Identity Center verwenden können. Wenn Sie SAML-Assertionen verwenden, können Sie die Attribute verwenden, die Ihr IdP unterstützt.

Unterstützte Attribute in Ihrem IdP
`${path:userName}`

Unterstützte Attribute in Ihrem IdP
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}
${path:enterprise.division}

Unterstützte Attribute in Ihrem IdP
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Standardzuordnungen

In der folgenden Tabelle sind die Standardzuordnungen für Benutzerattribute in IAM Identity Center zu den Benutzerattributen in Ihrem AWS Managed Microsoft AD Verzeichnis aufgeführt. IAM Identity Center unterstützt nur die Liste der Attribute im Benutzerattribut in der Spalte IAM Identity Center.

> **Note**
>
> Wenn Sie beim Aktivieren der konfigurierbaren AD-Synchronisierung keine Zuweisungen für Ihre Benutzer und Gruppen in IAM Identity Center haben, werden die Standardzuordnungen in der folgenden Tabelle verwendet. Informationen zum Anpassen dieser Zuordnungen finden Sie unter Konfigurieren von Attributzuordnungen für Ihre Synchronisierung.

Benutzerattribut in IAM Identity Center	Zuordnung zu diesem Attribut im Microsoft AD-Verzeichnis
`AD_GUID`	`${dir:guid}`
`email` *	`${dir:windowsUpn}`
`familyName`	`${dir:lastname}`
`givenName`	`${dir:firstname}`
`middleName`	`${dir:initials}`
`name`	`${dir:displayname}`
`preferredUsername`	`${dir:displayname}`
`subject`	`${dir:windowsUpn}`

* Das E-Mail-Attribut in IAM Identity Center muss innerhalb des Verzeichnisses eindeutig sein. Andernfalls könnte der JIT-Anmeldevorgang fehlschlagen.

Sie können die Standardzuordnungen ändern oder der SAML-2.0-Assertion je nach Ihren Anforderungen weitere Attribute hinzufügen. Angenommen, Ihre Anwendung benötigt die E-Mail des Benutzers im `User.Email` SAML-2.0-Attribut. Nehmen Sie außerdem an, dass E-Mail-Adressen im `windowsUpn` Attribut in Ihrem Microsoft-AD-Verzeichnis gespeichert sind. Um diese Zuordnung zu erreichen, müssen Sie Änderungen an den folgenden beiden Stellen der IAM-Identity-Center-Konsole vornehmen:

1. Ordnen Sie auf der Seite Directory (Verzeichnis) im Bereich Attribute mappings (Attributzuordnungen) das Benutzerattribut **`email`** dem Attribut **`${dir:windowsUpn}`** zu (in der Spalte Maps to this attribute in your directory (Zuordnung zum Attribut im Verzeichnis)).
2. Wählen Sie auf der Seite Anwendungen die Anwendung aus der Tabelle aus. Wählen Sie die Registerkarte Attributzuordnungen aus. Ordnen Sie dann das `User.Email` Attribut dem **`${user:email}`** Attribut zu (in der Spalte Zuordnungen zu diesem Zeichenfolgenwert oder Benutzerattribut in IAM Identity Center).

Beachten Sie, dass Sie jedes Verzeichnisattribut in der Form ${dir:**`AttributeName`**} angeben müssen. Das Attribut `firstname` in Ihrem Microsoft AD-Verzeichnis wird beispielsweise zu `${dir:firstname}`. Es ist wichtig, dass jedem Verzeichnisattribut ein tatsächlicher Wert zugewiesen wird. Attribute, die nach `${dir:` keinen Wert haben, verursachen Probleme bei der Benutzeranmeldung.

Zuordnen von Attributen in IAM Identity Center zu Attributen in Ihrem AWS Managed Microsoft AD Verzeichnis

Sie können das folgende Verfahren verwenden, um anzugeben, wie Ihre Benutzerattribute in IAM Identity Center entsprechenden Attributen in Ihrem Microsoft-AD-Verzeichnis zugeordnet werden sollen.

So ordnen Sie Attribute in IAM Identity Center Attributen in Ihrem Verzeichnis zu

1. Öffnen Sie die IAM-Identity-Center-Konsole .
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Attribute für die Zugriffskontrolle und dann Attribute verwalten aus.

4. Suchen Sie auf der Seite Attribut für die Zugriffskontrolle verwalten das Attribut in IAM Identity Center, das Sie zuordnen möchten, und geben Sie dann einen Wert in das Textfeld ein. Sie können beispielsweise das IAM Identity Center-Benutzerattribut dem Microsoft AD-Verzeichnisattribut **`email`** zuordnen**`${dir:windowsUpn}`**.
5. Wählen Sie Änderungen speichern aus.

Bereitstellen von Benutzern und Gruppen aus Active Directory

IAM Identity Center bietet die folgenden zwei Möglichkeiten, Benutzer und Gruppen aus Active Directory bereitzustellen.

- IAM Identity Center konfigurierbare Active Directory (AD)-Synchronisierung (empfohlen) – Mit dieser Synchronisierungsmethode können Sie Folgendes tun:
  - Steuern Sie Datengrenzen, indem Sie explizit die Benutzer und Gruppen in Microsoft Active Directory definieren, die automatisch mit IAM Identity Center synchronisiert werden. Sie können Benutzer und Gruppen hinzufügen oder Benutzer und Gruppen entfernen, um den Umfang der Synchronisierung jederzeit zu ändern.
  - Weisen Sie synchronisierten Benutzern und Gruppen Single-Sign-On-Zugriff auf AWS-Konten oder Zugriff auf Anwendungen zu. Die Anwendungen können AWS verwaltete Anwendungen oder vom Kunden verwaltete Anwendungen sein.
  - Steuern Sie den Synchronisationsprozess, indem Sie die Synchronisation nach Bedarf pausieren und fortsetzen. Auf diese Weise können Sie die Belastung der Produktionssysteme regulieren.
- IAM-Identity-Center-AD-Synchronisierung – Mit dieser Synchronisierungsmethode verwenden Sie IAM Identity Center, um Benutzer und Gruppen in Active Directory Zugriff auf AWS Konten und Anwendungen zuzuweisen. Alle Identitäten mit Zuweisungen werden automatisch mit IAM Identity Center synchronisiert.

Konfigurierbare AD-Synchronisierung von IAM Identity Center

Mit der konfigurierbaren Active-Directory-(AD)-Synchronisierung von IAM Identity Center können Sie die Identitäten in Microsoft Active Directory, die automatisch in IAM Identity Center synchronisiert werden, explizit konfigurieren und den Synchronisationsprozess steuern.

Die folgenden Themen enthalten Informationen, mit denen Sie die konfigurierbare AD-Synchronisierung konfigurieren und verwalten können.

Themen

- Voraussetzungen und Überlegungen
- So funktioniert konfigurierbare AD Sync
- Konfigurieren und Verwalten Ihres Synchronisierungsbereichs

Voraussetzungen und Überlegungen

Bevor Sie die konfigurierbare AD-Synchronisierung verwenden, sollten Sie die folgenden Voraussetzungen und Überlegungen beachten:

- Angeben von Benutzern und Gruppen in Active Directory zum Synchronisieren

  Bevor Sie IAM Identity Center verwenden können, um neuen Benutzern und Gruppen Zugriff auf AWS-Konten und zu AWS verwalteten Anwendungen oder kundenverwalteten Anwendungen zuzuweisen, müssen Sie die zu synchronisierenden Benutzer und Gruppen in Active Directory angeben und sie dann in IAM Identity Center synchronisieren.

  - AD-Synchronisierung – Wenn Sie Zuweisungen für neue Benutzer und Gruppen mithilfe der IAM-Identity-Center-Konsole oder verwandter Zuweisungs-API-Aktionen vornehmen, durchsucht IAM Identity Center den Domain-Controller direkt nach den angegebenen Benutzern oder Gruppen, schließt die Zuweisung ab und synchronisiert dann regelmäßig die Benutzer- oder Gruppenmetadaten mit IAM Identity Center.
  - Konfigurierbare AD-Synchronisierung – IAM Identity Center durchsucht Ihren Domain-Controller nicht direkt nach Benutzern und Gruppen. Stattdessen müssen Sie zuerst die Liste der Benutzer und Gruppen angeben, die synchronisiert werden sollen. Sie können diese Liste, auch bekannt als Synchronisierungsbereich, auf eine der folgenden Arten konfigurieren, je nachdem, ob Sie Benutzer und Gruppen haben, die bereits mit IAM Identity Center synchronisiert sind, oder ob Sie neue Benutzer und Gruppen haben, die Sie zum ersten Mal synchronisieren, indem Sie die konfigurierbare AD-Synchronisierung verwenden.
    - Bestehende Benutzer und Gruppen: Wenn Sie Benutzer und Gruppen haben, die bereits mit IAM Identity Center synchronisiert sind, ist der Synchronisierungsbereich in der konfigurierbaren AD-Synchronisierung mit einer Liste dieser Benutzer und Gruppen vorausgefüllt. Um neue Benutzer oder Gruppen zuzuweisen, müssen Sie sie speziell zum Synchronisierungsbereich hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Benutzern und Gruppen zu Ihrem Synchronisierungsbereich.
    - Neue Benutzer und Gruppen: Wenn Sie neuen Benutzern und Gruppen Zugriff auf AWS-Konten und auf Anwendungen zuweisen möchten, müssen Sie in der konfigurierbaren AD-Synchronisierung angeben, welche Benutzer und Gruppen dem Synchronisierungsbereich

hinzugefügt werden sollen, bevor Sie IAM Identity Center verwenden können, um die Zuweisung vorzunehmen. Weitere Informationen finden Sie unter Hinzufügen von Benutzern und Gruppen zu Ihrem Synchronisierungsbereich.

- Zuweisungen zu verschachtelten Gruppen in Active Directory vornehmen

  Gruppen, die Mitglieder anderer Gruppen sind, werden als verschachtelte Gruppen (oder untergeordnete Gruppen) bezeichnet. Wenn Sie Zuweisungen an eine Gruppe in Active Directory vornehmen, die verschachtelte Gruppen enthält, hängt die Art und Weise, wie die Zuweisungen angewendet werden, davon ab, ob Sie AD Sync oder konfigurierbare AD Sync verwenden.

  - AD-Synchronisierung – Wenn Sie Zuweisungen an eine Gruppe in Active Directory vornehmen, die verschachtelte Gruppen enthält, können nur die direkten Mitglieder der Gruppe auf das Konto zugreifen. Wenn Sie beispielsweise Zugriff auf Gruppe A zuweisen und Gruppe B Mitglied von Gruppe A ist, können nur die direkten Mitglieder von Gruppe A auf das Konto zugreifen. Keine Mitglieder von Gruppe B erben den Zugriff.
  - Konfigurierbare AD-Synchronisierung – Die Verwendung der konfigurierbaren AD-Synchronisierung für Zuweisungen an eine Gruppe in Active Directory, die verschachtelte Gruppen enthält, kann den Umfang der Benutzer erhöhen, die Zugriff auf AWS-Konten oder auf Anwendungen haben. In diesem Fall gilt die Zuweisung für alle Benutzer, einschließlich derjenigen in verschachtelten Gruppen. Wenn Sie beispielsweise Zugriff auf Gruppe A zuweisen und Gruppe B Mitglied von Gruppe A ist, erben Mitglieder von Gruppe B diesen Zugriff ebenfalls.
- Aktualisieren automatisierter Workflows

  Wenn Sie automatisierte Workflows haben, die die API-Aktionen des IAM Identity Center-Identitätsspeichers und die API-Aktionen für die IAM-Identity-Center-Zuweisung verwenden, um neuen Benutzern und Gruppen Zugriff auf Konten und Anwendungen zuzuweisen und sie mit IAM Identity Center zu synchronisieren, müssen Sie diese Workflows bis zum 15. April 2022 so anpassen, dass sie mit der konfigurierbaren AD-Synchronisierung wie erwartet funktionieren. Konfigurierbare AD-Synchronisierung ändert die Reihenfolge, in der Benutzer- und Gruppenzuweisung und -bereitstellung stattfinden, und die Art und Weise, in der Abfragen ausgeführt werden.

  - AD Sync – Der Prozess der Zuweisungen erfolgt zuerst. Sie weisen Benutzern und Gruppen Zugriff auf AWS-Konten und auf Anwendungen zu. Nachdem den Benutzern und Gruppen Zugriff zugewiesen wurde, werden sie automatisch bereitgestellt (in IAM Identity Center synchronisiert). Wenn Sie über einen automatisierten Workflow verfügen, bedeutet dies, dass Ihr automatisierter

Workflow beim Hinzufügen eines neuen Benutzers zu Active Directory Active Directory mithilfe der `ListUser` API-Aktion des Identitätsspeichers nach dem Benutzer abfragen und diesem dann mithilfe der API-Aktionen der IAM-Identity-Center-Zuweisung den Benutzerzugriff zuweisen kann. Da der Benutzer über eine Zuweisung verfügt, wird dieser Benutzer automatisch im IAM Identity Center bereitgestellt.

- Konfigurierbare AD-Synchronisierung – Die Bereitstellung erfolgt zuerst und wird nicht automatisch durchgeführt. Stattdessen müssen Sie Benutzer und Gruppen zunächst explizit zum Identitätsspeicher hinzufügen, indem Sie sie Ihrem Synchronisierungsbereich hinzufügen. Informationen zu den empfohlenen Schritten zur Automatisierung Ihrer Synchronisierungskonfiguration für die konfigurierbare AD-Synchronisierung finden Sie unter Automatisieren Ihrer Synchronisierungskonfiguration für konfigurierbare AD-Synchronisierung.

So funktioniert konfigurierbare AD Sync

IAM Identity Center aktualisiert die AD-basierten Identitätsdaten im Identitätsspeicher mithilfe des folgenden Verfahrens.

Erstellung

Nachdem Sie Ihr selbstverwaltetes Verzeichnis in Active Directory oder Ihr von verwaltetes AWS Managed Microsoft AD Verzeichnis AWS Directory Service mit IAM Identity Center verbunden haben, können Sie die Active-Directory-Benutzer und -Gruppen, die Sie mit dem IAM-Identity-Center-Identitätsspeicher synchronisieren möchten, explizit konfigurieren. Die von Ihnen ausgewählten Identitäten werden etwa alle drei Stunden mit dem IAM-Identity-Center-Identitätsspeicher synchronisiert. Abhängig von der Größe Ihres Verzeichnisses kann der Synchronisierungsprozess länger dauern.

Gruppen, die Mitglieder anderer Gruppen sind (sogenannte verschachtelte Gruppen oder untergeordnete Gruppen), werden ebenfalls in den Identitätsspeicher geschrieben. Wenn Sie Zuweisungen an eine Gruppe in Active Directory vornehmen, die verschachtelte Gruppen enthält, hängt die Art und Weise, wie die Zuweisungen angewendet werden, davon ab, ob Sie AD Sync oder konfigurierbare AD Sync verwenden. Weitere Informationen finden Sie unter Making assignments to nested groups in Active Directory.

Sie können neuen Benutzern oder Gruppen erst Zugriff zuweisen, nachdem sie im IAM-Identity-Center-Identitätsspeicher synchronisiert wurden.

Aktualisierung

Die Identitätsdaten im IAM-Identity-Center-Identitätsspeicher bleiben aktuell, indem sie regelmäßig Daten aus dem Quellverzeichnis in Active Directory lesen. IAM Identity Center synchronisiert Daten aus Ihrem Active Directory standardmäßig stündlich in einem Synchronisierungszyklus. Je nach Größe Ihres Active Directory kann es 30 Minuten bis 2 Stunden dauern, bis die Daten in IAM Identity Center synchronisiert sind.

Benutzer- und Gruppenobjekte, die sich im Synchronisierungsbereich befinden, und ihre Mitgliedschaften werden in IAM Identity Center erstellt oder aktualisiert, um sie den entsprechenden Objekten im Quellverzeichnis in Active Directory zuzuordnen. Bei Benutzerattributen wird nur die Teilmenge der Attribute aktualisiert, die im Abschnitt Attribute für die Zugriffskontrolle der IAM-Identity-Center-Konsole aufgeführt sind. Es kann einen Synchronisierungszyklus dauern, bis alle Attributaktualisierungen, die Sie in Active Directory vornehmen, in IAM Identity Center wiedergegeben werden.

Sie können auch die Teilmenge der Benutzer und Gruppen aktualisieren, die Sie mit dem IAM-Identity-Center-Identitätsspeicher synchronisieren. Sie können dieser Teilmenge neue Benutzer oder Gruppen hinzufügen oder sie entfernen. Alle Identitäten, die Sie hinzufügen, werden mit der nächsten geplanten Synchronisierung synchronisiert. Identitäten, die Sie aus der Teilmenge entfernen, werden im IAM-Identity-Center-Identitätsspeicher nicht mehr aktualisiert. Jeder Benutzer, der länger als 28 Tage nicht synchronisiert wurde, wird im IAM-Identity-Center-Identitätsspeicher deaktiviert. Die entsprechenden Benutzerobjekte werden während des nächsten Synchronisierungszyklus automatisch im IAM-Identity-Center-Identitätsspeicher deaktiviert, es sei denn, sie sind Teil einer anderen Gruppe, die noch Teil des Synchronisierungsbereichs ist.

Löschung

Benutzer und Gruppen werden aus dem IAM-Identity-Center-Identitätsspeicher gelöscht, wenn die entsprechenden Benutzer- oder Gruppenobjekte aus dem Quellverzeichnis in Active Directory gelöscht werden. Alternativ können Sie Benutzerobjekte mithilfe der IAM-Identity-Center-Konsole explizit aus dem IAM-Identity-Center-Identitätsspeicher löschen. Wenn Sie die IAM-Identity-Center-Konsole verwenden, müssen Sie die Benutzer auch aus dem Synchronisierungsbereich entfernen, um sicherzustellen, dass sie während des nächsten Synchronisierungszyklus nicht wieder in IAM Identity Center synchronisiert werden.

Sie können die Synchronisation auch jederzeit anhalten und neu starten. Wenn Sie die Synchronisation länger als 28 Tage anhalten, werden alle Ihre Benutzer deaktiviert.

Konfigurieren und Verwalten Ihres Synchronisierungsbereichs

Sie können Ihren Synchronisierungsbereich auf eine der folgenden Arten konfigurieren:

- Geführte Einrichtung: Wenn Sie Ihre Benutzer und Gruppen zum ersten Mal von Active Directory in IAM Identity Center synchronisieren, befolgen Sie die Schritte unter , Geführte Einrichtung um Ihren Synchronisierungsbereich zu konfigurieren. Nachdem Sie die geführte Einrichtung abgeschlossen haben, können Sie Ihren Synchronisierungsbereich jederzeit ändern, indem Sie die anderen Verfahren in diesem Abschnitt befolgen.
- Wenn Sie bereits Benutzer und Gruppen haben, die mit IAM Identity Center synchronisiert sind, oder Sie die geführte Einrichtung nicht befolgen möchten, wählen Sie Synchronisierung verwalten aus. Überspringen Sie das Verfahren zur geführten Einrichtung und folgen Sie den anderen Verfahren in diesem Abschnitt, wenn erforderlich, um Ihren Synchronisierungsbereich zu konfigurieren und zu verwalten.

Verfahren

- Geführte Einrichtung
- Hinzufügen von Benutzern und Gruppen zu Ihrem Synchronisierungsbereich
- Entfernen von Benutzern und Gruppen aus Ihrem Synchronisierungsbereich
- Pausieren und Fortsetzen Ihrer Synchronisierung
- Konfigurieren von Attributzuordnungen für Ihre Synchronisierung
- Automatisieren Ihrer Synchronisierungskonfiguration für konfigurierbare AD-Synchronisierung

Geführte Einrichtung

1. Öffnen Sie die IAM-Identity-Center-Konsole .

   > **Note**
   >
   > Stellen Sie sicher, dass die IAM-Identity-Center-Konsole eine der verwendet AWS-Regionen , in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie oben auf der Seite in der Benachrichtigungsmeldung die Option geführtes Setup starten aus.

4. Überprüfen Sie in Schritt 1 – optional : Konfigurieren von Attributzuordnungen die standardmäßigen Benutzer- und Gruppenattributzuordnungen. Wenn keine Änderungen erforderlich sind, wählen Sie Weiter aus. Wenn Änderungen erforderlich sind, nehmen Sie die Änderungen vor und wählen Sie dann Änderungen speichern aus.
5. Wählen Sie in Schritt 2 – optional: Konfigurieren des Synchronisierungsbereichs die Registerkarte Benutzer aus. Geben Sie dann den genauen Benutzernamen des Benutzers ein, den Sie Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen aus. Wählen Sie als Nächstes die Registerkarte Gruppen aus. Geben Sie den genauen Gruppennamen der Gruppe ein, die Sie Ihrem Synchronisierungsbereich hinzufügen möchten, und wählen Sie Hinzufügen aus. Wählen Sie anschließend Weiter. Wenn Sie später Benutzer und Gruppen zu Ihrem Synchronisierungsbereich hinzufügen möchten, nehmen Sie keine Änderungen vor und wählen Sie Weiter aus.
6. Bestätigen Sie in Schritt 3: Überprüfen und Speichern der Konfiguration Ihre Attributzuordnungen in Schritt 1: Attributzuordnungen und Ihre Benutzer und Gruppen in Schritt 2: Synchronisierungsbereich . Wählen Sie Save configuration (Konfiguration speichern) aus. Dadurch gelangen Sie zur Seite Sync verwalten.

Hinzufügen von Benutzern und Gruppen zu Ihrem Synchronisierungsbereich

So fügen Sie Benutzer hinzu

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie auf der Seite Sync 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. Überprüfen Sie unter Benutzer und Gruppen hinzugefügt den Benutzer, den Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.
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 angezeigt wird. Wählen Sie das Aktualisierungssymbol, um die Liste der Benutzer zu aktualisieren.

So fügen Sie Gruppen hinzu

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie auf der Seite Sync verwalten die Registerkarte Gruppen und dann Benutzer und Gruppen hinzufügen aus.
5. Wählen Sie die Registerkarte Groups (Gruppen). Geben Sie unter Gruppe den genauen Gruppennamen ein und wählen Sie Hinzufügen aus.
6. Überprüfen Sie unter Benutzer und Gruppen hinzugefügt die Gruppe, die Sie hinzufügen möchten.
7. Wählen Sie Absenden aus.
8. Wählen Sie im Navigationsbereich die Option Groups (Gruppen).
9. Auf der Seite Gruppen kann es einige Zeit dauern, bis die von Ihnen angegebene Gruppe in der Liste angezeigt wird. Wählen Sie das Aktualisierungssymbol, um die Liste der Gruppen zu aktualisieren.

Entfernen von Benutzern und Gruppen aus Ihrem Synchronisierungsbereich

Weitere Informationen darüber, was passiert, wenn Sie Benutzer und Gruppen aus Ihrem Synchronisierungsbereich entfernen, finden Sie unter So funktioniert konfigurierbare AD Sync.

So entfernen Sie Benutzer

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie die Registerkarte Users.

5. Aktivieren Sie unter Benutzer im Synchronisierungsbereich das Kontrollkästchen neben dem Benutzer, den Sie löschen möchten. Um alle Benutzer zu löschen, aktivieren Sie das Kontrollkästchen neben Benutzername .
6. Wählen Sie Remove (Entfernen) aus.

So entfernen Sie Gruppen

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Aktivieren Sie unter Gruppen im Synchronisierungsbereich das Kontrollkästchen neben dem Benutzer, den Sie löschen möchten. Um alle Gruppen zu löschen, aktivieren Sie das Kontrollkästchen neben Gruppenname .
6. Wählen Sie Remove (Entfernen) aus.

Pausieren und Fortsetzen Ihrer Synchronisierung

Durch das Anhalten Ihrer Synchronisierung werden alle zukünftigen Synchronisierungszyklen angehalten und alle Änderungen, die Sie an Benutzern und Gruppen in Active Directory vornehmen, werden im IAM Identity Center wiedergegeben. Nachdem Sie die Synchronisierung fortgesetzt haben, übernimmt der Synchronisierungszyklus diese Änderungen ab der nächsten geplanten Synchronisierung.

So pausieren Sie Ihre Synchronisierung

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie unter Sync verwalten die Option Synchronisierung anhalten aus.

So setzen Sie Ihre Synchronisierung fort

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie unter Sync verwalten die Option Synchronisierung fortsetzen aus.

> **Note**
>
> Wenn Sie Synchronisierung anhalten anstelle von Synchronisierung fortsetzen sehen, wurde die Synchronisierung von Active Directory zu IAM Identity Center bereits fortgesetzt.

Konfigurieren von Attributzuordnungen für Ihre Synchronisierung

Weitere Informationen zu verfügbaren Attributen finden Sie unter Attributzuordnungen für AWS Managed Microsoft AD das Verzeichnis.

So konfigurieren Sie Attributzuordnungen in IAM Identity Center zu Ihrem Verzeichnis

1. Öffnen Sie die IAM-Identity-Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, wählen Sie Aktionen und dann Synchronisierung verwalten aus.
4. Wählen Sie unter Sync verwalten die Option Attributzuordnung anzeigen aus.
5. Konfigurieren Sie unter Active-Directory-Benutzerattribute IAM-Identity-Center-Identitätsspeicherattribute und Active-Directory-Benutzerattribute. Beispielsweise können Sie das Identitätsspeicherattribut von IAM Identity Center dem Active-Directory-Benutzerverzeichnisattribut `email` zuordnen`${objectguid}`.

> **Note**
>
> Unter Gruppenattribute können IAM-Identity-Center-Identitätsspeicherattribute und Active-Directory-Gruppenattribute nicht geändert werden.

6. Wählen Sie Änderungen speichern aus. Dadurch kehren Sie zur Seite Sync verwalten zurück.

Automatisieren Ihrer Synchronisierungskonfiguration für konfigurierbare AD-Synchronisierung

Um sicherzustellen, dass Ihr automatisierter Workflow mit der konfigurierbaren AD-Synchronisierung wie erwartet funktioniert, empfehlen wir Ihnen, die folgenden Schritte auszuführen, um Ihre Synchronisierungskonfiguration zu automatisieren.

So automatisieren Sie Ihre Synchronisierungskonfiguration für die konfigurierbare AD-Synchronisierung

1. Erstellen Sie in Active Directory eine übergeordnete Synchronisierungsgruppe, die alle Benutzer und Gruppen enthält, die Sie mit IAM Identity Center synchronisieren möchten. Sie können beispielsweise die Gruppe IAMIdentityCenterAllUsersAndGroups benennen.
2. Fügen Sie in IAM Identity Center die übergeordnete Synchronisierungsgruppe zu Ihrer konfigurierbaren Synchronisierungsliste hinzu. IAM Identity Center synchronisiert alle Benutzer, Gruppen, Untergruppen und Mitglieder aller Gruppen, die in der übergeordneten Synchronisierungsgruppe enthalten sind.
3. Verwenden Sie die von Microsoft bereitgestellten API-Aktionen für die Active-Directory-Benutzer- und -Gruppenverwaltung, um Benutzer und Gruppen zur übergeordneten Synchronisierungsgruppe hinzuzufügen oder daraus zu entfernen.

IAM-Identity-Center-AD-Synchronisierung

Mit IAM Identity Center AD Sync verwenden Sie IAM Identity Center, um Benutzern und Gruppen in Active Directory Zugriff auf AWS-Konten und zu AWS verwalteten Anwendungen oder vom Kunden verwalteten Anwendungen zuzuweisen. Alle Identitäten mit Zuweisungen werden automatisch mit IAM Identity Center synchronisiert.

Funktionsweise von IAM Identity Center AD Sync

IAM Identity Center aktualisiert die AD-basierten Identitätsdaten im Identitätsspeicher mithilfe des folgenden Prozesses.

Erstellung

Wenn Sie Benutzer oder Gruppen mithilfe der AWS Konsole oder der Zuweisungs-API-Aufrufe AWS-Konten oder Anwendungen zuweisen, werden Informationen über die Benutzer, Gruppen und Mitgliedschaft regelmäßig im IAM-Identity-Center-Identitätsspeicher synchronisiert. Benutzer

oder Gruppen, die zu IAM-Identity-Center-Zuweisungen hinzugefügt werden, werden normalerweise innerhalb von zwei Stunden im AWS Identitätsspeicher angezeigt. Abhängig von der Menge der synchronisierten Daten kann dieser Vorgang länger dauern. Nur Benutzer und Gruppen, denen direkt Zugriff zugewiesen ist oder die Mitglieder einer Gruppe sind, denen Zugriff zugewiesen ist, werden synchronisiert.

Gruppen, die Mitglieder anderer Gruppen sind (sogenannte verschachtelte Gruppen), werden ebenfalls in den Identitätsspeicher geschrieben. Wenn Sie Zuweisungen an eine Gruppe in Active Directory vornehmen, die verschachtelte Gruppen enthält, hängt die Art und Weise, wie die Zuweisungen angewendet werden, davon ab, ob Sie AD Sync oder konfigurierbare AD Sync verwenden.

- AD-Synchronisierung – Wenn Sie Zuweisungen an eine Gruppe in Active Directory vornehmen, die verschachtelte Gruppen enthält, können nur die direkten Mitglieder der Gruppe auf das Konto zugreifen. Wenn Sie beispielsweise Zugriff auf Gruppe A zuweisen und Gruppe B Mitglied von Gruppe A ist, können nur die direkten Mitglieder von Gruppe A auf das Konto zugreifen. Keine Mitglieder von Gruppe B erben den Zugriff.
- Konfigurierbare AD-Synchronisierung – Die Verwendung der konfigurierbaren AD-Synchronisierung für Zuweisungen an eine Gruppe in Active Directory, die verschachtelte Gruppen enthält, kann den Umfang der Benutzer erhöhen, die Zugriff auf AWS-Konten oder auf Anwendungen haben. In diesem Fall gilt die Zuweisung für alle Benutzer, einschließlich derjenigen in verschachtelten Gruppen. Wenn Sie beispielsweise Zugriff auf Gruppe A zuweisen und Gruppe B Mitglied von Gruppe A ist, erben Mitglieder von Gruppe B diesen Zugriff ebenfalls.

Wenn ein Benutzer auf IAM Identity Center zugreift, bevor sein Benutzerobjekt zum ersten Mal synchronisiert wurde, wird das Identitätsspeicherobjekt dieses Benutzers bei Bedarf mithilfe just-in-time der (JIT)-Bereitstellung erstellt. Benutzer, die durch die JIT-Bereitstellung erstellt wurden, werden nur synchronisiert, wenn sie direkt oder gruppenbasierte IAM-Identity-Center-Berechtigungen zugewiesen haben. Gruppenmitgliedschaften für von JIT bereitgestellte Benutzer sind bis nach der Synchronisation nicht verfügbar.

Anweisungen zum Zuweisen von Benutzerzugriff auf AWS-Kontenfinden Sie unter Single Sign-On-Zugriff auf AWS-Konten.

Aktualisierung

Die Identitätsdaten im IAM-Identity-Center-Identitätsspeicher bleiben aktuell, indem sie regelmäßig Daten aus dem Quellverzeichnis in Active Directory lesen. Identitätsdaten, die in Active Directory

geändert werden, werden normalerweise innerhalb von vier Stunden im AWS Identitätsspeicher angezeigt. Abhängig von der Menge der synchronisierten Daten kann dieser Vorgang länger dauern.

Benutzer- und Gruppenobjekte und ihre Mitgliedschaften werden in IAM Identity Center erstellt oder aktualisiert, um sie den entsprechenden Objekten im Quellverzeichnis in Active Directory zuzuordnen. Für Benutzerattribute wird nur die Teilmenge der Attribute aktualisiert, die im Abschnitt Attribute für die Zugriffskontrolle verwalten der IAM-Identity-Center-Konsole aufgeführt sind. Darüber hinaus werden Benutzerattribute bei jedem Benutzerauthentifizierungsereignis aktualisiert.

Löschung

Benutzer und Gruppen werden aus dem IAM-Identity-Center-Identitätsspeicher gelöscht, wenn die entsprechenden Benutzer- oder Gruppenobjekte aus dem Quellverzeichnis in Active Directory gelöscht werden.

Stellen Sie eine Connect zu einem externen Identitätsanbieter her

Wenn Sie ein selbstverwaltetes Verzeichnis in Active Directory oder einem anderen verwenden, finden Sie weitere Informationen unter. AWS Managed Microsoft ADHerstellen einer Verbindung mit einem Microsoft AD Verzeichnis Bei anderen externen Identitätsanbietern (IdPs) können Sie Identitäten IdPs anhand des Security Assertion Markup Language (SAML) 2.0-Standards authentifizieren. AWS IAM Identity Center Auf diese Weise können sich Ihre Benutzer mit ihren Unternehmensanmeldedaten beim AWS Access Portal anmelden. Sie können dann zu den ihnen zugewiesenen Konten, Rollen und Anwendungen navigieren, die auf einem externen Server gehostet IdPs werden.

Sie können beispielsweise einen externen IdP wie Okta oder Microsoft Entra ID mit dem IAM Identity Center verbinden. Ihre Benutzer können sich dann mit ihren vorhandenen AWS Zugangsdaten Okta oder Microsoft Entra ID Anmeldedaten beim Zugriffsportal anmelden. Um zu kontrollieren, was Ihre Benutzer nach der Anmeldung tun können, können Sie ihnen zentral Zugriffsberechtigungen für alle Konten und Anwendungen in Ihrer AWS Organisation zuweisen. Darüber hinaus können sich Entwickler einfach mit ihren vorhandenen Anmeldeinformationen bei AWS Command Line Interface (AWS CLI) anmelden und von der automatischen kurzfristigen Generierung und Rotation von Anmeldeinformationen profitieren.

Das SAML-Protokoll bietet keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Daher müssen Sie IAM Identity Center auf diese Benutzer und Gruppen aufmerksam machen, indem Sie sie in IAM Identity Center bereitstellen.

Bereitstellung, wenn Benutzer von einem externen IdP kommen

Wenn Sie einen externen IdP verwenden, müssen Sie alle entsprechenden Benutzer und Gruppen in IAM Identity Center bereitstellen, bevor Sie Zuweisungen zu AWS-Konten unseren Anwendungen vornehmen können. Dazu können Sie Automatische Bereitstellung für Ihre Benutzer und Gruppen konfigurieren oder verwenden. Manuelle Bereitstellung Unabhängig davon, wie Sie Benutzer bereitstellen, leitet IAM Identity Center die AWS Management Console Befehlszeilenschnittstelle und die Anwendungsauthentifizierung an Ihren externen IdP weiter. IAM Identity Center gewährt dann Zugriff auf diese Ressourcen auf der Grundlage der Richtlinien, die Sie in IAM Identity Center erstellen. Weitere Informationen zur Bereitstellung finden Sie unter. Bereitstellung von Benutzern und Gruppen

Wie stelle ich eine Verbindung zu einem externen Identitätsanbieter her

Es sind step-by-step Tutorials für folgende Programme verfügbar IdPs:

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Ping-Identität

Für die verschiedenen unterstützten externen IdPs Geräte gelten unterschiedliche Voraussetzungen, Überlegungen und Bereitstellungsverfahren. Das folgende Verfahren bietet einen allgemeinen Überblick über das Verfahren, das bei allen externen Identitätsanbietern verwendet wird.

So stellen Sie eine Verbindung zu einem externen Identitätsanbieter her

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Identitätsquelle ändern“.
4. Wählen Sie unter Identitätsquelle auswählen die Option Externer Identitätsanbieter und dann Weiter aus.

5. Gehen Sie unter Externen Identitätsanbieter konfigurieren wie folgt vor:

   a. Wählen Sie unter Metadaten des Dienstanbieters die Option Metadatendatei herunterladen aus, um die Metadatendatei herunterzuladen und auf Ihrem System zu speichern. Die SAML-Metadatendatei von IAM Identity Center wird von Ihrem externen Identitätsanbieter benötigt.

   b. Wählen Sie unter Metadaten des Identitätsanbieters die Option Datei auswählen aus und suchen Sie nach der Metadatendatei, die Sie von Ihrem externen Identitätsanbieter heruntergeladen haben. Laden Sie dann die Datei hoch. Diese Metadatendatei enthält das erforderliche öffentliche x509-Zertifikat, das verwendet wird, um Nachrichten zu vertrauen, die vom IdP gesendet werden.

   c. Wählen Sie Weiter aus.

   > **Important**
   >
   > Wenn Sie Ihre Quelle zu oder von Active Directory ändern, werden alle vorhandenen Benutzer- und Gruppenzuweisungen entfernt. Sie müssen die Zuweisungen manuell erneut anwenden, nachdem Sie Ihre Quelle erfolgreich geändert haben.

6. Nachdem Sie den Haftungsausschluss gelesen haben und bereit sind, fortzufahren, geben Sie ACCEPT ein.
7. Wählen Sie „Identitätsquelle ändern“. In einer Statusmeldung werden Sie darüber informiert, dass Sie die Identitätsquelle erfolgreich geändert haben.

Themen

- Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern
- SCIM-Profil und SAML 2.0-Implementierung

Verwenden des SAML- und SCIM-Identitätsverbunds mit externen Identitätsanbietern

IAM Identity Center implementiert die folgenden standardbasierten Protokolle für den Identitätsverbund:

- SAML 2.0 für die Benutzerauthentifizierung
- SCIM für die Bereitstellung

Von jedem Identitätsanbieter (IdP), der diese Standardprotokolle implementiert, wird erwartet, dass er erfolgreich mit IAM Identity Center zusammenarbeitet, wobei die folgenden besonderen Überlegungen zu beachten sind:

- SAML
  - IAM Identity Center erfordert ein SAML-NameID-Format für die E-Mail-Adresse (d. h.). `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - Der Wert des Felds NameID in Assertionen muss eine RFC 2822 (https://tools.ietf.org/html/rfc2822) addr-spec-konforme („“) Zeichenfolge (https://tools.ietf.org/html/rfc2822#section-3.4.1) sein. `name@domain.com`
  - Die Metadatendatei darf nicht mehr als 75000 Zeichen enthalten.
  - Die Metadaten müssen eine EntityID und ein X509-Zertifikat enthalten und Teil der SingleSignOnService Anmelde-URL sein.
  - Ein Verschlüsselungsschlüssel wird nicht unterstützt.

- SCIM
  - Die SCIM-Implementierung von IAM Identity Center basiert auf den SCIM-RFCs 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643) und 7644 (https://tools.ietf.org/html/rfc7644) sowie den Interoperabilitätsanforderungen, die im Entwurf des Basic SCIM Profile 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4) vom März 2020 festgelegt wurden. FastFed Alle Unterschiede zwischen diesen Dokumenten und der aktuellen Implementierung in IAM Identity Center werden im Abschnitt Unterstützte API-Operationen des IAM Identity Center SCIM Implementation Developer Guide beschrieben.

IdPs die nicht den oben genannten Standards und Überlegungen entsprechen, werden nicht unterstützt. Bitte wenden Sie sich an Ihren IdP, wenn Sie Fragen oder Erläuterungen zur Konformität seiner Produkte mit diesen Standards und Überlegungen haben.

Wenn Sie Probleme haben, Ihren IdP mit dem IAM Identity Center zu verbinden, empfehlen wir Ihnen, Folgendes zu überprüfen:

- AWS CloudTrail protokolliert, indem nach dem Ereignisnamen P gefiltert wird ExternalId DirectoryLogin
- IDP-spezifische Logs und/oder Debug-Logs
- Behebung von Problemen mit IAM Identity Center

> **Note**
>
> Einige IdPs, wie die in derErste Schritte mit Tutorials, bieten eine vereinfachte Konfiguration für IAM Identity Center in Form einer „Anwendung“ oder eines „Connectors“, die speziell für IAM Identity Center entwickelt wurden. Wenn Ihr IdP diese Option anbietet, empfehlen wir Ihnen, sie zu verwenden. Achten Sie darauf, den Artikel auszuwählen, der speziell für IAM Identity Center entwickelt wurde. Andere Elemente, die als „AWS“, „AWS Federation“ oder ähnliche generische "AWS" Namen bezeichnet werden, verwenden möglicherweise andere Verbundansätze und/oder Endpunkte und funktionieren möglicherweise nicht wie erwartet mit IAM Identity Center.

SCIM-Profil und SAML 2.0-Implementierung

Sowohl SCIM als auch SAML sind wichtige Überlegungen bei der Konfiguration von IAM Identity Center.

SAML 2.0-Implementierung

IAM Identity Center unterstützt den Identitätsverbund mit SAML (Security Assertion Markup Language) 2.0. Dadurch kann IAM Identity Center Identitäten von externen Identitätsanbietern authentifizieren (). IdPs SAML 2.0 ist ein offener Standard, der für den sicheren Austausch von SAML-Assertionen verwendet wird. SAML 2.0 überträgt Informationen über einen Benutzer zwischen einer SAML-Behörde (als Identitätsanbieter oder IdP bezeichnet) und einem SAML-Verbraucher (als Service Provider oder SP bezeichnet). Der IAM Identity Center-Dienst verwendet diese Informationen, um föderiertes Single Sign-On bereitzustellen. Single Sign-On ermöglicht Benutzern den Zugriff auf AWS-Konten und die Konfiguration von Anwendungen auf der Grundlage ihrer vorhandenen Identity Provider-Anmeldeinformationen.

IAM Identity Center erweitert Ihren IAM Identity Center-Shop oder einen externen Identitätsanbieter um SAML-IdP-Funktionen. AWS Managed Microsoft AD Benutzer können sich dann per Single Sign-On bei Diensten anmelden, die SAML unterstützen, einschließlich Anwendungen AWS Management Console und Drittanbieteranwendungen wie, und. Microsoft 365 Concur Salesforce

Das SAML-Protokoll bietet jedoch keine Möglichkeit, den IdP abzufragen, um mehr über Benutzer und Gruppen zu erfahren. Daher müssen Sie IAM Identity Center auf diese Benutzer und Gruppen aufmerksam machen, indem Sie sie in IAM Identity Center bereitstellen.

SCIM-Profil

IAM Identity Center unterstützt den Standard System for Cross-Domain Identity Management (SCIM) v2.0. SCIM synchronisiert Ihre IAM Identity Center-Identitäten mit den Identitäten Ihres IdP. Dies beinhaltet jegliche Bereitstellung, Aktualisierung und Deprovisionierung von Benutzern zwischen Ihrem IdP und IAM Identity Center.

Weitere Informationen zur Implementierung von SCIM finden Sie unter. Automatische Bereitstellung Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im IAM Identity Center SCIM Implementation Developer Guide.

Themen

- Automatische Bereitstellung
- Manuelle Bereitstellung
- SAML 2.0-Zertifikate verwalten

Automatische Bereitstellung

IAM Identity Center unterstützt die automatische Bereitstellung (Synchronisation) von Benutzer- und Gruppeninformationen von Ihrem Identity Provider (IdP) in IAM Identity Center mithilfe des Systems for Cross-Domain Identity Management (SCIM) v2.0-Protokoll. Wenn Sie die SCIM-Synchronisierung konfigurieren, erstellen Sie eine Zuordnung Ihrer Identity Provider (IdP) -Benutzerattribute zu den benannten Attributen in IAM Identity Center. Dadurch stimmen die erwarteten Attribute zwischen IAM Identity Center und Ihrem IdP überein. Sie konfigurieren diese Verbindung in Ihrem IdP mithilfe Ihres SCIM-Endpunkts für IAM Identity Center und eines Bearer-Tokens, das Sie in IAM Identity Center erstellen.

Themen

- Überlegungen zur Verwendung der automatischen Bereitstellung
- Wie überwacht man den Ablauf von Zugriffstoken
- Wie aktiviert man die automatische Bereitstellung
- Wie deaktiviere ich die automatische Bereitstellung
- Wie generiert man ein neues Zugriffstoken
- Wie lösche ich ein Zugriffstoken
- Wie rotiert man ein Zugriffstoken

Überlegungen zur Verwendung der automatischen Bereitstellung

Bevor Sie mit der Bereitstellung von SCIM beginnen, empfehlen wir Ihnen, zunächst die folgenden wichtigen Überlegungen zur Funktionsweise von SCIM mit IAM Identity Center zu lesen. Weitere Überlegungen zur Bereitstellung finden Sie in den für Ihren IdP Erste Schritte mit Tutorials geltenden Bestimmungen.

- Wenn Sie eine primäre E-Mail-Adresse bereitstellen, muss dieser Attributwert für jeden Benutzer eindeutig sein. In einigen IdPs Fällen ist die primäre E-Mail-Adresse möglicherweise keine echte E-Mail-Adresse. Beispielsweise könnte es sich um einen Universal Principal Name (UPN) handeln, der nur wie eine E-Mail aussieht. Diese IdPs können eine sekundäre oder „andere“ E-Mail-Adresse haben, die die tatsächliche E-Mail-Adresse des Benutzers enthält. Sie müssen SCIM in Ihrem IdP so konfigurieren, dass die eindeutige E-Mail-Adresse ungleich NULL dem primären E-Mail-Adressattribut von IAM Identity Center zugeordnet wird. Und Sie müssen die eindeutige Anmelde-ID des Benutzers, die nicht NULL ist, dem Benutzernamenattribut von IAM Identity Center zuordnen. Prüfen Sie, ob Ihr IdP einen einzigen Wert hat, der sowohl die Anmelde-ID als auch den E-Mail-Namen des Benutzers ist. Wenn ja, können Sie dieses IdP-Feld sowohl der primären IAM Identity Center-E-Mail-Adresse als auch dem IAM Identity Center-Benutzernamen zuordnen.
- Damit die SCIM-Synchronisierung funktioniert, müssen für jeden Benutzer die Werte Vorname, Nachname, Benutzername und Anzeigename angegeben werden. Wenn einer dieser Werte bei einem Benutzer fehlt, wird diesem Benutzer keine Provisionierung zugewiesen.
- Wenn Sie Anwendungen von Drittanbietern verwenden müssen, müssen Sie zunächst das Betreffattribut für ausgehende SAML dem Benutzernamenattribut zuordnen. Wenn die Drittanbieteranwendung eine routbare E-Mail-Adresse benötigt, müssen Sie Ihrem IdP das E-Mail-Attribut zur Verfügung stellen.
- Die SCIM-Bereitstellungs- und Aktualisierungsintervalle werden von Ihrem Identitätsanbieter gesteuert. Änderungen an Benutzern und Gruppen in Ihrem Identity Provider werden erst in IAM Identity Center übernommen, nachdem Ihr Identity Provider diese Änderungen an IAM Identity Center gesendet hat. Einzelheiten zur Häufigkeit von Benutzer- und Gruppenaktualisierungen erhalten Sie bei Ihrem Identitätsanbieter.
- Derzeit werden mehrwertige Attribute (wie mehrere E-Mails oder Telefonnummern für einen bestimmten Benutzer) nicht mit SCIM bereitgestellt. Versuche, mehrwertige Attribute mit SCIM mit IAM Identity Center zu synchronisieren, schlagen fehl. Um Fehler zu vermeiden, stellen Sie sicher, dass für jedes Attribut nur ein einziger Wert übergeben wird. Wenn Sie Benutzer mit mehrwertigen Attributen haben, entfernen oder ändern Sie die doppelten Attributzuordnungen in SCIM bei Ihrem IdP für die Verbindung zum IAM Identity Center.

- Stellen Sie sicher, dass die `externalId` SCIM-Zuordnung bei Ihrem IdP einem Wert entspricht, der eindeutig und immer vorhanden ist und sich für Ihre Benutzer am wenigsten ändert. Beispielsweise kann Ihr IdP eine garantierte `objectId` oder eine andere Kennung bereitstellen, auf die sich Änderungen an Benutzerattributen wie Name und E-Mail nicht auswirken. Wenn ja, können Sie diesen Wert dem `externalId` SCIM-Feld zuordnen. Dadurch wird sichergestellt, dass Ihre Benutzer keine AWS Berechtigungen, Zuweisungen oder Berechtigungen verlieren, wenn Sie ihren Namen oder ihre E-Mail-Adresse ändern müssen.
- Benutzer, denen noch keine Anwendung zugewiesen wurde oder denen AWS-Konto keine Bereitstellung für IAM Identity Center möglich ist. Um Benutzer und Gruppen zu synchronisieren, stellen Sie sicher, dass sie der Anwendung oder einem anderen Setup zugewiesen sind, das die Verbindung Ihres IdP zum IAM Identity Center darstellt.
- Das Verhalten bei der Deprovisionierung von Benutzern wird vom Identitätsanbieter verwaltet und kann je nach Implementierung variieren. Einzelheiten zur Deprovisionierung von Benutzern erhalten Sie bei Ihrem Identitätsanbieter.

Weitere Informationen zur SCIM-Implementierung von IAM Identity Center finden Sie im IAM Identity Center SCIM Implementation Developer Guide.

Wie überwacht man den Ablauf von Zugriffstoken

SCIM-Zugriffstoken werden mit einer Gültigkeit von einem Jahr generiert. Wenn Ihr SCIM-Zugriffstoken so eingestellt ist, dass es in 90 Tagen oder weniger abläuft, AWS sendet es Ihnen in der IAM Identity Center-Konsole und über das AWS Health Dashboard Erinnerungen, damit Sie das Token wechseln können. Indem Sie das SCIM-Zugriffstoken rotieren, bevor es abläuft, stellen Sie kontinuierlich die automatische Bereitstellung von Benutzer- und Gruppeninformationen sicher. Wenn das SCIM-Zugriffstoken abläuft, wird die Synchronisation von Benutzer- und Gruppeninformationen von Ihrem Identitätsanbieter mit dem IAM Identity Center beendet, sodass bei der automatischen Bereitstellung keine Aktualisierungen mehr vorgenommen oder Informationen erstellt und gelöscht werden können. Eine Unterbrechung der automatischen Bereitstellung kann zu erhöhten Sicherheitsrisiken führen und den Zugriff auf Ihre Dienste beeinträchtigen.

Die Erinnerungen der Identity Center-Konsole bleiben bestehen, bis Sie das SCIM-Zugriffstoken rotieren und alle ungenutzten oder abgelaufenen Zugriffstoken löschen. Die AWS Health Dashboard-Ereignisse werden wöchentlich zwischen 90 und 60 Tagen, zweimal pro Woche zwischen 60 und 30 Tagen, dreimal pro Woche zwischen 30 und 15 Tagen und täglich zwischen 15 Tagen, bis die SCIM-Zugriffstoken ablaufen, erneuert.

Wie aktiviert man die automatische Bereitstellung

Gehen Sie wie folgt vor, um die automatische Bereitstellung von Benutzern und Gruppen von Ihrem IdP an das IAM Identity Center mithilfe des SCIM-Protokolls zu aktivieren.

> **Note**
>
> Bevor Sie mit diesem Verfahren beginnen, empfehlen wir Ihnen, zunächst die Überlegungen zur Bereitstellung zu überprüfen, die für Ihren IdP gelten. Weitere Informationen finden Sie unter Erste Schritte mit Tutorials Für Ihren IdP.

Um die automatische Bereitstellung im IAM Identity Center zu aktivieren

1. Nachdem Sie die Voraussetzungen erfüllt haben, öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Einstellungen aus.
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Automatische Bereitstellung und wählen Sie dann Aktivieren aus. Dadurch wird sofort die automatische Bereitstellung im IAM Identity Center aktiviert und die erforderlichen SCIM-Endpoint- und Zugriffstoken-Informationen werden angezeigt.
4. Kopieren Sie im Dialogfeld Automatische Bereitstellung für eingehende Nachrichten die einzelnen Werte für die folgenden Optionen. Sie müssen diese später einfügen, wenn Sie die Bereitstellung in Ihrem IdP konfigurieren.
   a. SCIM-Endpunkt
   b. Zugriffstoken
5. Klicken Sie auf Schließen.

Nachdem Sie dieses Verfahren abgeschlossen haben, müssen Sie die automatische Bereitstellung in Ihrem IdP konfigurieren. Weitere Informationen finden Sie unter Erste Schritte mit Tutorials Für Ihren IdP.

Wie deaktiviere ich die automatische Bereitstellung

Gehen Sie wie folgt vor, um die automatische Bereitstellung in der IAM Identity Center-Konsole zu deaktivieren.

> **Important**
>
> Sie müssen das Zugriffstoken löschen, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter Wie lösche ich ein Zugriffstoken.

Um die automatische Bereitstellung in der IAM Identity Center-Konsole zu deaktivieren

1. Wählen Sie in der IAM Identity Center-Konsole im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung die Option Deaktivieren aus.
4. Überprüfen Sie im Dialogfeld Automatische Bereitstellung deaktivieren die Informationen, geben Sie DISABLE ein, und wählen Sie dann Automatische Bereitstellung deaktivieren aus.

Wie generiert man ein neues Zugriffstoken

Gehen Sie wie folgt vor, um ein neues Zugriffstoken in der IAM Identity Center-Konsole zu generieren.

> **Note**
>
> Für dieses Verfahren müssen Sie zuvor die automatische Bereitstellung aktiviert haben. Weitere Informationen finden Sie unter Wie aktiviert man die automatische Bereitstellung.

Um ein neues Zugriffstoken zu generieren

1. Wählen Sie in der IAM Identity Center-Konsole im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung unter Zugriffstoken die Option Token generieren aus.
4. Kopieren Sie im Dialogfeld Neues Zugriffstoken generieren das neue Zugriffstoken und speichern Sie es an einem sicheren Ort.
5. Klicken Sie auf Schließen.

Wie lösche ich ein Zugriffstoken

Gehen Sie wie folgt vor, um ein vorhandenes Zugriffstoken in der IAM Identity Center-Konsole zu löschen.

Um ein vorhandenes Zugriffstoken zu löschen

1. Wählen Sie in der IAM Identity Center-Konsole im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Wählen Sie auf der Seite Automatische Bereitstellung unter Zugriffstoken das Zugriffstoken aus, das Sie löschen möchten, und wählen Sie dann Löschen aus.
4. Überprüfen Sie im Dialogfeld Zugriffstoken löschen die Informationen, geben Sie DELETE ein, und wählen Sie dann Zugriffstoken löschen aus.

Wie rotiert man ein Zugriffstoken

Ein IAM Identity Center-Verzeichnis unterstützt bis zu zwei Zugriffstoken gleichzeitig. Um vor jeder Rotation ein zusätzliches Zugriffstoken zu generieren, löschen Sie alle abgelaufenen oder ungenutzten Zugriffstoken.

Wenn Ihr SCIM-Zugriffstoken bald abläuft, können Sie das folgende Verfahren verwenden, um ein vorhandenes Zugriffstoken in der IAM Identity Center-Konsole rotieren zu lassen.

Um ein Zugriffstoken zu rotieren

1. Wählen Sie in der IAM Identity Center-Konsole im linken Navigationsbereich Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Bereitstellung verwalten“.
3. Notieren Sie sich auf der Seite Automatische Bereitstellung unter Zugriffstoken die Token-ID des Tokens, das Sie rotieren möchten.
4. Folgen Sie den Schritten unterWie generiert man ein neues Zugriffstoken, um ein neues Token zu erstellen. Wenn Sie bereits die maximale Anzahl von SCIM-Zugriffstoken erstellt haben, müssen Sie zunächst eines der vorhandenen Token löschen.
5. Rufen Sie die Website Ihres Identitätsanbieters auf und konfigurieren Sie das neue Zugriffstoken für die SCIM-Bereitstellung. Testen Sie dann die Konnektivität zum IAM Identity Center mithilfe des neuen SCIM-Zugriffstokens. Sobald Sie bestätigt haben, dass die Bereitstellung mit dem

neuen Token erfolgreich funktioniert, fahren Sie mit dem nächsten Schritt in diesem Verfahren fort.

6. Folgen Sie den Schritten unterWie lösche ich ein Zugriffstoken, um das alte Zugriffstoken zu löschen, das Sie zuvor notiert haben. Sie können das Erstellungsdatum des Tokens auch als Hinweis dafür verwenden, welches Token entfernt werden soll.

Manuelle Bereitstellung

Einige bieten IdPs keine SCIM-Unterstützung (System for Cross-Domain Identity Management) oder verfügen über eine inkompatible SCIM-Implementierung. In diesen Fällen können Sie Benutzer manuell über die IAM Identity Center-Konsole bereitstellen. Wenn Sie Benutzer zu IAM Identity Center hinzufügen, stellen Sie sicher, dass der Benutzername mit dem Benutzernamen identisch ist, den Sie in Ihrem IdP haben. Sie müssen mindestens eine eindeutige E-Mail-Adresse und einen eindeutigen Benutzernamen haben. Weitere Informationen finden Sie unter Eindeutigkeit von Benutzername und E-Mail-Adresse.

Außerdem müssen Sie alle Gruppen manuell in IAM Identity Center verwalten. Dazu erstellen Sie die Gruppen und fügen sie mithilfe der IAM Identity Center-Konsole hinzu. Diese Gruppen müssen nicht mit dem übereinstimmen, was in Ihrem IdP vorhanden ist. Weitere Informationen finden Sie unter Gruppen.

SAML 2.0-Zertifikate verwalten

IAM Identity Center verwendet Zertifikate, um eine SAML-Vertrauensstellung zwischen IAM Identity Center und Ihrem externen Identitätsanbieter (IdP) einzurichten. Wenn Sie einen externen IdP in IAM Identity Center hinzufügen, müssen Sie außerdem mindestens ein öffentliches SAML 2.0 X.509-Zertifikat vom externen IdP beziehen. Dieses Zertifikat wird normalerweise automatisch während des IdP-SAML-Metadatenaustauschs während der Vertrauenserstellung installiert.

Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere IdP-Zertifikate durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein IdP-Zertifikat ersetzen, wenn sich das Ablaufdatum des Zertifikats nähert. Der Vorgang des Ersetzens eines älteren Zertifikats durch ein neueres wird als Zertifikatsrotation bezeichnet.

Themen

- Ein SAML 2.0-Zertifikat rotieren
- Indikatoren für den Ablaufstatus des Zertifikats

Ein SAML 2.0-Zertifikat rotieren

Möglicherweise müssen Sie Zertifikate regelmäßig importieren, um ungültige oder abgelaufene Zertifikate, die von Ihrem Identitätsanbieter ausgestellt wurden, rotieren zu lassen. Dies trägt dazu bei, Unterbrechungen oder Ausfallzeiten bei der Authentifizierung zu vermeiden. Alle importierten Zertifikate sind automatisch aktiv. Zertifikate sollten erst gelöscht werden, nachdem sichergestellt wurde, dass sie nicht mehr mit dem zugehörigen Identitätsanbieter verwendet werden.

Sie sollten auch berücksichtigen, dass einige Zertifikate IdPs möglicherweise nicht mehrere Zertifikate unterstützen. In diesem Fall IdPs kann die Rotation von Zertifikaten mit diesen Zertifikaten eine vorübergehende Unterbrechung des Dienstes für Ihre Benutzer bedeuten. Der Dienst wird wiederhergestellt, wenn das Vertrauen zu diesem IdP erfolgreich wiederhergestellt wurde. Planen Sie diesen Vorgang möglichst außerhalb der Spitzenzeiten sorgfältig.

> **Note**
>
> Aus Sicherheitsgründen sollten Sie bei Anzeichen einer Beeinträchtigung oder falschen Handhabung eines vorhandenen SAML-Zertifikats das Zertifikat sofort entfernen und rotieren lassen.

Die Rotation eines IAM Identity Center-Zertifikats ist ein mehrstufiger Prozess, der Folgendes umfasst:

- Ein neues Zertifikat vom IdP erhalten
- Das neue Zertifikat wird in das IAM Identity Center importiert
- Aktivierung des neuen Zertifikats im IdP
- Löschen des älteren Zertifikats

Verwenden Sie alle der folgenden Verfahren, um den Zertifikatsrotationsprozess abzuschließen und gleichzeitig Ausfallzeiten bei der Authentifizierung zu vermeiden.

Schritt 1: Besorgen Sie sich ein neues Zertifikat vom IdP

Gehen Sie zur IdP-Website und laden Sie ihr SAML 2.0-Zertifikat herunter. Stellen Sie sicher, dass die Zertifikatsdatei im PEM-codierten Format heruntergeladen wurde. Bei den meisten Anbietern können Sie mehrere SAML 2.0-Zertifikate im IdP erstellen. Es ist wahrscheinlich, dass diese als deaktiviert oder inaktiv markiert werden.

Schritt 2: Importieren Sie das neue Zertifikat in IAM Identity Center

Gehen Sie wie folgt vor, um das neue Zertifikat mithilfe der IAM Identity Center-Konsole zu importieren.

1. Wählen Sie in der IAM Identity Center-Konsole Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Authentifizierung verwalten“.
3. Wählen Sie auf der Seite SAML 2.0-Zertifikate verwalten die Option Zertifikat importieren aus.
4. Wählen Sie im Dialogfeld SAML 2.0-Zertifikat importieren die Option Datei auswählen aus, navigieren Sie zu Ihrer Zertifikatsdatei, wählen Sie sie aus und wählen Sie dann Zertifikat importieren aus.

Ab diesem Zeitpunkt vertraut IAM Identity Center allen eingehenden SAML-Nachrichten, die von beiden importierten Zertifikaten signiert wurden.

Schritt 3: Aktivieren Sie das neue Zertifikat im IdP

Gehen Sie zurück zur IdP-Website und markieren Sie das neue Zertifikat, das Sie zuvor erstellt haben, als primär oder aktiv. Zu diesem Zeitpunkt sollten alle vom IdP signierten SAML-Nachrichten das neue Zertifikat verwenden.

Schritt 4: Löschen Sie das alte Zertifikat

Gehen Sie wie folgt vor, um den Zertifikatsrotationsprozess für Ihren IdP abzuschließen. Es muss immer mindestens ein gültiges Zertifikat aufgeführt sein, das nicht entfernt werden kann.

> **Note**
>
> Stellen Sie sicher, dass Ihr Identitätsanbieter keine SAML-Antworten mehr mit diesem Zertifikat signiert, bevor Sie es löschen.

1. Wählen Sie auf der Seite SAML 2.0-Zertifikate verwalten das Zertifikat aus, das Sie löschen möchten. Wählen Sie Löschen aus.
2. Geben Sie im Dialogfeld SAML 2.0-Zertifikat löschen **DELETE** zur Bestätigung den Text ein, und wählen Sie dann Löschen aus.

3. Kehren Sie zur Website des IdP zurück und führen Sie die erforderlichen Schritte aus, um das ältere inaktive Zertifikat zu entfernen.

Indikatoren für den Ablaufstatus des Zertifikats

Auf der Seite „SAML 2.0-Zertifikate verwalten“ werden Ihnen möglicherweise farbige Statusanzeigesymbole auffallen. Diese Symbole werden in der Spalte Läuft ab neben jedem Zertifikat in der Liste angezeigt. Im Folgenden werden die Kriterien beschrieben, anhand derer IAM Identity Center bestimmt, welches Symbol für jedes Zertifikat angezeigt wird.

- Rot — Zeigt an, dass ein Zertifikat derzeit abgelaufen ist.
- Gelb — Zeigt an, dass ein Zertifikat in 90 Tagen oder weniger abläuft.
- Grün — Zeigt an, dass ein Zertifikat derzeit gültig ist und noch mindestens 90 Tage gültig bleibt.

Um den aktuellen Status eines Zertifikats zu überprüfen

1. Wählen Sie in der IAM Identity Center-Konsole Einstellungen aus.
2. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Identitätsquelle“ und dann „Aktionen“ > „Authentifizierung verwalten“.
3. Überprüfen Sie auf der Seite SAML 2.0-Authentifizierung verwalten unter SAML 2.0-Zertifikate verwalten den Status der Zertifikate in der Liste, wie in der Spalte Läuft ab am angegeben.

Nutzung des AWS Zugangsportals

Das AWS Zugriffsportal bietet Ihnen (Endbenutzern) Single Sign-On-Zugriff auf all Ihre AWS-Konten und die am häufigsten verwendeten Cloud-Anwendungen wie Office 365, Concur, Salesforce und viele mehr. Sie können schnell mehrere Anwendungen starten, indem Sie einfach das Anwendungssymbol AWS-Konto oder im Portal auswählen. Das Vorhandensein von Anwendungssymbolen in Ihrem AWS Zugriffsportal bedeutet, dass Ihnen ein Administrator Ihres Unternehmens Zugriff auf diese AWS-Konten oder Anwendungen gewährt hat. Dies bedeutet auch, dass Sie vom Access-Portal aus ohne zusätzliche Anmeldeaufforderungen auf all diese Konten oder Anwendungen AWS zugreifen können.

Wenden Sie sich in den folgenden Situationen an Ihren Administrator, um zusätzlichen Zugriff anzufordern:

- Sie sehen keine AWS-Konto Oder-Anwendung, auf die Sie zugreifen müssen.

- Der Zugriff, den Sie auf ein bestimmtes Konto oder eine bestimmte Anwendung haben, entspricht nicht Ihren Erwartungen.

Themen

Annahme der Einladung zum Beitritt zum IAM Identity Center

Wenn Sie sich zum ersten Mal beim AWS Zugangsportal anmelden, finden Sie in Ihrer E-Mail Anweisungen zur Aktivierung Ihrer Benutzeranmeldedaten.

Um Ihre Benutzeranmeldedaten zu aktivieren

1. Wählen Sie je nach der E-Mail, die Sie von Ihrem Unternehmen erhalten haben, eine der folgenden Methoden, um Ihre Benutzeranmeldeinformationen zu aktivieren, damit Sie das AWS Zugangsportal nutzen können.

   a. Wenn Sie eine E-Mail mit dem Betreff Einladung zum Beitritt zu AWS IAM Identity Center (Nachfolger von AWS Single Sign-On) erhalten haben, öffnen Sie sie und wählen Sie Einladung annehmen aus. Geben Sie auf der Anmeldeseite für neue Benutzer ein Passwort ein, bestätigen Sie es und wählen Sie dann Neues Passwort festlegen. Sie verwenden dieses Passwort jedes Mal, wenn Sie sich im Portal anmelden.

   b. Wenn Sie vom IT-Support oder IT-Administrator Ihres Unternehmens eine E-Mail erhalten haben, folgen Sie den dort angegebenen Anweisungen, um Ihre Benutzeranmeldeinformationen zu aktivieren.

2. Nachdem Sie Ihre Benutzeranmeldedaten durch Eingabe eines neuen Kennworts aktiviert haben, meldet Sie das AWS Zugangsportal automatisch an. Geschieht dies nicht, können Sie sich mithilfe der Anweisungen im nächsten Abschnitt manuell beim AWS Access Portal anmelden.

Melden Sie sich beim AWS Access-Portal an

Zu diesem Zeitpunkt sollte Ihnen von einem Administrator eine bestimmte Anmelde-URL für das AWS Zugangsportal zur Verfügung gestellt worden sein. Sobald Sie diese URL haben, können Sie mit der Anmeldung im Portal fortfahren. Weitere Informationen finden Sie unter Beim AWS Access-Portal anmelden.

> **Note**
>
> Nachdem Sie sich angemeldet haben, beträgt die Standarddauer für Ihre AWS Access-Portal-Sitzung 8 Stunden. Beachten Sie, dass ein Administrator die Dauer dieser Sitzung ändern kann.

Vertrauenswürdige Geräte

Wenn Sie auf der Anmeldeseite die Option Dies ist ein vertrauenswürdiges Gerät auswählen, betrachtet IAM Identity Center alle future Anmeldungen von diesem Gerät als autorisiert. Das bedeutet, dass IAM Identity Center keine Option zur Eingabe eines MFA-Code anbietet, solange Sie dieses vertrauenswürdige Gerät verwenden. Es gibt jedoch einige Ausnahmen, z. B. wenn Sie sich über einen neuen Browser anmelden oder wenn Ihrem Gerät eine unbekannte IP-Adresse zugewiesen wurde.

Tipps zur Anmeldung für das AWS Zugangsportal

Im Folgenden finden Sie einige Tipps, die Ihnen bei der Verwaltung Ihres AWS Access-Portal-Erlebnisses helfen sollen.

- Gelegentlich müssen Sie sich möglicherweise ab- und wieder beim AWS Access Portal anmelden. Dies kann eventuell notwendig sein, um auf neue Anwendungen zuzugreifen, die Ihnen vom Administrator erst kürzlich zugewiesen wurden. Es ist jedoch nicht zwingend erforderlich, da alle neuen Anwendungen stündlich aktualisiert werden.
- Wenn Sie sich beim AWS Access-Portal anmelden, können Sie jede der im Portal aufgelisteten Anwendungen öffnen, indem Sie das Anwendungssymbol auswählen. Nachdem Sie die Anwendung nicht mehr verwendet haben, können Sie die Anwendung entweder schließen oder sich vom AWS Access-Portal abmelden. Durch das Schließen der Anwendung werden Sie nur von dieser Anwendung abgemeldet. Alle anderen Anwendungen, die Sie über das AWS Access-Portal geöffnet haben, bleiben geöffnet und laufen weiter.

- Bevor Sie sich als ein anderer Benutzer anmelden können, müssen Sie sich zuerst vom AWS Access Portal abmelden. Durch das Abmelden vom Portal werden Ihre Anmeldeinformationen vollständig aus der Browsersitzung entfernt.
- Sobald Sie sich beim AWS Access-Portal angemeldet haben, können Sie zu einer Rolle wechseln. Durch einen vorübergehenden Rollenwechsel werden Ihre ursprünglichen Benutzerberechtigungen aufgehoben und Sie erhalten stattdessen die der Rolle zugewiesenen Berechtigungen. Weitere Informationen finden Sie unter Wechseln zu einer Rolle (Konsole).

Abmelden vom AWS Zugriffsportal

Wenn Sie sich vom Portal abmelden, werden Ihre Anmeldeinformationen vollständig aus der Browsersitzung entfernt. Weitere Informationen finden Sie im AWS-AnmeldungHandbuch unter Abmelden vom AWS Access-Portal.

So melden Sie sich vom AWS Access-Portal ab

- Wählen Sie im AWS Access-Portal in der Navigationsleiste Abmelden aus.

> **Note**
>
> Wenn Sie sich als ein anderer Benutzer anmelden möchten, müssen Sie sich zuerst vom AWS Access-Portal abmelden.

Ihr IAM Identity Center-Benutzerkennwort zurücksetzen

Das AWS Zugriffsportal bietet Benutzern von IAM Identity Center über ein Webportal Single Sign-On-Zugriff auf alle ihnen zugewiesenen AWS Konten und Cloud-Anwendungen. Das AWS Zugriffsportal unterscheidet sich von dem AWS Management Console, bei dem es sich um eine Sammlung von Servicekonsolen zur Verwaltung AWS von Ressourcen handelt.

Gehen Sie wie folgt vor, um Ihr IAM Identity Center-Benutzerkennwort für das AWS Zugriffsportal zurückzusetzen. Weitere Informationen zu Benutzertypen finden Sie im AWS-Anmeldung Benutzerhandbuch.

Überlegungen

Die Funktion zum Zurücksetzen Ihres Passworts für Ihr AWS Zugriffsportal ist nur für Benutzer von Identity Center-Instanzen verfügbar, die das Identity Center-Verzeichnis oder AWS Managed Microsoft ADals Identitätsquelle verwenden. Wenn Ihr Benutzer mit einem externen Identitätsanbieter oder AD Connector verbunden ist, müssen Benutzerpasswörter vom externen Identitätsanbieter oder über eine Verbindung Active Directory zurückgesetzt werden.

- Wenn es sich bei Ihrer Identitätsquelle um ein IAM Identity Center-Verzeichnis handelt, finden Sie weitere Informationen unter. Passwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center
- Wenn es sich bei Ihrer Identitätsquelle um eine handelt AWS Managed Microsoft AD, finden Sie weitere Informationen unter Kennwortanforderungen beim Zurücksetzen eines Kennworts in. AWS Managed Microsoft AD

So setzen Sie Ihr Passwort für das Zugangsportal zurück AWS

1. Öffnen Sie einen Webbrowser und rufen Sie die Anmeldeseite für Ihr AWS Zugangsportal auf.

   Wenn Sie Ihre AWS Access-Portal-URL nicht haben, überprüfen Sie Ihre E-Mails. Sie sollten per E-Mail eine Einladung zur Teilnahme AWS am IAM Identity Center erhalten haben, die eine bestimmte Anmelde-URL für das AWS Zugangsportal enthält. Alternativ hat Ihnen Ihr Administrator möglicherweise direkt ein Einmalpasswort und die URL des AWS Zugriffsportals zur Verfügung gestellt. Wenn Sie diese Informationen nicht finden können, bitten Sie Ihren Administrator, sie Ihnen zu senden.

   Weitere Informationen zur Anmeldung beim AWS Access-Portal finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmelden im AWS Access-Portal.
2. Geben Sie Ihren Benutzernamen ein und wählen Sie dann Weiter.
3. Wählen Sie unter Passwort die Option Passwort vergessen aus.

   Bestätigen Sie Ihren Benutzernamen und geben Sie die Zeichen für das bereitgestellte Bild ein, um zu bestätigen, dass Sie kein Roboter sind. Wählen Sie anschließend Weiter. Möglicherweise müssen Sie die Werbeblocker-Software deaktivieren, wenn Sie keine Zeichen eingeben können.
4. In einer Meldung wird bestätigt, dass eine E-Mail zum Zurücksetzen des Passworts gesendet wurde. Klicken Sie auf Weiter.
5. Sie erhalten eine E-Mail von `no-reply@signin.aws` mit dem Betreff Passwort zurücksetzen angefordert. Wählen Sie in Ihrer E-Mail die Option Passwort zurücksetzen aus.

6. Bestätigen Sie auf der Seite „Passwort zurücksetzen“ Ihren Benutzernamen, geben Sie ein neues Passwort für das AWS Zugangsportal ein und wählen Sie dann Neues Passwort einrichten aus.
7. Sie erhalten eine E-Mail von `no-reply@signin.aws` mit der Betreffzeile „Passwort aktualisiert“.

> **Note**
>
> Ein Administrator kann Ihr Passwort zurücksetzen, indem er Ihnen entweder eine E-Mail mit Anweisungen zum Zurücksetzen Ihres Passworts sendet oder ein Einmalpasswort generiert und es Ihnen mitteilt. Wenn Sie ein Administrator sind, finden Sie weitere Informationen unter. Setzen Sie das IAM Identity Center-Benutzerkennwort für einen Endbenutzer zurück

Abrufen der IAM Identity Center-Benutzeranmeldedaten für die AWS CLI oder SDKs AWS

Sie können programmgesteuert auf AWS Dienste zugreifen, indem Sie die AWS Command Line Interface oder AWS Software Development Kits (SDKs) mit Benutzeranmeldedaten von IAM Identity Center verwenden. In diesem Thema wird beschrieben, wie Sie temporäre Anmeldeinformationen für einen Benutzer in IAM Identity Center abrufen.

Das AWS Zugriffsportal bietet Benutzern von IAM Identity Center mit einmaliger Anmeldung Zugriff auf ihre AWS-Konten und Cloud-Anwendungen. Nachdem Sie sich als IAM Identity Center-Benutzer beim AWS Zugriffsportal angemeldet haben, können Sie temporäre Anmeldeinformationen erhalten. Sie können dann die Anmeldeinformationen, die auch als IAM Identity Center-Benutzeranmeldedaten bezeichnet werden, in den AWS CLI oder AWS SDKs verwenden, um auf Ressourcen in einem zuzugreifen. AWS-Konto

Wenn Sie den für den programmgesteuerten AWS CLI Zugriff auf AWS Dienste verwenden, können Sie die Verfahren in diesem Thema verwenden, um den Zugriff auf die zu initiieren. AWS CLI Informationen zu den AWS CLI finden Sie im AWS Command Line Interface Benutzerhandbuch.

Wenn Sie die AWS SDKs für den programmgesteuerten Zugriff auf AWS Dienste verwenden, wird durch das Befolgen der Verfahren in diesem Thema auch direkt die Authentifizierung für die SDKs eingerichtet. AWS Informationen zu den SDKs finden Sie im AWS Referenzhandbuch zu AWS SDKs und Tools.

> **Note**
>
> Benutzer in IAM Identity Center unterscheiden sich von IAM-Benutzern. IAM-Benutzern werden langfristige Anmeldeinformationen für Ressourcen gewährt. AWS Benutzern im IAM Identity Center werden temporäre Anmeldeinformationen gewährt. Wir empfehlen Ihnen, temporäre Anmeldeinformationen als bewährte Sicherheitsmethode für den Zugriff auf Ihre zu verwenden AWS-Konten , da diese Anmeldeinformationen bei jeder Anmeldung generiert werden.

Voraussetzungen

Um temporäre Anmeldeinformationen für Ihren IAM Identity Center-Benutzer zu erhalten, benötigen Sie Folgendes:

- Ein IAM Identity Center-Benutzer — Sie melden sich als dieser Benutzer beim AWS Zugriffsportal an. Sie oder Ihr Administrator können diesen Benutzer erstellen. Informationen zum Aktivieren von IAM Identity Center und zum Erstellen eines IAM Identity Center-Benutzers finden Sie unter. Erste Schritte mit allgemeinen Aufgaben in IAM Identity Center
- Benutzerzugriff auf AWS-Konto— Um einem IAM Identity Center-Benutzer die Erlaubnis zu erteilen, seine temporären Anmeldeinformationen abzurufen, müssen Sie oder ein Administrator den IAM Identity Center-Benutzer einem Berechtigungssatz zuweisen. Berechtigungssätze werden in IAM Identity Center gespeichert und definieren die Zugriffsebene, auf die ein IAM Identity Center-Benutzer Zugriff hat. AWS-Konto Wenn Ihr Administrator den IAM Identity Center-Benutzer für Sie erstellt hat, bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter Weisen Sie Benutzerzugriff zu AWS-Konten.
- AWS CLI installiert — Um die temporären Anmeldeinformationen zu verwenden, müssen Sie den AWS CLI installieren. Weitere Anweisungen finden Sie unter Installation oder Aktualisierung der aktuellen Version der AWS CLI im Benutzerhandbuch zu AWS CLI .

Überlegungen

Bevor Sie die Schritte zum Abrufen temporärer Anmeldeinformationen für Ihren IAM Identity Center-Benutzer ausführen, sollten Sie die folgenden Überlegungen berücksichtigen:

- IAM Identity Center erstellt IAM-Rollen — Wenn Sie einen Benutzer in IAM Identity Center einem Berechtigungssatz zuweisen, erstellt IAM Identity Center aus dem Berechtigungssatz eine

entsprechende IAM-Rolle. Durch Berechtigungssätze erstellte IAM-Rollen unterscheiden sich von IAM-Rollen, die auf folgende Weise erstellt wurden: AWS Identity and Access Management

- IAM Identity Center besitzt und schützt die Rollen, die durch Berechtigungssätze erstellt wurden. Nur IAM Identity Center kann diese Rollen ändern.
- Nur Benutzer in IAM Identity Center können die Rollen übernehmen, die ihren zugewiesenen Berechtigungssätzen entsprechen. Sie können IAM-Benutzern, IAM-Verbundbenutzern oder Dienstkonten keinen Zugriff auf Berechtigungssätze zuweisen.
- Sie können eine Rollenvertrauensrichtlinie für diese Rollen nicht ändern, um den Zugriff auf Prinzipale außerhalb von IAM Identity Center zu ermöglichen.

Informationen zum Abrufen temporärer Anmeldeinformationen für eine Rolle, die Sie in IAM erstellen, finden Sie unter Verwenden temporärer Sicherheitsanmeldedaten mit dem AWS CLIAWS Identity and Access Management im Benutzerhandbuch.

- Sie können die Sitzungsdauer für Berechtigungssätze festlegen. Nachdem Sie sich beim AWS Access Portal angemeldet haben, wird der Berechtigungssatz, dem Ihr IAM Identity Center-Benutzer zugewiesen ist, als verfügbare Rolle angezeigt. IAM Identity Center erstellt eine separate Sitzung für diese Rolle. Diese Sitzung kann je nach der für den Berechtigungssatz konfigurierten Sitzungsdauer zwischen einer und 12 Stunden dauern. Die Standardsitzungsdauer beträgt eine Stunde. Weitere Informationen finden Sie unter Legen Sie die Sitzungsdauer fest.

Temporäre Anmeldeinformationen abrufen und aktualisieren

Sie können temporäre Anmeldeinformationen für Ihren IAM Identity Center-Benutzer automatisch oder manuell abrufen und aktualisieren.

Themen

- Automatische Aktualisierung der Anmeldeinformationen (empfohlen)
- Manuelle Aktualisierung der Anmeldeinformationen

Automatische Aktualisierung der Anmeldeinformationen (empfohlen)

Die automatische Aktualisierung der Anmeldeinformationen verwendet den Gerätecode-Autorisierungsstandard Open ID Connect (OIDC). Mit dieser Methode initiieren Sie den Zugriff direkt, indem Sie den `aws configure sso` Befehl in der verwenden. AWS CLI Sie können diesen Befehl verwenden, um automatisch auf jede Rolle zuzugreifen, die einem beliebigen Berechtigungssatz zugeordnet ist, dem Sie für eine Rolle zugewiesen sind AWS-Konto.

Um auf die Rolle zuzugreifen, die für Ihren IAM Identity Center-Benutzer erstellt wurde, führen Sie den `aws configure sso` Befehl AWS CLI aus und autorisieren Sie ihn dann in einem Browserfenster. Solange Sie über eine aktive AWS Access-Portal-Sitzung verfügen, ruft das AWS CLI automatisch temporäre Anmeldeinformationen ab und aktualisiert die Anmeldeinformationen automatisch.

Weitere Informationen finden Sie unter Konfigurieren Ihres Profils mit dem `aws configure sso wizard` im AWS Command Line Interface Benutzerhandbuch.

Um temporäre Anmeldeinformationen zu erhalten, die automatisch aktualisiert werden

1. Melden Sie sich mit der spezifischen Anmelde-URL, die Sie von Ihrem Administrator erhalten haben, beim AWS Zugriffsportal an. Wenn Sie den IAM Identity Center-Benutzer erstellt haben, AWS haben Sie eine E-Mail-Einladung mit Ihrer Anmelde-URL gesendet. Weitere Informationen finden Sie unter Anmelden im AWS Access-Portal im AWS Anmelde-Benutzerhandbuch.
2. Suchen Sie auf der Registerkarte Konten nach dem Konto, AWS-Konto von dem Sie die Anmeldeinformationen abrufen möchten. Wenn Sie das Konto auswählen, werden der Kontoname, die Konto-ID und die E-Mail-Adresse angezeigt, die dem Konto zugeordnet sind.

   > **Note**
   >
   > Wenn Sie nichts in der AWS-KontenListe sehen, wurde Ihnen wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Wenden Sie sich in diesem Fall an Ihren Administrator und bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter Weisen Sie Benutzerzugriff zu AWS-Konten.

3. Unter dem Namen des Kontos wird der Berechtigungssatz, dem Ihr IAM Identity Center-Benutzer zugewiesen ist, als verfügbare Rolle angezeigt. Wenn Ihrem IAM Identity Center-Benutzer beispielsweise der PowerUserAccessBerechtigungssatz für das Konto zugewiesen ist, wird die Rolle im AWS Zugriffsportal als angezeigt. PowerUserAccess
4. Abhängig von Ihrer Option neben dem Rollennamen wählen Sie entweder Zugriffstasten oder Befehlszeilen- oder programmgesteuerten Zugriff.
5. Wählen Sie im Dialogfeld Anmeldeinformationen abrufen entweder macOS und Linux, Windows oder PowerShell, je nach dem Betriebssystem, auf dem Sie das installiert haben AWS CLI.
6. Unter AWS IAM Identity Center-Anmeldeinformationen (empfohlen) `SSO Region` werden Ihr `SSO Start URL` und angezeigt. Diese Werte sind erforderlich, um sowohl ein für IAM Identity Center aktiviertes Profil als auch für Ihr Profil `sso-session` zu konfigurieren. AWS CLI Um

diese Konfiguration abzuschließen, folgen Sie den Anweisungen unter Konfigurieren Sie Ihr Profil mit dem `aws configure sso wizard` im AWS Command Line Interface Benutzerhandbuch.

Verwenden Sie das AWS CLI so lange, wie es für Sie erforderlich ist, AWS-Konto bis die Anmeldeinformationen abgelaufen sind.

Manuelle Aktualisierung der Anmeldeinformationen

Sie können die Methode zur manuellen Aktualisierung von Anmeldeinformationen verwenden, um temporäre Anmeldeinformationen für eine Rolle abzurufen, die mit einem bestimmten Berechtigungssatz in einer bestimmten Rolle verknüpft ist. AWS-Konto Dazu kopieren Sie die erforderlichen Befehle für die temporären Anmeldeinformationen und fügen sie ein. Bei dieser Methode müssen Sie die temporären Anmeldeinformationen manuell aktualisieren.

Sie können AWS CLI Befehle ausführen, bis Ihre temporären Anmeldeinformationen ablaufen.

Um Anmeldeinformationen abzurufen, die Sie manuell aktualisieren

1. Melden Sie sich mit der spezifischen Anmelde-URL, die Sie von Ihrem Administrator erhalten haben, beim AWS Zugriffsportal an. Wenn Sie den IAM Identity Center-Benutzer erstellt haben, AWS haben Sie eine E-Mail-Einladung mit Ihrer Anmelde-URL gesendet. Weitere Informationen finden Sie unter Anmelden im AWS Access-Portal im AWS Anmelde-Benutzerhandbuch.
2. Suchen Sie auf der Registerkarte Konten die Datei, AWS-Konto von der Sie die Zugangsdaten abrufen möchten, und erweitern Sie sie, sodass der IAM-Rollenname angezeigt wird (z. B. Administrator). Abhängig von Ihrer Option neben dem IAM-Rollennamen wählen Sie entweder Zugriffstasten oder Befehlszeilen - oder programmgesteuerten Zugriff aus.

   > **Note**
   >
   > Wenn Sie keine Rechte in der AWS-KontenListe sehen, wurde Ihnen wahrscheinlich noch kein Berechtigungssatz für dieses Konto zugewiesen. Wenden Sie sich in diesem Fall an Ihren Administrator und bitten Sie ihn, diesen Zugriff für Sie hinzuzufügen. Weitere Informationen finden Sie unter Weisen Sie Benutzerzugriff zu AWS-Konten.

3. Wählen Sie im Dialogfeld Anmeldeinformationen abrufen die Option macOS und Linux, Windows oder PowerShell, je nachdem, auf welchem Betriebssystem Sie das installiert haben AWS CLI.
4. Wählen Sie eine der folgenden Optionen:

   - Option 1: Legen Sie AWS Umgebungsvariablen fest

Wählen Sie diese Option, um alle Anmeldeinformationseinstellungen zu überschreiben, einschließlich aller Einstellungen in den `credentials` Dateien und `config` Dateien. Weitere Informationen finden Sie unter Umgebungsvariablen zur Konfiguration von AWS CLI im AWS CLI Benutzerhandbuch.

Um diese Option zu verwenden, kopieren Sie die Befehle in die Zwischenablage, fügen Sie sie in Ihr AWS CLI Terminalfenster ein und drücken Sie dann die EINGABETASTE, um die erforderlichen Umgebungsvariablen festzulegen.

- Option 2: Fügen Sie Ihrer AWS Anmeldeinformationsdatei ein Profil hinzu

  Wählen Sie diese Option, um Befehle mit unterschiedlichen Anmeldeinformationen auszuführen.

  Um diese Option zu verwenden, kopieren Sie die Befehle in Ihre Zwischenablage und fügen Sie sie dann in Ihre gemeinsam genutzte AWS `credentials` Datei ein, um ein neues benanntes Profil einzurichten. Weitere Informationen finden Sie im Referenzhandbuch für AWS SDKs und Tools unter Dateien mit gemeinsam genutzten Konfigurationen und Anmeldeinformationen. Um diese Anmeldeinformationen zu verwenden, geben Sie die `--profile` Option in Ihrem AWS CLI Befehl an. Dies wirkt sich auf alle Umgebungen aus, die dieselbe Anmeldeinformationsdatei verwenden.

- Option 3: Verwenden Sie individuelle Werte in Ihrem AWS Service-Client

  Wählen Sie diese Option, um von einem AWS Service-Client aus auf AWS Ressourcen zuzugreifen. Weitere Informationen finden Sie unter Tools, auf denen Sie aufbauen können AWS.

  Um diese Option zu verwenden, kopieren Sie die Werte in Ihre Zwischenablage, fügen Sie die Werte in Ihren Code ein und weisen Sie sie den entsprechenden Variablen für Ihr SDK zu. Weitere Informationen finden Sie in der Dokumentation zu Ihrer spezifischen SDK-API.

Shortcut-Links zu AWS Management Console Zielen erstellen

Im AWS Zugriffsportal erstellte Shortcut-Links führen IAM Identity Center-Benutzer zu einem bestimmten Ziel in AWS Management Console, mit einem bestimmten Berechtigungssatz und in einem bestimmten. AWS-Konto

Shortcut-Links sparen Zeit für Sie und Ihre Mitarbeiter. Anstatt über mehrere Seiten, einschließlich des AWS Zugriffsportals, zu einer gewünschten Ziel-URL AWS Management Console (z. B. einer Amazon S3 S3-Bucket-Instance-Seite) zu navigieren, können Sie einen Shortcut-Link verwenden, um automatisch zum selben Ziel zu gelangen.

Zieloptionen für Shortcut-Links

Für Shortcut-Links gibt es drei Zieloptionen, die hier nach Priorität aufgelistet sind:

- (Optional) Jede Ziel-URL in der im Shortcut-Link AWS Management Console angegebenen URL. Zum Beispiel die Amazon S3 S3-Bucket-Instance-Seite.
- (Optional) Vom Administrator konfigurierte Relay-State-URL für den betreffenden Berechtigungssatz. Weitere Informationen zum Einstellen des Relay-Status finden Sie unter. Stellen Sie den Relay-Status ein
- AWS Management Console Zuhause. Das Standardziel, wenn Sie keins angeben.

> **Note**
>
> Die automatische Navigation zu einem Ziel ist nur erfolgreich, wenn Sie bei IAM Identity Center authentifiziert sind und Ihnen der erforderliche Berechtigungssatz für das AWS Konto und die Ziel-URL zugewiesen wurde.

Das AWS Zugriffsportal enthält eine Schaltfläche „Verknüpfung erstellen“, mit der Sie einen gemeinsam nutzbaren Shortcut-Link erstellen können. Wenn Sie eine Ziel-URL angeben möchten (die erste Option in der vorherigen Liste), können Sie die URL in eine Zwischenablage kopieren, um sie gemeinsam zu nutzen.

Erstellen Sie einen Shortcut-Link im AWS Access-Portal

1. Während Sie im AWS Access-Portal angemeldet sind, wählen Sie die Registerkarte Konten und dann die Schaltfläche Verknüpfung erstellen.
2. Im Dialogfeld:

    a. Wählen Sie eine aus, AWS-Konto indem Sie die Konto-ID oder den Kontonamen verwenden. Während der Eingabe werden in einem Drop-down-Menü passende Konto-IDs und Namen angezeigt, auf die Sie zugreifen können. Sie können nur ein Konto auswählen, auf das Sie Zugriff haben.

b. Wählen Sie optional eine IAM-Rolle aus der Dropdownliste aus. Dies sind die Berechtigungssätze, die Ihnen für das ausgewählte Konto zugewiesen wurden. Wenn Sie die Rolle nicht auswählen, werden Benutzer aufgefordert, eine Rolle auszuwählen, die ihnen für das gewählte Konto zugewiesen wurde, wenn sie den Shortcut-Link verwenden.

> **Note**
>
> Sie können keinen neuen Zugriff mit Shortcut-Links gewähren. Shortcut-Links funktionieren nur mit den Berechtigungssätzen, die dem Benutzer bereits zugewiesen wurden. Wenn dem Benutzer nicht die erforderlichen Berechtigungssätze für das Konto und die Ziel-URL zugewiesen wurden, wird ihm der Zugriff verweigert.

c. Geben Sie optional die Ziel-URL des AWS Access-Portals ein. Wenn Sie die Eingabe einer URL auslassen, wird das Ziel bei der Verwendung des Shortcut-Links automatisch anhand der zuvor genannten Zieloptionen für den Shortcut-Link bestimmt.

d. Ihr Shortcut-Link wird am unteren Rand des Dialogfelds auf der Grundlage Ihrer Eingabe generiert. Wählen Sie die Schaltfläche „URL kopieren“. Sie können jetzt ein Lesezeichen mit dem kopierten Kurzlink erstellen oder es mit Ihren Mitarbeitern teilen, die Zugriff auf dasselbe Konto mit demselben Berechtigungssatz oder einem anderen ausreichenden Berechtigungssatz haben.

Erstellung sicherer AWS Management Console Shortcut-Links mit URL-Kodierung

Alle Parameterwerte der URL, einschließlich der Konto-ID, des Namens des Berechtigungssatzes und der Ziel-URL, müssen URL-codiert sein.

Durch Shortcut-Links wird die URL des AWS Access-Portals um den folgenden Pfad erweitert:

```
/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Die vollständige URL in der klassischen AWS Partition folgt diesem Muster:

```
https://[your_subdomain].awsapps.com/start/#/console?
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination
```

Im Folgenden finden Sie ein Beispiel für einen Shortcut-Link, der einen Benutzer `123456789012` mit dem entsprechenden `S3FullAccess` Berechtigungssatz als Konto anmeldet und ihn zur Startseite der S3-Konsole weiterleitet:

- `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Ein Gerät für MFA registrieren

Verwenden Sie das folgende Verfahren im AWS Zugangsportal, um Ihr neues Gerät für die Multi-Faktor-Authentifizierung (MFA) zu registrieren.

> **Note**
>
> Wir empfehlen, dass Sie zuerst die entsprechende Authenticator-App auf Ihr Gerät herunterladen, bevor Sie mit den Schritten in diesem Verfahren beginnen. Eine Liste der Apps, die Sie für MFA-Geräte verwenden können, finden Sie unterApps für virtuelle Authentifikatoren.

Um Ihr Gerät für die Verwendung mit MFA zu registrieren

1. Melden Sie sich bei Ihrem AWS Zugangsportal an. Weitere Informationen finden Sie unter Melden Sie sich beim AWS Access-Portal an.
2. Wählen Sie oben rechts auf der Seite die Option MFA-Geräte aus.
3. Wählen Sie auf der Seite Multi-Factor Authentication (MFA) -Geräte die Option Gerät registrieren aus.

   > **Note**
   >
   > Wenn die Option MFA-Gerät registrieren ausgegraut ist, wenden Sie sich an Ihren Administrator, um Unterstützung bei der Registrierung Ihres Geräts zu erhalten.

4. Wählen Sie auf der Seite MFA-Gerät registrieren einen der folgenden MFA-Gerätetypen aus und folgen Sie den Anweisungen:

   - Authenticator-App

     1. Auf der Seite Authentifikator-App einrichten finden Sie möglicherweise Konfigurationsinformationen für das neue MFA-Gerät, einschließlich einer QR-Code-Grafik. Die Grafik ist eine Darstellung des geheimen Schlüssels, der für die manuelle Eingabe auf Geräten verfügbar ist, die QR-Codes nicht unterstützen.
     2. Gehen Sie mit dem physischen MFA-Gerät wie folgt vor:
        a. Öffnen Sie eine kompatible MFA-Authenticator-App. Eine Liste der getesteten Apps, die Sie mit MFA-Geräten verwenden können, finden Sie unterApps für virtuelle Authentifikatoren. Wenn die MFA-App mehrere Konten (mehrere MFA-Geräte) unterstützt, wählen Sie die Option zum Erstellen eines neuen Kontos (ein neues MFA-Gerät).
        b. Stellen Sie fest, ob die MFA-App QR-Codes unterstützt, und führen Sie dann auf der Seite Authenticator-App einrichten einen der folgenden Schritte aus:
           i. Wählen Sie Show QR code (QR-Code anzeigen) und verwenden Sie anschließend die App, um den QR-Code zu scannen. Sie können beispielsweise das Kamerasymbol oder eine ähnliche Option wie Scan code (Code scannen) auswählen. Verwenden Sie anschließend die Kamera des Geräts, um den Code zu scannen.
           ii. Wählen Sie Geheimen Schlüssel anzeigen und geben Sie dann diesen geheimen Schlüssel in Ihre MFA-App ein.

              > **Important**
              >
              > Wenn Sie ein MFA-Gerät für IAM Identity Center konfigurieren, empfehlen wir Ihnen, eine Kopie des QR-Codes oder geheimen Schlüssels an einem sicheren Ort aufzubewahren. Dies kann helfen, wenn Sie das Telefon verlieren oder die MFA-Authentifikator-App neu installieren müssen. Wenn eines dieser Dinge eintritt, können Sie die App schnell neu konfigurieren, um dieselbe MFA-Konfiguration zu verwenden.

     3. Geben Sie auf der Seite Authenticator-App einrichten unter Authenticator-Code das Einmalpasswort ein, das derzeit auf dem physischen MFA-Gerät angezeigt wird.

> **Important**
>
> Senden Sie die Anforderung direkt nach der Erzeugung der Codes. Wenn Sie den Code generieren und dann zu lange warten, um die Anfrage einzureichen, wurde das MFA-Gerät erfolgreich mit Ihrem Benutzer verknüpft, aber das MFA-Gerät ist nicht synchronisiert. Dies liegt daran, weil die zeitgesteuerten Einmalpasswörter (TOTP) nach einer kurzen Zeit ungültig werden. In diesem Fall können Sie das Gerät erneut synchronisieren.

4. Klicken Sie auf Assign MFA (MFA zuordnen). Das MFA-Gerät kann jetzt mit der Generierung von Einmalkennwörtern beginnen und ist jetzt für die Verwendung mit AWS bereit.

- Sicherheitsschlüssel oder integrierter Authentifikator

  1. Folgen Sie auf der Seite Sicherheitsschlüssel Ihres Benutzers registrieren den Anweisungen Ihres Browsers oder Ihrer Plattform.

     > **Note**
     >
     > Die Benutzererfahrung variiert je nach Browser oder Plattform. Nachdem Ihr Gerät erfolgreich registriert wurde, können Sie Ihrem neu registrierten Gerät einen benutzerfreundlichen Anzeigenamen zuordnen. Um den Namen zu ändern, wählen Sie „Umbenennen“, geben Sie den neuen Namen ein und wählen Sie dann „Speichern“.

Anpassen der URL des AWS Access-Portals

Standardmäßig können Sie auf das Access-Portal AWS zugreifen, indem Sie eine URL verwenden, die diesem Format folgt:`d-`*`xxxxxxxxxx`*`.awsapps.com/start`. Sie können die URL wie folgt anpassen:*`your_subdomain`*`.awsapps.com/start`.

> **Important**
>
> Wenn Sie die URL des AWS Access-Portals ändern, können Sie sie später nicht bearbeiten.

Um Ihre URL anzupassen

1. Öffnen Sie die AWS IAM Identity Center Konsole unter https://console.aws.amazon.com/singlesignon/.
2. Wählen Sie in der IAM Identity Center-Konsole im Navigationsbereich Dashboard aus und suchen Sie den Abschnitt mit der Zusammenfassung der Einstellungen.
3. Klicken Sie unter der URL Ihres AWS Zugriffsportals auf die Schaltfläche Anpassen.

> **Note**
>
> Wenn die Schaltfläche Anpassen nicht angezeigt wird, bedeutet dies, dass das AWS Zugangsportal bereits angepasst wurde. Das Anpassen der URL des AWS Access-Portals ist ein einmaliger Vorgang, der nicht rückgängig gemacht werden kann.

4. Geben Sie den gewünschten Subdomainnamen ein und wählen Sie Speichern.

Sie können sich jetzt über Ihr AWS Zugangsportal mit Ihrer benutzerdefinierten URL bei der AWS Konsole anmelden.

Multi-Faktor-Authentifizierung für Identity Center-Benutzer

Die Multi-Faktor-Authentifizierung (MFA) bietet eine einfache und sichere Möglichkeit, zusätzlich zum Standardauthentifizierungsmechanismus mit Benutzername und Passwort eine zusätzliche Schutzebene hinzuzufügen.

Wenn Administratoren MFA aktivieren, müssen sich Benutzer anhand von zwei Faktoren beim AWS Access Portal anmelden:

- Ihr Benutzername und Passwort. Dies ist der erste Faktor und ist etwas, das die Benutzer wissen.
- Entweder ein Code, ein Sicherheitsschlüssel oder Biometrie. Dies ist der zweite Faktor und ist etwas, das Benutzer besitzen (besitzen) oder sind (biometrisch). Der zweite Faktor kann entweder ein von ihrem Mobilgerät generierter Authentifizierungscode, ein mit ihrem Computer verbundener Sicherheitsschlüssel oder ein biometrischer Scan des Benutzers sein.

Zusammen sorgen diese verschiedenen Faktoren für mehr Sicherheit, indem sie unbefugten Zugriff auf Ihre AWS Ressourcen verhindern, es sei denn, eine gültige MFA-Anfrage wurde erfolgreich abgeschlossen.

Jeder Benutzer kann bis zu zwei virtuelle Authentifikator-Apps registrieren, bei denen es sich um Einmalpasswortauthentifizierungsanwendungen handelt, die auf Ihrem Mobilgerät oder Tablet installiert sind, sowie sechs FIDO-Authentifikatoren, die integrierte Authentifikatoren und Sicherheitsschlüssel enthalten, für insgesamt acht MFA-Geräte. Weitere Informationen zu Verfügbare MFA-Typen für IAM Identity Center.

> **Important**
>
> Aus Sicherheitsgründen empfehlen wir dringend, MFA zu aktivieren.

Themen

Verfügbare MFA-Typen für IAM Identity Center

Die Multi-Faktor-Authentifizierung (MFA) ist ein einfacher und effektiver Mechanismus, um die Sicherheit Ihrer Benutzer zu erhöhen. Der erste Faktor eines Benutzers — sein Passwort — ist ein Geheimnis, das er sich merkt, auch Wissensfaktor genannt. Andere Faktoren können Besitzfaktoren (etwas, das Sie besitzen, z. B. ein Sicherheitsschlüssel) oder Inhärenzfaktoren (etwas, das Sie sind, z. B. ein biometrischer Scan) sein. Wir empfehlen dringend, MFA zu konfigurieren, um Ihrem Konto eine zusätzliche Sicherheitsebene hinzuzufügen.

IAM Identity Center MFA unterstützt die folgenden Gerätetypen. Alle MFA-Typen werden sowohl für den browserbasierten Konsolenzugriff als auch für die Verwendung der AWS CLI Version v2 mit IAM Identity Center unterstützt.

- FIDO2-Authentifikatoren, einschließlich integrierter Authentifikatoren und Sicherheitsschlüssel
- Apps für virtuelle Authentifikatoren
- Ihre eigene RADIUS MFA Implementierung ist verbunden durch AWS Managed Microsoft AD

Ein Benutzer kann bis zu acht MFA-Geräte, darunter bis zu zwei virtuelle Authentifikator-Apps und sechs FIDO-Authentifikatoren, für ein Konto registrieren. Sie können die MFA-Aktivierungseinstellungen auch so konfigurieren, dass bei jeder Anmeldung Ihrer Benutzer MFA

erforderlich ist, oder dass vertrauenswürdige Geräte aktiviert werden, für die MFA nicht bei jeder Anmeldung erforderlich ist. Weitere Informationen zur Konfiguration von MFA-Typen für Ihre Benutzer finden Sie unter Wählen Sie MFA-Typen undMFA-Gerätedurchsetzung konfigurieren.

FIDO2-Authentifikatoren

FIDO2 ist ein Standard, der CTAP2 beinhaltet WebAuthnund auf der Kryptografie mit öffentlichen Schlüsseln basiert. FIDO-Anmeldeinformationen sind Phishing-resistent, da sie nur für die Website gelten, auf der die Anmeldeinformationen erstellt wurden, z. B. AWS

AWSunterstützt die beiden gängigsten Formfaktoren für FIDO-Authentifikatoren: integrierte Authentifikatoren und Sicherheitsschlüssel. Im Folgenden finden Sie weitere Informationen zu den gängigsten Arten von FIDO-Authentifikatoren.

Themen

- Integrierte Authentifikatoren
- Sicherheitsschlüssel
- Passwort-Manager, Passkey-Anbieter und andere FIDO-Authentifikatoren

Integrierte Authentifikatoren

Viele moderne Computer und Mobiltelefone verfügen über integrierte Authentifikatoren, z. B. TouchID auf einem Macbook oder eine Windows Hello-kompatible Kamera. Wenn Ihr Gerät über einen integrierten FIDO-kompatiblen Authentifikator verfügt, können Sie Ihren Fingerabdruck, Ihr Gesicht oder Ihre Geräte-PIN als zweiten Faktor verwenden.

Sicherheitsschlüssel

Sicherheitsschlüssel sind FIDO-kompatible externe Hardware-Authentifikatoren, die Sie erwerben und über USB, BLE oder NFC mit Ihrem Gerät verbinden können. Wenn Sie zur Eingabe von MFA aufgefordert werden, führen Sie einfach eine Geste mit dem Sensor der Taste aus. Zu den Sicherheitsschlüsseln gehören beispielsweise Feitian-Schlüssel, YubiKeys und mit den gängigsten Sicherheitsschlüsseln werden gerätegebundene FIDO-Anmeldeinformationen erstellt. Eine Liste aller FIDO-zertifizierten Sicherheitsschlüssel finden Sie unter FIDO-zertifizierte Produkte.

Passwort-Manager, Passkey-Anbieter und andere FIDO-Authentifikatoren

Zahlreiche Drittanbieter unterstützen die FIDO-Authentifizierung in mobilen Anwendungen, z. B. in Passwort-Managern, Smartcards mit FIDO-Modus und anderen Formfaktoren. Diese FIDO-

kompatiblen Geräte können mit IAM Identity Center verwendet werden. Wir empfehlen jedoch, dass Sie einen FIDO-Authentifikator selbst testen, bevor Sie diese Option für MFA aktivieren.

> **Note**
>
> Einige FIDO-Authentifikatoren können auffindbare FIDO-Anmeldeinformationen, sogenannte Hauptschlüssel, erstellen. Hauptschlüssel können an das Gerät gebunden sein, das sie erstellt, oder sie können synchronisiert und in einer Cloud gesichert werden. Sie können beispielsweise einen Hauptschlüssel mit der Apple Touch ID auf einem unterstützten Macbook registrieren und sich dann von einem Windows-Laptop aus mithilfe von Google Chrome mit Ihrem Hauptschlüssel in iCloud bei einer Website anmelden, indem Sie bei der Anmeldung den Anweisungen auf dem Bildschirm folgen. Weitere Informationen darüber, welche Geräte synchronisierbare Hauptschlüssel und die aktuelle Passkey-Interoperabilität zwischen Betriebssystemen und Browsern Support, finden Sie unter Geräteunterstützung auf passkeys.dev, einer Ressource, die vom FIDO Alliance And World Wide Web Consortium (W3C) verwaltet wird.

Apps für virtuelle Authentifikatoren

Bei Authenticator-Apps handelt es sich im Wesentlichen um Authentifikatoren von Drittanbietern, die auf Einmalkennwörtern (OTP) basieren. Sie können eine auf Ihrem Mobilgerät oder Tablet installierte Authentifizierungsanwendung als autorisiertes MFA-Gerät verwenden. Die Authentifizierungs-App eines Drittanbieters muss mit RFC 6238 konform sein. Dabei handelt es sich um einen standardbasierten Algorithmus für zeitgesteuerte Einmalpasswörter (TOTP), der sechsstellige Authentifizierungscodes erzeugen kann.

Wenn Benutzer zur Eingabe von MFA aufgefordert werden, müssen sie einen gültigen Code aus ihrer Authenticator-App in das angezeigte Eingabefeld eingeben. Jedes MFA-Gerät, das einem Benutzer zugeordnet ist, muss eindeutig sein. Für jeden Benutzer können zwei Authentifizierungs-Apps registriert werden.

Getestete Authenticator-Apps

Jede TOTP-konforme Anwendung funktioniert mit IAM Identity Center MFA. In der folgenden Tabelle sind bekannte Authentifikator-Apps von Drittanbietern aufgeführt, aus denen Sie wählen können.

Betriebssystem	Getestete Authentifizierungs-App
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

Der Remote Authentication Dial-In User Service (RADIUS) ist ein branchenübliches Client-Server-Protokoll, das Authentifizierung, Autorisierung und Kontoverwaltung ermöglicht, sodass Benutzer eine Verbindung zu Netzwerkdiensten herstellen können. AWS Directory Servicebeinhaltet einen RADIUS-Client, der eine Verbindung zu dem RADIUS-Server herstellt, auf dem Sie Ihre MFA-Lösung implementiert haben. Weitere Informationen finden Sie unter Aktivieren der Multi-Faktor-Authentifizierung für. AWS Managed Microsoft AD

Sie können entweder RADIUS MFA oder MFA in IAM Identity Center für Benutzeranmeldungen am Benutzerportal verwenden, aber nicht beide. MFA in IAM Identity Center ist eine Alternative zu RADIUS MFA in Fällen, in denen Sie eine AWS native Zwei-Faktor-Authentifizierung für den Zugriff auf das Portal wünschen.

Wenn Sie MFA in IAM Identity Center aktivieren, benötigen Ihre Benutzer ein MFA-Gerät, um sich beim Access Portal anzumelden. AWS Wenn Sie zuvor RADIUS MFA verwendet haben, überschreibt die Aktivierung von MFA in IAM Identity Center RADIUS MFA für Benutzer, die sich beim Access Portal anmelden. AWS RADIUS MFA stellt Benutzer jedoch weiterhin vor Herausforderungen, wenn sie sich bei allen anderen Anwendungen anmelden, die mit arbeitenAWS Directory Service, z. B. Amazon WorkDocs.

Wenn Ihr MFA auf der IAM Identity Center-Konsole deaktiviert ist und Sie RADIUS MFA mit konfiguriert habenAWS Directory Service, regelt AWS RADIUS MFA die Anmeldung am Access Portal. Das bedeutet, dass IAM Identity Center auf die RADIUS-MFA-Konfiguration zurückgreift, wenn MFA deaktiviert ist.

MFA konfigurieren

Die folgenden Themen enthalten Anweisungen zur Konfiguration von MFA-Geräten in IAM Identity Center.

Themen

Überlegungen vor der Aktivierung von MFA in IAM Identity Center

Bevor Sie MFA aktivieren, sollten Sie Folgendes beachten:

- Benutzern wird empfohlen, mehrere Backup-Authentifikatoren für alle aktivierten MFA-Typen zu registrieren. Diese Vorgehensweise kann verhindern, dass der Zugriff verloren geht, falls ein MFA-Gerät defekt oder falsch platziert ist.
- Wählen Sie nicht die Option Per E-Mail zugesandtes Einmalpasswort verlangen, wenn sich Ihre Benutzer beim AWS Zugriffsportal anmelden müssen, um auf ihre E-Mails zuzugreifen. Beispielsweise könnten Ihre Benutzer das AWS Access Portal verwendenMicrosoft 365, um ihre E-Mails zu lesen. In diesem Fall können Benutzer den Bestätigungscode nicht abrufen und sich nicht beim AWS Access-Portal anmelden. Weitere Informationen finden Sie unter MFA-Gerätedurchsetzung konfigurieren.
- Wenn Sie bereits RADIUS MFA verwenden, mit dem Sie konfiguriert habenAWS Directory Service, müssen Sie MFA nicht in IAM Identity Center aktivieren. MFA in IAM Identity Center ist eine Alternative zu RADIUS MFA für Microsoft Active Directory Benutzer von IAM Identity Center. Weitere Informationen finden Sie unter RADIUS MFA.
- Sie können MFA-Funktionen in IAM Identity Center verwenden, wenn Ihre Identitätsquelle mit dem Identitätsspeicher oder AD Connector von IAM Identity Center konfiguriert ist. AWS Managed Microsoft AD MFA in IAM Identity Center wird derzeit nicht für externe Identitätsanbieter unterstützt.

MFA im IAM Identity Center aktivieren

Sie können den sicheren Zugriff auf das AWS Zugriffsportal, die integrierten Apps AWS CLI von IAM Identity Center und die Aktivierung der Multi-Faktor-Authentifizierung (MFA) aktivieren.

Themen

- Deaktivieren Sie MFA für Ihr IAM Identity Center-Verzeichnis

Benutzer zur MFA auffordern

Gehen Sie wie folgt vor, um MFA in der IAM Identity Center-Konsole zu aktivieren. Bevor Sie beginnen, empfehlen wir Ihnen, die zu verstehen. Verfügbare MFA-Typen für IAM Identity Center

> **Note**
>
> Wenn Sie einen externen IdP verwenden, ist der Bereich Multi-Faktor-Authentifizierung nicht verfügbar. Ihr externer IdP verwaltet die MFA-Einstellungen, nicht IAM Identity Center.

Um MFA zu aktivieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Benutzer zur MFA auffordern je nach Sicherheitsstufe, die Ihr Unternehmen benötigt, einen der folgenden Authentifizierungsmodi aus:

   - Nur wenn sich ihr Anmeldekontext ändert (kontextsensitiv)

     In diesem Modus (Standard) bietet IAM Identity Center Benutzern die Möglichkeit, ihrem Gerät bei der Anmeldung zu vertrauen. Nachdem ein Benutzer angegeben hat, dass er einem Gerät vertrauen möchte, fordert IAM Identity Center den Benutzer einmal zur Eingabe von MFA auf und analysiert den Anmeldekontext (wie Gerät, Browser und Standort) für die nachfolgenden Anmeldungen des Benutzers. Bei nachfolgenden Anmeldungen ermittelt IAM Identity Center, ob sich der Benutzer mit einem zuvor vertrauenswürdigen Kontext anmeldet. Wenn sich der Anmeldekontext des Benutzers ändert, fordert IAM Identity Center den Benutzer zusätzlich zu seiner E-Mail-Adresse und seinen Kennwortanmeldeinformationen zur Eingabe von MFA auf.

     Dieser Modus bietet Benutzern, die sich häufig von ihrem Arbeitsplatz aus anmelden, eine einfache Bedienung, sodass sie nicht bei jeder Anmeldung die MFA abschließen müssen. Sie werden nur dann zur Eingabe von MFA aufgefordert, wenn sich ihr Anmeldekontext ändert.

- Jedes Mal, wenn sie sich anmelden (immer aktiv)

  In diesem Modus verlangt IAM Identity Center, dass Benutzer mit einem registrierten MFA-Gerät bei jeder Anmeldung dazu aufgefordert werden. Sie sollten diesen Modus verwenden, wenn Sie Organisations- oder Compliance-Richtlinien haben, nach denen Ihre Benutzer bei jeder Anmeldung am AWS Access Portal die MFA abschließen müssen. PCI DSS empfiehlt beispielsweise nachdrücklich, bei jeder Anmeldung MFA zu verwenden, um auf Anwendungen zuzugreifen, die Zahlungsvorgänge mit hohem Risiko unterstützen.

- Niemals (deaktiviert)

  In diesem Modus melden sich alle Benutzer nur mit ihrem Standardbenutzernamen und Passwort an. Wenn Sie diese Option wählen, wird IAM Identity Center MFA deaktiviert.

  > **Note**
  >
  > Wenn Sie RADIUS MFA bereits mit verwenden und es weiterhin als Standard-MFA-Typ verwenden möchtenAWS Directory Service, können Sie den Authentifizierungsmodus deaktiviert lassen, um die MFA-Funktionen in IAM Identity Center zu umgehen. Wenn Sie vom deaktivierten Modus in den kontextsensitiven oder Always-On-Modus wechseln, werden die vorhandenen RADIUS-MFA-Einstellungen außer Kraft gesetzt. Weitere Informationen finden Sie unter RADIUS MFA.

6. Wählen Sie Save Changes.

   Verwandte Themen

   - Wählen Sie MFA-Typen
   - MFA-Gerätedurchsetzung konfigurieren
   - Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren

Deaktivieren Sie MFA für Ihr IAM Identity Center-Verzeichnis

Wenn Sie die Multi-Faktor-Authentifizierung (MFA) für Ihr IAM Identity Center-Verzeichnis deaktivieren, können sich Benutzer nur mit ihrem Standardbenutzernamen und Passwort anmelden. MFA ist zwar für Ihr Identity Center-Verzeichnis für Benutzer deaktiviert, aber Sie können MFA-Geräte nicht in ihren Benutzerdetails verwalten, und Identity Center-Verzeichnisbenutzer können MFA-Geräte nicht über das AWS Zugriffsportal verwalten.

So deaktivieren Sie MFA für Ihr IAM Identity Center-Verzeichnis

> **Important**
>
> Die Anweisungen in diesem Abschnitt gelten für. AWS IAM Identity Center Sie gelten nicht für AWS Identity and Access Management(IAM). IAM Identity Center-Benutzer, -Gruppen und -Benutzeranmeldedaten unterscheiden sich von IAM-Benutzern, -Gruppen und IAM-Benutzeranmeldedaten. Anweisungen zur Deaktivierung von MFA für IAM-Benutzer finden Sie im Benutzerhandbuch unter Deaktivierung von MFA-Geräten. AWS Identity and Access Management

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren im Abschnitt Benutzer zur MFA auffordern das Optionsfeld Nie (deaktiviert) aus.
6. Wählen Sie Änderungen speichern aus.

Wählen Sie MFA-Typen

Gehen Sie wie folgt vor, um die Gerätetypen auszuwählen, mit denen sich Ihre Benutzer authentifizieren können, wenn sie im AWS Access Portal zur Eingabe von MFA aufgefordert werden.

So konfigurieren Sie MFA-Typen für Ihre Benutzer

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Benutzer können sich mit diesen MFA-Typen authentifizieren je nach Ihren Geschäftsanforderungen einen der folgenden MFA-Typen aus. Weitere Informationen finden Sie unter Verfügbare MFA-Typen für IAM Identity Center.

- FIDO2-Authentifikatoren, einschließlich integrierter Authentifikatoren und Sicherheitsschlüssel
- Apps für virtuelle Authentifikatoren

6. Wählen Sie Änderungen speichern aus.

MFA-Gerätedurchsetzung konfigurieren

Gehen Sie wie folgt vor, um zu ermitteln, ob Ihre Benutzer bei der Anmeldung am AWS Access Portal über ein registriertes MFA-Gerät verfügen müssen.

So konfigurieren Sie die MFA-Gerätedurchsetzung für Ihre Benutzer

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Falls ein Benutzer noch kein registriertes MFA-Gerät besitzt, je nach Ihren Geschäftsanforderungen eine der folgenden Optionen aus:

   - Fordere sie auf, bei der Anmeldung ein MFA-Gerät zu registrieren

     Dies ist die Standardeinstellung, wenn Sie MFA für IAM Identity Center zum ersten Mal konfigurieren. Verwenden Sie diese Option, wenn Sie festlegen möchten, dass Benutzer, die noch kein registriertes MFA-Gerät haben, ein Gerät bei der Anmeldung nach erfolgreicher Passwortauthentifizierung selbst registrieren müssen. Auf diese Weise können Sie die AWS Umgebungen Ihres Unternehmens mit MFA schützen, ohne Authentifizierungsgeräte einzeln registrieren und an Ihre Benutzer verteilen zu müssen. Während der Selbstregistrierung können Ihre Benutzer jedes Gerät aus den verfügbaren Verfügbare MFA-Typen für IAM Identity Center Geräten registrieren, die Sie zuvor aktiviert haben. Nach Abschluss der Registrierung haben Benutzer die Möglichkeit, ihrem neu registrierten MFA-Gerät einen benutzerfreundlichen Namen zu geben. Danach leitet IAM Identity Center den Benutzer zu seinem ursprünglichen Ziel weiter. Wenn das Gerät des Benutzers verloren geht oder gestohlen wird, können Sie dieses Gerät einfach aus seinem Konto entfernen. IAM Identity Center fordert ihn dann auf, ein neues Gerät bei der nächsten Anmeldung selbst zu registrieren.
   - Fordere sie auf, ein Einmalpasswort per E-Mail einzugeben, um sich anzumelden

Verwenden Sie diese Option, wenn Sie Benutzern Bestätigungscodes per E-Mail zusenden möchten. Da E-Mails nicht an ein bestimmtes Gerät gebunden sind, erfüllt diese Option nicht die Anforderungen für die branchenübliche Multi-Faktor-Authentifizierung. Sie verbessert jedoch die Sicherheit gegenüber der alleinigen Verwendung eines Kennworts. Eine E-Mail-Bestätigung wird nur angefordert, wenn ein Benutzer kein MFA-Gerät registriert hat. Wenn die kontextsensitive Authentifizierungsmethode aktiviert wurde, hat der Benutzer die Möglichkeit, das Gerät, auf dem er die E-Mail erhält, als vertrauenswürdig zu markieren. Danach müssen sie bei future Anmeldungen von dieser Kombination aus Gerät, Browser und IP-Adresse keinen E-Mail-Code mehr verifizieren.

> **Note**
>
> Wenn Sie Active Directory als Ihre IAM Identity Center-fähige Identitätsquelle verwenden, basiert die E-Mail-Adresse immer auf dem Active Directory-Attribut. `email` Durch benutzerdefinierte Active Directory-Attributzuordnungen wird dieses Verhalten nicht außer Kraft gesetzt.

- Blockieren Sie ihre Anmeldung

  Verwenden Sie die Option „Ihre Anmeldung blockieren“, wenn Sie die Verwendung von MFA durch alle Benutzer erzwingen möchten, bevor sie sich anmelden können. AWS

  > **Important**
  >
  > Wenn Ihre Authentifizierungsmethode auf Kontextsensitiv eingestellt ist, kann ein Benutzer auf der Anmeldeseite das Kontrollkästchen Dies ist ein vertrauenswürdiges Gerät aktivieren. In diesem Fall wird dieser Benutzer nicht zur Eingabe von MFA aufgefordert, auch wenn Sie die Einstellung Anmeldung blockieren aktiviert haben. Wenn Sie möchten, dass diese Benutzer dazu aufgefordert werden, ändern Sie Ihre Authentifizierungsmethode auf Immer aktiviert.

- Erlauben Sie ihnen, sich anzumelden

  Verwenden Sie diese Option, um anzugeben, dass keine MFA-Geräte erforderlich sind, damit sich Ihre Benutzer beim AWS Access Portal anmelden können. Benutzer, die sich für die Registrierung von MFA-Geräten entschieden haben, werden weiterhin zur Eingabe von MFA aufgefordert.

6. Wählen Sie Änderungen speichern aus.

Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren

Gehen Sie wie folgt vor, damit Ihre Benutzer ihre eigenen MFA-Geräte selbst registrieren können.

Um Benutzern die Registrierung ihrer eigenen MFA-Geräte zu ermöglichen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie im Abschnitt Multi-Faktor-Authentifizierung die Option Konfigurieren aus.
5. Wählen Sie auf der Seite Multi-Faktor-Authentifizierung konfigurieren unter Wer kann MFA-Geräte verwalten die Option Benutzer können ihre eigenen MFA-Geräte hinzufügen und verwalten aus.
6. Wählen Sie Änderungen speichern aus.

> **Note**
>
> Nachdem Sie die Selbstregistrierung für Ihre Benutzer eingerichtet haben, möchten Sie ihnen möglicherweise einen Link zum Verfahren senden. Ein Gerät für MFA registrieren Dieses Thema enthält Anweisungen zum Einrichten ihrer eigenen MFA-Geräte.

MFA-Geräte im IAM Identity Center verwalten

Die folgenden Themen enthalten Anweisungen zur Verwaltung von MFA-Geräten in IAM Identity Center.

Themen

- Ein MFA-Gerät registrieren
- Das MFA-Gerät eines Benutzers verwalten

Ein MFA-Gerät registrieren

Gehen Sie wie folgt vor, um ein neues MFA-Gerät für den Zugriff durch einen bestimmten Benutzer in der IAM Identity Center-Konsole einzurichten. Sie müssen physischen Zugriff auf das MFA-Gerät des Benutzers haben, um es registrieren zu können. Wenn Sie beispielsweise MFA für einen Benutzer konfigurieren, der ein MFA-Gerät verwendet, das auf einem Smartphone ausgeführt wird, benötigen Sie physischen Zugriff auf das Smartphone, um den Registrierungsprozess abzuschließen. Alternativ können Sie Benutzern ermöglichen, ihre eigenen MFA-Geräte zu konfigurieren und zu verwalten. Weitere Informationen finden Sie unter Erlauben Sie Benutzern, ihre eigenen MFA-Geräte zu registrieren.

Um ein MFA-Gerät zu registrieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie einen Benutzer in der Liste aus. Markieren Sie für diesen Schritt nicht das Kontrollkästchen neben dem Benutzer.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte und dann MFA-Gerät registrieren aus.
4. Wählen Sie auf der Seite MFA-Gerät registrieren einen der folgenden MFA-Gerätetypen aus und folgen Sie den Anweisungen:

   - Authenticator-App

     1. Auf der Seite Authentifikator-App einrichten zeigt IAM Identity Center Konfigurationsinformationen für das neue MFA-Gerät an, einschließlich einer QR-Code-Grafik. Die Grafik ist eine Darstellung des geheimen Schlüssels, der für die manuelle Eingabe auf Geräten verfügbar ist, die QR-Codes nicht unterstützen.
     2. Gehen Sie mit dem physischen MFA-Gerät wie folgt vor:

        a. Öffnen Sie eine kompatible MFA-Authenticator-App. Eine Liste der getesteten Apps, die Sie mit MFA-Geräten verwenden können, finden Sie unterApps für virtuelle Authentifikatoren. Wenn die MFA-App mehrere Konten (mehrere MFA-Geräte) unterstützt, wählen Sie die Option zum Erstellen eines neuen Kontos (ein neues MFA-Gerät).

        b. Stellen Sie fest, ob die MFA-App QR-Codes unterstützt, und führen Sie dann auf der Seite Authenticator-App einrichten einen der folgenden Schritte aus:

           i. Wählen Sie Show QR code (QR-Code anzeigen) und verwenden Sie anschließend die App, um den QR-Code zu scannen. Sie können beispielsweise das Kamerasymbol

oder eine ähnliche Option wie Scan code (Code scannen) auswählen. Verwenden Sie anschließend die Kamera des Geräts, um den Code zu scannen.

ii. Wählen Sie Geheimen Schlüssel anzeigen und geben Sie dann diesen geheimen Schlüssel in Ihre MFA-App ein.

> **Important**
>
> Wenn Sie ein MFA-Gerät für IAM Identity Center konfigurieren, empfehlen wir Ihnen, eine Kopie des QR-Codes oder geheimen Schlüssels an einem sicheren Ort aufzubewahren. Dies kann hilfreich sein, wenn der zugewiesene Benutzer das Telefon verliert oder die MFA-Authentifikator-App neu installieren muss. Wenn eines dieser Dinge eintritt, können Sie die App schnell neu konfigurieren, um dieselbe MFA-Konfiguration zu verwenden. Dadurch entfällt die Notwendigkeit, ein neues MFA-Gerät in IAM Identity Center für den Benutzer zu erstellen.

3. Geben Sie auf der Seite Authenticator-App einrichten unter Authenticator-Code das Einmalpasswort ein, das derzeit auf dem physischen MFA-Gerät angezeigt wird.

> **Important**
>
> Senden Sie die Anforderung direkt nach der Erzeugung der Codes. Wenn Sie den Code generieren und dann zu lange warten, um die Anfrage einzureichen, wurde das MFA-Gerät erfolgreich mit dem Benutzer verknüpft. Das MFA-Gerät ist jedoch nicht synchron. Dies liegt daran, weil die zeitgesteuerten Einmalpasswörter (TOTP) nach einer kurzen Zeit ungültig werden. In diesem Fall können Sie das Gerät neu synchronisieren.

4. Klicken Sie auf Assign MFA (MFA zuordnen). Das MFA-Gerät kann jetzt mit der Generierung von Einmalkennwörtern beginnen und ist jetzt für die Verwendung mit AWS bereit.

- Sicherheitsschlüssel

1. Folgen Sie auf der Seite Sicherheitsschlüssel Ihres Benutzers registrieren den Anweisungen Ihres Browsers oder Ihrer Plattform.

> **Note**
>
> Die Benutzererfahrung ist je nach Betriebssystem und Browser unterschiedlich. Folgen Sie daher bitte den Anweisungen Ihres Browsers oder Ihrer Plattform. Nachdem das Gerät Ihres Benutzers erfolgreich registriert wurde, haben Sie die Möglichkeit, dem neu registrierten Gerät Ihres Benutzers einen benutzerfreundlichen Anzeigenamen zuzuweisen. Wenn Sie dies ändern möchten, wählen Sie Umbenennen, geben Sie den neuen Namen ein und wählen Sie dann Speichern. Wenn Sie die Option aktiviert haben, dass Benutzer ihre eigenen Geräte verwalten können, wird dem Benutzer dieser benutzerfreundliche Name im AWS Zugriffsportal angezeigt.

Das MFA-Gerät eines Benutzers verwalten

Gehen Sie wie folgt vor, wenn Sie das MFA-Gerät eines Benutzers umbenennen oder löschen müssen.

Um ein MFA-Gerät umzubenennen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie den Benutzer in der Liste aus. Markieren Sie für diesen Schritt nicht das Kontrollkästchen neben dem Benutzer.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte, wählen Sie das Gerät aus und klicken Sie dann auf Umbenennen.
4. Wenn Sie dazu aufgefordert werden, geben Sie den neuen Namen ein und wählen Sie dann Umbenennen.

So löschen Sie ein MFA-Gerät

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich Benutzer aus. Wählen Sie den Benutzer in der Liste aus.
3. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte MFA-Geräte, wählen Sie das Gerät aus und klicken Sie dann auf Löschen.
4. Geben Sie zur Bestätigung DELETE ein und wählen Sie dann Löschen.

Zugriff verwalten auf AWS-Konten

AWS IAM Identity Center ist in integriert AWS Organizations, sodass Sie Berechtigungen für mehrere Benutzer zentral verwalten können, AWS-Konten ohne jedes Ihrer Konten manuell konfigurieren zu müssen. Sie können Berechtigungen definieren und diese Berechtigungen Workforce-Benutzern zuweisen, um deren Zugriff auf bestimmte Benutzer zu kontrollieren AWS-Konten.

AWS-Konto Typen

Es gibt zwei Arten von AWS-Konten Einträgen AWS Organizations:

- Verwaltungskonto — Das Konto AWS-Konto , das zur Erstellung der Organisation verwendet wird.
- Mitgliedskonten — Die AWS-Konten restlichen Konten gehören zu einer Organisation.

Weitere Informationen zu AWS-Konto Typen finden Sie unter AWS Organizations Terminologie und Konzepte im AWS Organizations Benutzerhandbuch.

Sie können sich auch dafür entscheiden, ein Mitgliedskonto als delegierter Administrator für IAM Identity Center zu registrieren. Benutzer mit diesem Konto können die meisten Verwaltungsaufgaben im IAM Identity Center ausführen. Weitere Informationen finden Sie unter Delegierte Verwaltung.

Für jede Aufgabe und jeden Kontotyp gibt die folgende Tabelle an, ob die IAM Identity Center-Verwaltungsaufgabe von Benutzern des Kontos ausgeführt werden kann.

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
Benutzer oder Gruppen lesen (die Gruppe selbst und die Gruppenmitgliedschaft lesen)	 Ja	 Ja	 Ja

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
Benutzer oder Gruppen hinzufügen, bearbeiten oder löschen	 Nein	 Ja	 Ja
Benutzerzugriff aktivieren oder deaktivieren	 Nein	 Ja	 Ja
Aktivieren, deaktivieren oder verwalten Sie eingehende Attribute	 Nein	 Ja	 Ja
Identitätsquellen ändern oder verwalten	 Nein	 Ja	 Ja
Anwendungen erstellen, bearbeiten oder löschen	 Nein	 Ja	 Ja
MFA konfigurieren	 Nein	 Ja	 Ja

Verwaltungsaufgaben von IAM Identity Center	Mitgliedskonto	Delegiertes Administratorkonto	Verwaltungskonto
Verwalten Sie Berechtigungssätze, die nicht im Verwaltungskonto bereitgestellt wurden	Nein	Ja	Ja
Verwalten Sie die im Verwaltungskonto bereitgestellten Berechtigungssätze	Nein	Nein	Ja
IAM Identity Center aktivieren	Nein	Nein	Ja
Löschen Sie die IAM Identity Center-Konfiguration	Nein	Nein	Ja
Aktivieren oder deaktivieren Sie den Benutzerzugriff im Verwaltungskonto	Nein	Nein	Ja
Registrieren oder deregistrieren Sie ein Mitgliedskonto als delegierter Administrator	Nein	Nein	Ja

Zugriff zuweisen AWS-Konto

Mithilfe von Berechtigungssätzen können Sie Benutzern und Gruppen in Ihrer Organisation den Zugriff darauf vereinfachen AWS-Konten. Berechtigungssätze werden in IAM Identity Center gespeichert und definieren die Zugriffsebene, auf die Benutzer und Gruppen zugreifen können. AWS-Konto Sie können einen einzelnen Berechtigungssatz erstellen und ihn mehreren AWS-Konten innerhalb Ihrer Organisation zuweisen. Sie können demselben Benutzer auch mehrere Berechtigungssätze zuweisen.

Weitere Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze erstellen, verwalten und löschen.

> **Note**
>
> Sie können Ihren Benutzern auch Single Sign-On-Zugriff auf Anwendungen zuweisen. Weitere Informationen finden Sie unter Zugriff auf Anwendungen verwalten.

Erfahrung für Endbenutzer

Das AWS Zugriffsportal bietet Benutzern von IAM Identity Center über ein Webportal Single Sign-On-Zugriff auf alle ihnen zugewiesenen AWS-Konten Anwendungen. Das AWS Zugriffsportal unterscheidet sich von dem AWS Management Console, bei dem es sich um eine Sammlung von Servicekonsolen für die Verwaltung AWS von Ressourcen handelt.

Wenn Sie einen Berechtigungssatz erstellen, wird der Name, den Sie für den Berechtigungssatz angeben, im AWS Access-Portal als verfügbare Rolle angezeigt. Benutzer melden sich beim AWS Access-Portal an, wählen eine AWS-Konto und dann die Rolle aus. Nachdem sie die Rolle ausgewählt haben, können sie mithilfe der auf AWS Dienste zugreifen AWS Management Console oder temporäre Anmeldeinformationen abrufen, um programmgesteuert auf AWS Dienste zuzugreifen.

Um die temporären Anmeldeinformationen für den AWS programmgesteuerten Zugriff zu öffnen AWS Management Console oder abzurufen, führen Benutzer die folgenden Schritte aus:

1. Benutzer öffnen ein Browserfenster und verwenden die von Ihnen angegebene Anmelde-URL, um zum Access-Portal zu navigieren. AWS
2. Mit ihren Verzeichnisanmeldedaten melden sie sich beim AWS Access-Portal an.

3. Nach der Authentifizierung wählen sie auf der AWS Access-Portalseite die Registerkarte Konten aus, um die Liste AWS-Konten anzuzeigen, auf die sie Zugriff haben.
4. Die Benutzer wählen dann AWS-Konto die aus, die sie verwenden möchten.
5. Unter dem Namen der werden alle Berechtigungssätze AWS-Konto, denen Benutzer zugewiesen sind, als verfügbare Rollen angezeigt. Wenn Sie dem `PowerUser` Berechtigungssatz beispielsweise `john_stiles` einen Benutzer zugewiesen haben, wird die Rolle im AWS Zugriffsportal als angezeigt`PowerUser/john_stiles`. Benutzer mit mehreren Berechtigungssätzen wählen aus, welche -Rolle verwendet werden soll. Benutzer können ihre Rolle für den Zugriff auf auswählen AWS Management Console.
6. Zusätzlich zur Rolle können AWS Access-Portal-Benutzer temporäre Anmeldeinformationen für den Befehlszeilen- oder programmgesteuerten Zugriff abrufen, indem sie Zugriffstasten wählen.

step-by-step Anleitungen, die Sie Ihren Mitarbeitern zur Verfügung stellen können, finden Sie unter Nutzung des AWS Zugangsportals undAbrufen der IAM Identity Center-Benutzeranmeldedaten für die AWS CLI oder SDKs AWS.

Erzwingung und Beschränkung des Zugriffs

Wenn Sie IAM Identity Center aktivieren, erstellt IAM Identity Center eine dienstbezogene Rolle. Sie können auch Service Control Policies (SCPs) verwenden.

Zugriff delegieren und erzwingen

Eine dienstverknüpfte Rolle ist eine Art von IAM-Rolle, die direkt mit einem Dienst verknüpft ist. AWS Nachdem Sie IAM Identity Center aktiviert haben, kann IAM Identity Center in jeder Rolle in Ihrer Organisation eine dienstbezogene Rolle erstellen. AWS-Konto Diese Rolle bietet vordefinierte Berechtigungen, mit denen IAM Identity Center delegieren und durchsetzen kann, welche Benutzer über Single Sign-On-Zugriff auf bestimmte Bereiche in Ihrer Organisation verfügen. AWS-Konten AWS Organizations Sie müssen einem oder mehreren Benutzern Zugriff auf ein Konto zuweisen, um diese Rolle verwenden zu können. Weitere Informationen finden Sie unter Service-verknüpfte Rollen und Verwendung von serviceverknüpften Rollen für IAM Identity Center.

Beschränken Sie den Zugriff auf den Identitätsspeicher von Mitgliedskonten aus

Für den von IAM Identity Center verwendeten Identitätsspeicherdienst können Benutzer, die Zugriff auf ein Mitgliedskonto haben, API-Aktionen verwenden, für die Leseberechtigungen erforderlich

sind. Mitgliedskonten haben Zugriff auf Leseaktionen sowohl im sso-directory - als auch im identitystore-Namespaces. Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS IAM Identity Center Verzeichnisse und Aktionen, Ressourcen und Bedingungsschlüssel für Identity Store in der Service Authorization Reference. AWS

Um zu verhindern, dass Benutzer in Mitgliedskonten API-Operationen im Identitätsspeicher verwenden, können Sie eine Service Control Policy (SCP) anhängen. Ein SCP ist eine Art von Organisationsrichtlinie, mit der Sie Berechtigungen in Ihrer Organisation verwalten können. Das folgende Beispiel für SCP verhindert, dass Benutzer in Mitgliedskonten auf API-Operationen im Identitätsspeicher zugreifen.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> Die Einschränkung des Zugriffs von Mitgliedskonten kann die Funktionalität von IAM Identity Center-fähigen Anwendungen beeinträchtigen.

Weitere Informationen finden Sie unter Service-Kontrollrichtlinien (SCPs) im AWS Organizations - Benutzerhandbuch.

Delegierte Verwaltung

Delegierte Administration bietet zugewiesenen Benutzern in einem registrierten Mitgliedskonto eine bequeme Möglichkeit, die meisten Verwaltungsaufgaben in IAM Identity Center auszuführen. Wenn Sie IAM Identity Center aktivieren, wird Ihre IAM Identity Center-Instanz standardmäßig im Verwaltungskonto erstellt. AWS Organizations Dies wurde ursprünglich so konzipiert, dass IAM Identity Center Rollen für alle Mitgliedskonten Ihrer Organisation bereitstellen, deren Bereitstellung aufheben und aktualisieren kann. Auch wenn sich Ihre IAM Identity Center-Instanz immer im Verwaltungskonto befinden muss, können Sie sich dafür entscheiden, die Verwaltung von IAM Identity Center an ein Mitgliedskonto in zu delegieren AWS Organizations, wodurch die Möglichkeit erweitert wird, IAM Identity Center von außerhalb des Verwaltungskontos zu verwalten.

Die Aktivierung der delegierten Administration bietet die folgenden Vorteile:

- Minimiert die Anzahl der Personen, die Zugriff auf das Verwaltungskonto benötigen, um Sicherheitsbedenken auszuräumen
- Ermöglicht ausgewählten Administratoren, Benutzern und Gruppen Anwendungen und Mitgliedskonten Ihrer Organisation zuzuweisen

Weitere Informationen zur Verwendung von IAM Identity Center finden Sie AWS Organizations unterZugriff verwalten auf AWS-Konten. Weitere Informationen und ein Beispiel für ein Unternehmensszenario zur Konfiguration der delegierten Administration finden Sie unter Erste Schritte mit der delegierten IAM Identity Center-Administration im Sicherheits-Blog.AWS

Themen

Bewährte Methoden

Im Folgenden finden Sie einige bewährte Methoden, die Sie berücksichtigen sollten, bevor Sie die delegierte Administration konfigurieren.

- Gewähren Sie dem Verwaltungskonto die geringsten Rechte — In dem Wissen, dass es sich bei dem Verwaltungskonto um ein Konto mit hohen Rechten handelt und dass Sie sich an das Prinzip der geringsten Rechte halten, empfehlen wir dringend, den Zugriff auf das Verwaltungskonto auf so wenige Personen wie möglich zu beschränken. Mit der Funktion für delegierte Administratoren soll die Anzahl der Personen minimiert werden, die Zugriff auf das Verwaltungskonto benötigen.
- Erstellen Sie Berechtigungssätze, die nur im Verwaltungskonto verwendet werden können — Dies erleichtert die Verwaltung von Berechtigungssätzen, die speziell auf Benutzer zugeschnitten sind, die auf Ihr Verwaltungskonto zugreifen, und hilft, sie von den Berechtigungssätzen zu unterscheiden, die von Ihrem delegierten Administratorkonto verwaltet werden.
- Berücksichtigen Sie Ihren Active Directory-Standort — Wenn Sie Active Directory als Ihre IAM Identity Center-Identitätsquelle verwenden möchten, suchen Sie das Verzeichnis in dem

Mitgliedskonto, in dem Sie die Funktion für delegierte Administratoren von IAM Identity Center aktiviert haben. Wenn Sie beschließen, die IAM Identity Center-Identitätsquelle von einer anderen Quelle in Active Directory oder 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.

- Benutzerzuweisungen nur im Verwaltungskonto erstellen — Der delegierte Administrator kann die im Verwaltungskonto bereitgestellten Berechtigungssätze nicht ändern. Delegierte Administratoren können jedoch Gruppen und Gruppenzuweisungen hinzufügen, bearbeiten und löschen.

Voraussetzungen

Bevor Sie ein Konto als delegierter Administrator registrieren können, müssen Sie zunächst die folgende Umgebung bereitstellen:

- AWS Organizations muss zusätzlich zu Ihrem Standard-Verwaltungskonto mit mindestens einem Mitgliedskonto aktiviert und konfiguriert sein.
- Wenn Ihre Identitätsquelle auf Active Directory eingestellt ist, muss die Konfigurierbare AD-Synchronisierung von IAM Identity Center Funktion aktiviert sein.

Registrieren Sie ein Mitgliedskonto

Um die delegierte Administration zu konfigurieren, müssen Sie zunächst ein Mitgliedskonto in Ihrer Organisation als delegierter Administrator registrieren. Benutzer in diesem Mitgliedskonto, die über ausreichende Berechtigungen verfügen, haben Administratorzugriff auf IAM Identity Center. Nachdem ein Mitgliedskonto erfolgreich für die delegierte Verwaltung registriert wurde, wird es als delegiertes Administratorkonto bezeichnet. Weitere Informationen zu den Aufgaben, die das delegierte Administratorkonto ausführen kann, finden Sie unter. AWS-Konto Typen

IAM Identity Center unterstützt die Registrierung jeweils nur eines Mitgliedskontos als delegierter Administrator. Sie können ein Mitgliedskonto nur registrieren, wenn Sie mit den Anmeldeinformationen des Verwaltungskontos angemeldet sind.

Gehen Sie wie folgt vor, um Administratorzugriff auf IAM Identity Center zu gewähren, indem Sie ein bestimmtes Mitgliedskonto in Ihrer AWS Organisation als delegierten Administrator registrieren.

> **Important**
>
> Durch diesen Vorgang wird der Administratorzugriff für IAM Identity Center an Administratorbenutzer in diesem Mitgliedskonto delegiert. Alle Benutzer, die über ausreichende Berechtigungen für dieses delegierte Administratorkonto verfügen, können alle administrativen Aufgaben von IAM Identity Center von diesem Konto aus ausführen, mit Ausnahme von:
>
> - IAM Identity Center aktivieren
> - Löschen von IAM Identity Center-Konfigurationen
> - Verwaltung der im Verwaltungskonto bereitgestellten Berechtigungssätze
> - Registrierung oder Abmeldung anderer Mitgliedskonten als delegierte Administratoren
> - Benutzerzugriff im Verwaltungskonto aktivieren oder deaktivieren
>
> Der delegierte Administrator kann die Gruppenmitgliedschaft bearbeiten.

Um ein Mitgliedskonto zu registrieren

1. Melden Sie sich AWS Management Console mit den Anmeldeinformationen Ihres Verwaltungskontos unter an AWS Organizations. Für die Ausführung der RegisterDelegatedAdministratorAPI sind Anmeldeinformationen für das Verwaltungskonto erforderlich.
2. Wählen Sie die Region aus, in der IAM Identity Center aktiviert ist, und öffnen Sie dann die IAM Identity Center-Konsole.
3. Wählen Sie Einstellungen und dann die Registerkarte Verwaltung aus.
4. Wählen Sie im Bereich Delegierter Administrator die Option Konto registrieren aus.
5. Wählen Sie auf der Seite Delegierten Administrator registrieren den Administrator aus, den AWS-Konto Sie registrieren möchten, und klicken Sie dann auf Konto registrieren.

Aufheben der Registrierung eines Mitgliedskontos

Sie können ein Mitgliedskonto nur abmelden, wenn Sie mit den Anmeldeinformationen des Verwaltungskontos angemeldet sind.

Gehen Sie wie folgt vor, um den Administratorzugriff auf IAM Identity Center zu entfernen, indem Sie ein Mitgliedskonto in Ihrer AWS Organisation abmelden, das zuvor als delegierter Administrator benannt wurde.

> **Important**
>
> Wenn Sie ein Konto abmelden, entziehen Sie effektiv allen Administratorbenutzern die Möglichkeit, IAM Identity Center von diesem Konto aus zu verwalten. Daher können sie IAM Identity Center-Identitäten, Zugriffsmanagement, Authentifizierung oder Anwendungszugriff von diesem Konto aus nicht mehr verwalten. Dieser Vorgang wirkt sich nicht auf die in IAM Identity Center konfigurierten Berechtigungen oder Zuweisungen aus und hat daher keine Auswirkungen auf Ihre Endbenutzer, da diese weiterhin Zugriff auf ihre Apps haben, und zwar vom Zugriffsportal AWS-Konten aus. AWS

Um ein Mitgliedskonto abzumelden

1. Melden Sie sich AWS Management Console mit den Anmeldeinformationen Ihres Verwaltungskontos unter an. AWS Organizations Für die Ausführung der DeregisterDelegatedAdministratorAPI sind Anmeldeinformationen für das Verwaltungskonto erforderlich.
2. Wählen Sie die Region aus, in der IAM Identity Center aktiviert ist, und öffnen Sie dann die IAM Identity Center-Konsole.
3. Wählen Sie Einstellungen und dann die Registerkarte Verwaltung aus.
4. Wählen Sie im Bereich Delegierter Administrator die Option Konto abmelden aus.
5. Überprüfen Sie im Dialogfeld „Konto abmelden“ die Sicherheitsauswirkungen und geben Sie dann den Namen des Mitgliedskontos ein, um zu bestätigen, dass Sie damit einverstanden sind.
6. Wählen Sie Konto abmelden.

Sehen Sie sich an, welches Mitgliedskonto als delegierter Administrator registriert wurde

Gehen Sie wie folgt vor, um herauszufinden, welches Mitgliedskonto in Ihrem Konto als delegierter Administrator für IAM Identity Center konfiguriert AWS Organizations wurde.

Um Ihr registriertes Mitgliedskonto einzusehen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Suchen Sie im Abschnitt Details unter Delegierter Administrator nach dem registrierten Kontonamen. Sie können diese Informationen auch finden, indem Sie die Registerkarte Verwaltung auswählen und sie im Bereich Delegierter Administrator anzeigen.

Temporärer Zugriff mit erhöhten Rechten

Jeder Zugriff auf Ihren AWS-Konto ist mit einem gewissen Maß an Rechten verbunden. Vertrauliche Vorgänge, wie das Ändern der Konfiguration für eine wertvolle Ressource, z. B. eine Produktionsumgebung, erfordern aufgrund ihres Umfangs und ihrer möglichen Auswirkungen eine besondere Behandlung. Temporärer erweiterter Zugriff (auch als just-in-time Zugriff bezeichnet) ist eine Möglichkeit, die Verwendung einer Berechtigung zur Ausführung einer bestimmten Aufgabe während eines bestimmten Zeitraums anzufordern, zu genehmigen und nachzuverfolgen. Temporärer erweiterter Zugriff ergänzt andere Formen der Zugriffskontrolle, wie z. B. Berechtigungssätze und Multi-Faktor-Authentifizierung.

AWS IAM Identity Center bietet die folgenden Optionen für die Verwaltung temporärer Zugriffsberechtigungen mit erhöhten Zugriffsrechten in verschiedenen geschäftlichen und technischen Umgebungen:

- Vom Anbieter verwaltete und unterstützte Lösungen — AWS hat die IAM Identity Center-Integrationen ausgewählter Partnerangebote validiert und deren Fähigkeiten anhand gängiger Kundenanforderungen bewertet. Wählen Sie die Lösung, die am besten zu Ihrem Szenario passt, und folgen Sie den Anweisungen des Anbieters, um die Funktionen mit IAM Identity Center zu aktivieren.
- Selbstverwaltet und eigenständig unterstützt — Diese Option bietet einen Ausgangspunkt, wenn Sie an einem temporären erweiterten Zugriff interessiert sind. Sie können die Funktionen AWS dann selbst implementieren, anpassen und verwalten. Weitere Informationen finden Sie unter Temporäre Verwaltung erhöhter Zugriffsrechte (TEAM).

Validierte AWS Sicherheitspartner für temporären Zugriff mit erhöhten Zugriffsrechten

AWS Sicherheitspartner verwenden unterschiedliche Ansätze, um gemeinsame Anforderungen an temporäre erhöhte Zugriffsrechte zu erfüllen. Wir empfehlen Ihnen, jede Partnerlösung sorgfältig zu prüfen, damit Sie eine auswählen können, die Ihren Bedürfnissen und Vorlieben am besten entspricht, einschließlich Ihres Unternehmens, der Architektur Ihrer Cloud-Umgebung und Ihres Budgets.

> **Note**
>
> Für die Notfallwiederherstellung empfehlen wir, dass Sie den Notfallzugriff auf die einrichten, AWS Management Console bevor es zu einer Unterbrechung kommt.

AWS Identity hat die Funktionen und die Integration mit IAM Identity Center für die folgenden just-in-time Angebote von AWS Sicherheitspartnern validiert:

- CyberArk Secure Cloud Access— Dieses Angebot ist Teil von und bietet erweiterten Zugriff auf On-Demand-Umgebungen AWS sowie Multi-Cloud-Umgebungen. CyberArk Identity Security Platform Genehmigungen werden entweder durch die Integration mit ITSM oder Tools gewährleistet. ChatOps Alle Sitzungen können aus Prüfungs- und Compliance-Gründen aufgezeichnet werden.
- Tenable (previously Ermetic)— Die Tenable Plattform umfasst die Bereitstellung von just-in-time privilegiertem Zugriff für Verwaltungsvorgänge in AWS und Multi-Cloud-Umgebungen. Sitzungsprotokolle aus allen Cloud-Umgebungen, einschließlich AWS CloudTrail Zugriffsprotokollen, sind in einer einzigen Oberfläche für Analysen und Audits verfügbar. Die Funktion lässt sich in Unternehmens- und Entwicklertools wie Slack und Microsoft Teams integrieren.
- OktaZugriffsanfragen — Als Teil von Okta Identity Governance können Sie einen Workflow für just-in-time Zugriffsanfragen konfigurieren, indem Sie Okta als IAM Identity Center einen externen Identitätsanbieter (IdP) und Ihre IAM Identity Center-Berechtigungssätze verwenden.

Diese Liste wird aktualisiert, um die Funktionen zusätzlicher Partnerlösungen und die Integration dieser Lösungen mit IAM Identity Center zu AWS überprüfen.

> **Note**
>
> Wenn Sie ressourcenbasierte Richtlinien, Amazon Elastic Kubernetes Service (Amazon EKS) oder AWS Key Management Service (AWS KMS) verwenden, informieren Sie sich, Referenzieren von Berechtigungssätzen in Ressourcenrichtlinien, Amazon EKS und AWS KMS bevor Sie sich für Ihre Lösung entscheiden. just-in-time

Temporäre Funktionen für erhöhten Zugriff wurden zur Partnervalidierung bewertet AWS

AWS Identity hat bestätigt, dass die von CyberArk Secure Cloud AccessTenable, und Access Requests angebotenen Funktionen für temporären erhöhten Okta Zugriff die folgenden allgemeinen Kundenanforderungen erfüllen:

- Benutzer können Zugriff auf einen Berechtigungssatz für einen vom Benutzer angegebenen Zeitraum anfordern und dabei das AWS Konto, den Berechtigungssatz, den Zeitraum und den Grund angeben.
- Benutzer können den Genehmigungsstatus für ihre Anfrage erhalten.
- Benutzer können eine Sitzung mit einem bestimmten Bereich nicht aufrufen, es sei denn, es liegt eine genehmigte Anfrage mit demselben Umfang vor und sie rufen die Sitzung während des genehmigten Zeitraums auf.
- Es gibt eine Möglichkeit, festzulegen, wer Anfragen genehmigen kann.
- Genehmiger können ihre eigenen Anfragen nicht genehmigen.
- Genehmigende Personen haben eine Liste mit ausstehenden, genehmigten und abgelehnten Anfragen und können diese für Prüfer exportieren.
- Genehmiger können ausstehende Anträge genehmigen und ablehnen.
- Genehmiger können eine Notiz hinzufügen, in der sie ihre Entscheidung erläutern.
- Genehmiger können eine genehmigte Anfrage zurückziehen und so die future Verwendung von erhöhtem Zugriff verhindern.

> **Note**
>
> Wenn ein Benutzer beim Widerruf einer genehmigten Anfrage mit erhöhten Zugriffsrechten angemeldet ist, bleibt seine Sitzung bis zu einer Stunde nach dem Widerruf der

Genehmigung aktiv. Informationen zu Authentifizierungssitzungen finden Sie unter. Authentifizierung

- Benutzeraktionen und Genehmigungen stehen zur Prüfung zur Verfügung.

Single Sign-On-Zugriff auf AWS-Konten

Sie können Benutzern in Ihrem verbundenen Verzeichnis AWS Organizations basierend auf den allgemeinen Aufgabenfunktionen Berechtigungen für das Verwaltungskonto oder die Mitgliedskonten in Ihrer Organisation zuweisen. Alternativ können Sie benutzerdefinierte Berechtigungen verwenden, um Ihre spezifischen Sicherheitsanforderungen zu erfüllen. Beispielsweise können Sie Datenbankadministratoren umfassende Berechtigungen für Amazon RDS in Entwicklungskonten gewähren, ihre Berechtigungen jedoch in Produktionskonten einschränken. IAM Identity Center konfiguriert automatisch alle erforderlichen Benutzerberechtigungen in Ihrem AWS-Konten .

> **Note**
>
> Möglicherweise müssen Sie Benutzern oder Gruppen Berechtigungen gewähren, um im AWS Organizations Verwaltungskonto arbeiten zu können. Da es sich um ein Konto mit hohen Rechten handelt, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen über die FullAccessIAM-Richtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

Weisen Sie Benutzerzugriff zu AWS-Konten

Gehen Sie wie folgt vor, um Benutzern und Gruppen in Ihrem verbundenen Verzeichnis Single Sign-On-Zugriff zuzuweisen und mithilfe von Berechtigungssätzen deren Zugriffsebene zu bestimmen.

Informationen zum Überprüfen vorhandener Benutzer- und Gruppenzugriffe finden Sie unterBenutzer- und Gruppenzuweisungen anzeigen.

> **Note**
>
> Zur vereinfachten Administration der Zugriffsberechtigungen wird empfohlen, den Zugriff direkt den Gruppen zuzuweisen (und nicht einzelnen Benutzern). Bei Gruppen können Sie Berechtigungen für Benutzergruppen gewähren oder verweigern, anstatt dies für jede

Einzelperson individuell zu tun. Wenn ein Benutzer zu einer anderen Organisation wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe. Er erhält dann automatisch die Berechtigungen für die neue Organisation.

So weisen Sie Benutzer- oder Gruppenzugriff zu AWS-Konten

1. Öffnen Sie die IAM Identity Center-Konsole.

   > **Note**
   >
   > Stellen Sie sicher, dass die IAM Identity Center-Konsole die Region verwendet, in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie mit dem nächsten Schritt fortfahren.

2. Wählen Sie im Navigationsbereich unter Berechtigungen für mehrere Konten die Option. AWS-Konten
3. Auf der AWS-KontenSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Aktivieren Sie das Kontrollkästchen neben einem oder mehreren, denen AWS-Konten Sie Single Sign-On-Zugriff zuweisen möchten.

   > **Note**
   >
   > Sie können pro Berechtigungssatz bis zu 10 AWS-Konten gleichzeitig auswählen, wenn Sie Benutzern und Gruppen Single Sign-On-Zugriff zuweisen. Um derselben Gruppe von Benutzern und Gruppen mehr als 10 AWS-Konten zuzuweisen, wiederholen Sie dieses Verfahren nach Bedarf für die zusätzlichen Konten. Wenn Sie dazu aufgefordert werden, wählen Sie dieselben Benutzer, Gruppen und denselben Berechtigungssatz aus.

4. Wählen Sie Benutzer oder Gruppen zuweisen aus.
5. Gehen Sie für Schritt 1: Benutzer und Gruppen auswählen auf der Seite Benutzer und Gruppen zu "***AWS-account-name***" zuweisen wie folgt vor:

   1. Wählen Sie auf der Registerkarte Benutzer einen oder mehrere Benutzer aus, denen Sie Single Sign-On-Zugriff gewähren möchten.

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

2. Wählen Sie auf der Registerkarte Gruppen eine oder mehrere Gruppen aus, denen Sie Single Sign-On-Zugriff gewähren möchten.

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

3. Um die ausgewählten Benutzer und Gruppen anzuzeigen, klicken Sie auf das seitliche Dreieck neben Ausgewählte Benutzer und Gruppen.

4. Nachdem Sie bestätigt haben, dass die richtigen Benutzer und Gruppen ausgewählt sind, wählen Sie Weiter.

6. Gehen Sie für Schritt 2: Berechtigungssätze auswählen auf der Seite "***AWS-account-name***" Berechtigungssätze zuweisen wie folgt vor:

   1. Wählen Sie einen oder mehrere Berechtigungssätze aus. Bei Bedarf können Sie neue Berechtigungssätze erstellen und auswählen.

      - Um einen oder mehrere vorhandene Berechtigungssätze auszuwählen, wählen Sie unter Berechtigungssätze die Berechtigungssätze aus, die Sie auf die Benutzer und Gruppen anwenden möchten, die Sie im vorherigen Schritt ausgewählt haben.
      - Um einen oder mehrere neue Berechtigungssätze zu erstellen, wählen Sie Berechtigungssatz erstellen aus und folgen Sie den Schritten unterBerechtigungssatz erstellen. Nachdem Sie die Berechtigungssätze erstellt haben, die Sie anwenden möchten, kehren Sie in der IAM Identity Center-Konsole zu den Anweisungen zurück AWS-Kontenund folgen Sie den Anweisungen, bis Sie zu Schritt 2: Berechtigungssätze auswählen gelangen. Wenn Sie diesen Schritt erreicht haben, wählen Sie die neuen Berechtigungssätze aus, die Sie erstellt haben, und fahren Sie mit dem nächsten Schritt in diesem Verfahren fort.

   2. Nachdem Sie bestätigt haben, dass die richtigen Berechtigungssätze ausgewählt wurden, wählen Sie Weiter.

7. Gehen Sie für Schritt 3: Überprüfen und abschicken auf der Seite Aufgaben überprüfen und an "***AWS-account-name***" senden wie folgt vor:

   1. Überprüfen Sie die ausgewählten Benutzer, Gruppen und Berechtigungssätze.

   2. Nachdem Sie sich vergewissert haben, dass die richtigen Benutzer, Gruppen und Berechtigungssätze ausgewählt wurden, wählen Sie Senden aus.

> **Important**
>
> Der Vorgang der Benutzer- und Gruppenzuweisung kann einige Minuten dauern. Lassen Sie diese Seite geöffnet, bis der Vorgang erfolgreich abgeschlossen ist.

> **Note**
>
> Möglicherweise müssen Sie Benutzern oder Gruppen Berechtigungen gewähren, um mit dem AWS Organizations Verwaltungskonto arbeiten zu können. Da es sich um ein Konto mit hohen Rechten handelt, müssen Sie aufgrund zusätzlicher Sicherheitseinschränkungen über die FullAccessIAM-Richtlinie oder entsprechende Berechtigungen verfügen, bevor Sie dieses Konto einrichten können. Diese zusätzlichen Sicherheitseinschränkungen sind für keines der Mitgliedskonten in Ihrer AWS Organisation erforderlich.

Entfernen Sie den Benutzer- und Gruppenzugriff

Gehen Sie wie folgt vor, um den Single Sign-On-Zugriff AWS-Konto für einen oder mehrere Benutzer und Gruppen in Ihrem verbundenen Verzeichnis zu entfernen.

So entfernen Sie den Benutzer- und Gruppenzugriff auf ein AWS-Konto

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im Navigationsbereich unter Berechtigungen für mehrere Konten die Option. AWS-Konten
3. Auf der AWS-KontenSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Wählen Sie den Namen der Datei aus AWS-Konto , die die Benutzer und Gruppen enthält, für die Sie den Single Sign-On-Zugriff entfernen möchten.
4. Wählen Sie auf der Übersichtsseite für unter Zugewiesene Benutzer und Gruppen den Namen eines oder mehrerer Benutzer oder Gruppen aus, und wählen Sie Zugriff entfernen aus. AWS-Konto
5. Vergewissern Sie sich im Dialogfeld Zugriff entfernen, dass die Namen der Benutzer oder Gruppen korrekt sind, und wählen Sie Zugriff entfernen aus.

Widerrufen Sie aktive IAM-Rollensitzungen, die mit Berechtigungssätzen erstellt wurden

Im Folgenden finden Sie ein allgemeines Verfahren zum Widerrufen einer aktiven Berechtigungssatz-Sitzung für einen IAM Identity Center-Benutzer. Das Verfahren geht davon aus, dass Sie einem Benutzer, dessen Anmeldeinformationen kompromittiert wurden, oder einem böswilligen Akteur, der sich im System befindet, jeglichen Zugriff entziehen möchten. Voraussetzung ist, dass Sie die Anweisungen in Bereiten Sie sich darauf vor, eine aktive IAM-Rollensitzung zu widerrufen, die mit einem Berechtigungssatz erstellt wurde befolgt haben. Wir gehen davon aus, dass die Richtlinie „Alle verweigern“ in einer Service Control Policy (SCP) enthalten ist.

> **Note**
>
> AWS empfiehlt, dass Sie eine Automatisierung für alle Schritte einrichten, mit Ausnahme von Vorgängen, die nur auf der Konsole ausgeführt werden.

1. Besorgen Sie sich die Benutzer-ID der Person, deren Zugriff Sie widerrufen müssen. Sie können die Identitätsspeicher-APIs verwenden, um den Benutzer anhand seines Benutzernamens zu finden.
2. Aktualisieren Sie die Deny-Richtlinie, um die Benutzer-ID aus Schritt 1 zu Ihrer Service Control Policy (SCP) hinzuzufügen. Nach Abschluss dieses Schritts verliert der Zielbenutzer den Zugriff und kann keine Aktionen mit Rollen ausführen, die von der Richtlinie betroffen sind.
3. Entfernen Sie alle Zuweisungen von Berechtigungssätzen für den Benutzer. Wenn der Zugriff über Gruppenmitgliedschaften zugewiesen wird, entfernen Sie den Benutzer aus allen Gruppen und allen direkten Zuweisungen von Berechtigungssätzen. Dieser Schritt verhindert, dass der Benutzer zusätzliche IAM-Rollen übernimmt. Wenn ein Benutzer über eine aktive AWS Access-Portal-Sitzung verfügt und Sie den Benutzer deaktivieren, kann er weiterhin neue Rollen annehmen, bis Sie ihm den Zugriff entziehen.
4. Wenn Sie einen Identitätsanbieter (IdP) oder Microsoft Active Directory als Identitätsquelle verwenden, deaktivieren Sie den Benutzer in der Identitätsquelle. Durch die Deaktivierung des Benutzers wird die Erstellung zusätzlicher AWS Access-Portal-Sitzungen verhindert. Verwenden Sie Ihre IdP- oder Microsoft Active Directory-API-Dokumentation, um zu erfahren, wie Sie diesen Schritt automatisieren können. Wenn Sie das IAM Identity Center-Verzeichnis als Identitätsquelle verwenden, deaktivieren Sie den Benutzerzugriff noch nicht. In Schritt 6 deaktivieren Sie den Benutzerzugriff.

5. Suchen Sie in der IAM Identity Center-Konsole nach dem Benutzer und löschen Sie seine aktive Sitzung.

   a. Wählen Sie Users (Benutzer) aus.

   b. Wählen Sie den Benutzer aus, dessen aktive Sitzung Sie löschen möchten.

   c. Wählen Sie auf der Detailseite des Benutzers den Tab Aktive Sitzungen aus.

   d. Aktivieren Sie die Kontrollkästchen neben den Sitzungen, die Sie löschen möchten, und wählen Sie Sitzung löschen aus.

   Dadurch wird sichergestellt, dass die AWS Access-Portal-Sitzung des Benutzers innerhalb von etwa 60 Minuten beendet wird. Erfahren Sie mehr über die Sitzungsdauer.

6. Deaktivieren Sie in der IAM Identity Center-Konsole den Benutzerzugriff.

   a. Wählen Sie Users (Benutzer) aus.

   b. Wählen Sie den Benutzer aus, dessen Zugriff Sie deaktivieren möchten.

   c. Erweitern Sie auf der Detailseite des Benutzers den Bereich Allgemeine Informationen und klicken Sie auf die Schaltfläche Benutzerzugriff deaktivieren, um weitere Anmeldungen des Benutzers zu verhindern.

7. Lassen Sie die Ablehnungsrichtlinie mindestens 12 Stunden lang bestehen. Andernfalls hat der Benutzer mit einer aktiven IAM-Rollensitzung Aktionen mit der IAM-Rolle wiederhergestellt. Wenn Sie 12 Stunden warten, laufen aktive Sitzungen ab und der Benutzer kann nicht mehr auf die IAM-Rolle zugreifen.

> **Important**
>
> Wenn Sie den Zugriff eines Benutzers deaktivieren, bevor Sie die Benutzersitzung beenden (Sie haben Schritt 6 abgeschlossen, ohne Schritt 5 abgeschlossen zu haben), können Sie die Benutzersitzung nicht mehr über die IAM Identity Center-Konsole beenden. Wenn Sie versehentlich den Benutzerzugriff deaktivieren, bevor Sie die Benutzersitzung beenden, können Sie den Benutzer erneut aktivieren, seine Sitzung beenden und dann seinen Zugriff wieder deaktivieren.

Sie können jetzt die Anmeldeinformationen des Benutzers ändern, falls sein Passwort kompromittiert wurde, und seine Zuweisungen wiederherstellen.

Delegieren Sie, wer Benutzern und Gruppen im Verwaltungskonto Single Sign-On-Zugriff zuweisen kann

Die Zuweisung von Single Sign-On-Zugriff auf das Verwaltungskonto mithilfe der IAM Identity Center-Konsole ist eine privilegierte Aktion. Standardmäßig kann nur ein Benutzer Root-Benutzer des AWS-Kontos oder ein Benutzer, dem die Richtlinien zugewiesen AWSSSOMasterAccountAdministratorund IAMFullAccess AWS verwaltet wurden, dem Verwaltungskonto Single Sign-On-Zugriff zuweisen. Die IAMFullAccessRichtlinien AWSSSOMasterAccountAdministratorund verwalten den Single Sign-On-Zugriff auf das Verwaltungskonto innerhalb einer AWS Organizations Organisation.

Gehen Sie wie folgt vor, um Berechtigungen zur Verwaltung des Single Sign-On-Zugriffs an Benutzer und Gruppen in Ihrem Verzeichnis zu delegieren.

So gewähren Sie Benutzern und Gruppen in Ihrem Verzeichnis Berechtigungen zur Verwaltung des Single Sign-On-Zugriffs

1. Melden Sie sich bei der IAM Identity Center-Konsole als Root-Benutzer des Verwaltungskontos oder mit einem anderen Benutzer an, der über Administratorrechte für das Verwaltungskonto verfügt.
2. Folgen Sie den Schritten unterBerechtigungssatz erstellen, um einen Berechtigungssatz zu erstellen, und gehen Sie dann wie folgt vor:

    1. Aktivieren Sie auf der Seite Neuen Berechtigungssatz erstellen das Kontrollkästchen Benutzerdefinierten Berechtigungssatz erstellen und wählen Sie dann Weiter: Details aus.
    2. Geben Sie auf der Seite Neuen Berechtigungssatz erstellen einen Namen für den benutzerdefinierten Berechtigungssatz und optional eine Beschreibung an. Ändern Sie bei Bedarf die Sitzungsdauer und geben Sie eine Relay-Status-URL an.

        > **Note**
        >
        > Für die Relay-State-URL müssen Sie eine URL angeben, die sich in der befindet AWS Management Console. Beispielsweise:
        > **`https://console.aws.amazon.com/ec2/`**
        > Weitere Informationen finden Sie unter Stellen Sie den Relay-Status ein.

    3. Unter Welche Richtlinien möchten Sie in Ihren Berechtigungssatz aufnehmen? , aktivieren Sie das Kontrollkästchen AWS Verwaltete Richtlinien anhängen.

4. Wählen Sie in der Liste der IAM-Richtlinien sowohl die als auch die AWSSSOMasterAccountAdministratorIAMFullAccess AWS verwalteten Richtlinien aus. Diese Richtlinien gewähren allen Benutzern und Gruppen, denen in future Zugriff auf diesen Berechtigungssatz zugewiesen wird, Berechtigungen.
5. Wählen Sie Weiter: Markierungen.
6. Geben Sie unter Tags hinzufügen (optional) Werte für Schlüssel und Wert (optional) an und wählen Sie dann Weiter: Überprüfen aus. Weitere Informationen zu Tags erhalten Sie unter Markieren von AWS IAM Identity Center-Ressourcen.
7. Überprüfen Sie die von Ihnen getroffenen Auswahlen und wählen Sie dann Erstellen aus.

3. Folgen Sie den Schritten unterWeisen Sie Benutzerzugriff zu AWS-Konten, um dem soeben erstellten Berechtigungssatz die entsprechenden Benutzer und Gruppen zuzuweisen.
4. Teilen Sie den zugewiesenen Benutzern Folgendes mit: Wenn sie sich beim AWS Zugriffsportal anmelden und die Registerkarte Konten auswählen, müssen sie den entsprechenden Rollennamen auswählen, um mit den Berechtigungen authentifiziert zu werden, die Sie gerade delegiert haben.

Berechtigungssätze

Ein Berechtigungssatz ist eine von Ihnen erstellte und verwaltete Vorlage, die eine Sammlung von einer oder mehreren IAM-Richtlinien definiert. Berechtigungssätze vereinfachen die Zuweisung von AWS-Konto Zugriffen für Benutzer und Gruppen in Ihrer Organisation. Sie können beispielsweise einen Berechtigungssatz für Datenbankadministratoren erstellen, der Richtlinien für die Verwaltung von AWS RDS-, DynamoDB- und Aurora-Diensten enthält, und diesen einzigen Berechtigungssatz verwenden, um Ihren Datenbankadministratoren Zugriff auf eine Liste von Zielen AWS-Konten innerhalb Ihrer AWS Organisation zu gewähren.

IAM Identity Center weist einem Benutzer oder einer Gruppe in einer oder mehreren Gruppen Zugriff mit Berechtigungssätzen zu. AWS-Konten Wenn Sie einen Berechtigungssatz zuweisen, erstellt IAM Identity Center in jedem Konto die entsprechenden, vom IAM Identity Center kontrollierten IAM-Rollen und ordnet diesen Rollen die im Berechtigungssatz angegebenen Richtlinien zu. IAM Identity Center verwaltet die Rolle und ermöglicht es den von Ihnen definierten autorisierten Benutzern, die Rolle mithilfe des IAM Identity Center-Benutzerportals oder AWS der CLI zu übernehmen. Wenn Sie den Berechtigungssatz ändern, stellt IAM Identity Center sicher, dass die entsprechenden IAM-Richtlinien und -Rollen entsprechend aktualisiert werden.

Sie können Ihren Berechtigungssätzen verwaltete Richtlinien, vom Kunden verwaltete Richtlinien, Inline-Richtlinien und AWS verwaltete Richtlinien für Jobfunktionen hinzufügen AWS . Sie können auch eine AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie als Berechtigungsgrenze zuweisen.

Informationen zum Erstellen eines Berechtigungssatzes finden Sie unterBerechtigungssätze erstellen, verwalten und löschen.

Themen

Vordefinierte Berechtigungen

Sie können einen vordefinierten Berechtigungssatz mit AWS verwalteten Richtlinien erstellen.

Wenn Sie einen Berechtigungssatz mit vordefinierten Berechtigungen erstellen, wählen Sie eine Richtlinie aus einer Liste AWS verwalteter Richtlinien aus. Innerhalb der verfügbaren Richtlinien können Sie zwischen allgemeinen Berechtigungsrichtlinien und Richtlinien für Jobfunktionen wählen.

Allgemeine Genehmigungsrichtlinien

Wählen Sie aus einer Liste AWS verwalteter Richtlinien, die den Zugriff auf Ihre gesamten Ressourcen ermöglichen AWS-Konto. Sie können eine der folgenden Richtlinien hinzufügen:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Richtlinien für Berufsfunktionen

Wählen Sie aus einer Liste AWS verwalteter Richtlinien, mit denen Sie auf Ressourcen in Ihrem Unternehmen zugreifen können AWS-Konto , die für eine Stelle in Ihrem Unternehmen relevant sein könnten. Sie können eine der folgenden Richtlinien hinzufügen:

- Billing

- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Eine ausführliche Beschreibung der verfügbaren allgemeinen Berechtigungsrichtlinien und Richtlinien für Jobfunktionen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter AWS Verwaltete Richtlinien für Jobfunktionen.

Anweisungen zum Erstellen eines Berechtigungssatzes finden Sie unterBerechtigungssätze erstellen, verwalten und löschen.

Benutzerdefinierte Berechtigungen

Sie können einen Berechtigungssatz mit benutzerdefinierten Berechtigungen erstellen und dabei alle AWS verwalteten und kundenverwalteten Richtlinien, die Sie in AWS Identity and Access Management (IAM) haben, mit Inline-Richtlinien kombinieren. Sie können auch eine Berechtigungsgrenze angeben und so die maximal möglichen Berechtigungen festlegen, die andere Richtlinien Benutzern Ihres Berechtigungssatzes gewähren können.

Anweisungen zum Erstellen eines Berechtigungssatzes finden Sie unterBerechtigungssätze erstellen, verwalten und löschen.

Richtlinientypen, die Sie Ihrem Berechtigungssatz hinzufügen können

Themen

- Eingebundene Richtlinien
- AWS verwaltete Richtlinien
- Kundenverwaltete Richtlinien
- Berechtigungsgrenzen

Eingebundene Richtlinien

Sie können eine Inline-Richtlinie an einen Berechtigungssatz anhängen. Eine Inline-Richtlinie ist ein Textblock, der als IAM-Richtlinie formatiert ist und den Sie direkt zu Ihrem Berechtigungssatz

hinzufügen. Sie können eine Richtlinie einfügen oder mit dem Tool zur Richtlinienerstellung in der IAM Identity Center-Konsole eine neue Richtlinie generieren, wenn Sie einen neuen Berechtigungssatz erstellen. Sie können IAM-Richtlinien auch mit dem AWS Policy Generator erstellen.

Wenn Sie einen Berechtigungssatz mit einer Inline-Richtlinie bereitstellen, erstellt IAM Identity Center dort, AWS-Konten wo Sie Ihren Berechtigungssatz zuweisen, eine IAM-Richtlinie. IAM Identity Center erstellt die Richtlinie, wenn Sie dem Konto den Berechtigungssatz zuweisen. Die Richtlinie wird dann an die IAM-Rolle in Ihrem System angehängt AWS-Konto , die Ihr Benutzer annimmt.

Wenn Sie eine Inline-Richtlinie erstellen und Ihren Berechtigungssatz zuweisen, konfiguriert IAM Identity Center die Richtlinien für Sie AWS-Konten . Wenn Sie Ihren Berechtigungssatz mit erstellenKundenverwaltete Richtlinien, müssen Sie die Richtlinien AWS-Konten selbst erstellen, bevor Sie den Berechtigungssatz zuweisen.

AWS verwaltete Richtlinien

Sie können AWS verwaltete Richtlinien an Ihren Berechtigungssatz anhängen. AWS Verwaltete Richtlinien sind IAM-Richtlinien, die AWS beibehalten werden. Im Gegensatz dazu Kundenverwaltete Richtlinien sind es IAM-Richtlinien in Ihrem Konto, die Sie erstellen und verwalten. AWS verwaltete Richtlinien befassen sich mit den häufigsten Anwendungsfällen mit den geringsten Rechten in Ihrem AWS-Konto. Sie können eine AWS verwaltete Richtlinie als Berechtigungen für die Rolle, die IAM Identity Center erstellt, oder als Rechtegrenze zuweisen.

AWS verwaltet AWS verwaltete Richtlinien für Jobfunktionen, die Ihren Ressourcen auftragsspezifische Zugriffsberechtigungen zuweisen. AWS Sie können eine Richtlinie für bestimmte Funktionen hinzufügen, wenn Sie vordefinierte Berechtigungen mit Ihrem Berechtigungssatz verwenden möchten. Wenn Sie Benutzerdefinierte Berechtigungen wählen, können Sie mehr als eine Richtlinie für berufliche Funktionen hinzufügen.

Ihre enthält AWS-Konto auch eine große Anzahl AWS verwalteter IAM-Richtlinien für bestimmte AWS-Services und Kombinationen von. AWS-Services Wenn Sie einen Berechtigungssatz mit benutzerdefinierten Berechtigungen erstellen, können Sie aus vielen zusätzlichen AWS verwalteten Richtlinien wählen, die Sie Ihrem Berechtigungssatz zuweisen möchten.

AWS füllt jede AWS-Konto mit AWS verwalteten Richtlinien auf. Um einen Berechtigungssatz mit AWS verwalteten Richtlinien bereitzustellen, müssen Sie nicht zuerst eine Richtlinie in Ihrem AWS-Konten erstellen. Wenn Sie Ihren Berechtigungssatz mit erstellenKundenverwaltete Richtlinien, müssen Sie die Richtlinien AWS-Konten selbst erstellen, bevor Sie den Berechtigungssatz zuweisen.

Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

Kundenverwaltete Richtlinien

Sie können Ihrem Berechtigungssatz vom Kunden verwaltete Richtlinien hinzufügen. Kundenverwaltete Richtlinien sind IAM-Richtlinien in Ihrem Konto, die Sie erstellen und verwalten. Im Gegensatz dazu AWS verwaltete Richtlinien gelten für Ihr Konto die IAM-Richtlinien, die AWS beibehalten werden. Sie können eine vom Kunden verwaltete Richtlinie als Berechtigungen für die Rolle, die IAM Identity Center erstellt, oder als Rechtegrenze zuweisen.

Wenn Sie einen Berechtigungssatz mit einer vom Kunden verwalteten Richtlinie erstellen, müssen Sie in allen Bereichen, AWS-Konto denen IAM Identity Center Ihren Berechtigungssatz zuweist, eine IAM-Richtlinie mit demselben Namen und Pfad erstellen. Wenn Sie einen benutzerdefinierten Pfad angeben, stellen Sie sicher, dass Sie in jedem Pfad denselben Pfad angeben. AWS-Konto Weitere Informationen finden Sie unter Anzeigenamen und -pfade im IAM-Benutzerhandbuch. IAM Identity Center fügt die IAM-Richtlinie der IAM-Rolle hinzu, die es in Ihrem erstellt. AWS-Konto Es hat sich bewährt, in jedem Konto, dem Sie den Berechtigungssatz zuweisen, dieselben Berechtigungen auf die Richtlinie anzuwenden. Weitere Informationen finden Sie unter Verwenden Sie IAM-Richtlinien in Berechtigungssätzen.

Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Vom Kunden verwaltete Richtlinien.

Berechtigungsgrenzen

Sie können Ihrem Berechtigungssatz eine Berechtigungsgrenze hinzufügen. Eine Berechtigungsgrenze ist eine AWS verwaltete oder vom Kunden verwaltete IAM-Richtlinie, die die maximalen Berechtigungen festlegt, die eine identitätsbasierte Richtlinie einem IAM-Prinzipal gewähren kann. Wenn Sie eine Berechtigungsgrenze anwenden, AWS verwaltete Richtlinien können Ihre Eingebundene RichtlinienKundenverwaltete Richtlinien, und keine Berechtigungen gewähren, die die durch Ihre Berechtigungsgrenze gewährten Berechtigungen überschreiten. Eine Berechtigungsgrenze gewährt keine Berechtigungen, sondern sorgt dafür, dass IAM alle Berechtigungen ignoriert, die über diese Grenze hinausgehen.

Wenn Sie einen Berechtigungssatz mit einer vom Kunden verwalteten Richtlinie als Berechtigungsgrenze erstellen, müssen Sie in allen Bereichen, AWS-Konto denen IAM Identity Center Ihren Berechtigungssatz zuweist, eine IAM-Richtlinie mit demselben Namen erstellen. IAM

Identity Center fügt der IAM-Rolle, die es in Ihrem erstellt, die IAM-Richtlinie als Berechtigungsgrenze hinzu. AWS-Konto

Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

Berechtigungssätze erstellen, verwalten und löschen

Berechtigungssätze definieren die Zugriffsebene, auf die Benutzer und Gruppen zugreifen können. AWS-Konto Berechtigungssätze werden im IAM Identity Center gespeichert und können für einen oder mehrere Personen bereitgestellt werden. AWS-Konten Sie können einem Benutzer mehrere Berechtigungssätze zuweisen. Weitere Informationen zu Berechtigungssätzen und deren Verwendung in IAM Identity Center finden Sie unter. Berechtigungssätze

Beachten Sie bei der Erstellung von Berechtigungssätzen die folgenden Überlegungen:

- Beginnen Sie mit einem vordefinierten Berechtigungssatz

  Mit einem vordefinierten Berechtigungssatz, der vordefinierte Berechtigungen verwendet, wählen Sie eine einzelne AWS verwaltete Richtlinie aus einer Liste verfügbarer Richtlinien aus. Jede Richtlinie gewährt eine bestimmte Zugriffsebene auf AWS Dienste und Ressourcen oder Berechtigungen für eine allgemeine Aufgabenfunktion. Informationen zu jeder dieser Richtlinien finden Sie unter AWS Verwaltete Richtlinien für Berufsfunktionen. Nachdem Sie Nutzungsdaten erfasst haben, können Sie den Berechtigungssatz so verfeinern, dass er restriktiver ist.
- Beschränken Sie die Dauer der Verwaltungssitzung auf angemessene Arbeitszeiträume

  Wenn Benutzer sich mit ihnen verbinden AWS-Konto und die AWS Management Console oder die AWS Befehlszeilenschnittstelle (AWS CLI) verwenden, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Wenn die Benutzersitzung die Sitzungsdauer erreicht, werden sie von der Konsole abgemeldet und aufgefordert, sich erneut anzumelden. Aus Sicherheitsgründen empfehlen wir, die Sitzungsdauer nicht länger festzulegen, als für die Ausführung der Rolle erforderlich ist. Standardmäßig ist der Wert für die Sitzungsdauer eine Stunde. Sie können einen Höchstwert von 12 Stunden angeben. Weitere Informationen finden Sie unter Legen Sie die Sitzungsdauer fest.
- Beschränken Sie die Sitzungsdauer des Workforce-Benutzerportals

  Workforce-Benutzer verwenden Portalsitzungen, um Rollen auszuwählen und auf Anwendungen zuzugreifen. Standardmäßig beträgt der Wert für Maximale Sitzungsdauer, der bestimmt, wie lange ein Workforce-Benutzer beim AWS Access-Portal angemeldet sein kann, bevor er sich erneut

authentifizieren muss, acht Stunden. Sie können einen Höchstwert von 90 Tagen angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Sitzungsdauer des AWS Zugriffsportals und der integrierten IAM Identity Center-Anwendungen.

- Verwenden Sie die Rolle, die Berechtigungen mit den geringsten Rechten gewährt

  Jeder Berechtigungssatz, den Sie erstellen und Ihrem Benutzer zuweisen, wird im Zugriffsportal als verfügbare Rolle angezeigt. AWS Wenn Sie sich als dieser Benutzer beim Portal anmelden, wählen Sie die Rolle aus, die dem restriktivsten Berechtigungssatz entspricht, den Sie für die Ausführung von Aufgaben im Konto verwenden können, und nicht`AdministratorAccess`. Testen Sie Ihre Berechtigungssätze, um sicherzustellen, dass sie den erforderlichen Zugriff gewähren, bevor Sie die Benutzereinladung senden.

> **Note**
>
> Sie können sie auch verwenden AWS CloudFormation, um Berechtigungssätze zu erstellen und zuzuweisen und diesen Berechtigungssätzen Benutzer zuzuweisen.

Themen

Berechtigungssatz erstellen

Gehen Sie wie folgt vor, um einen vordefinierten Berechtigungssatz zu erstellen, der eine einzelne AWS verwaltete Richtlinie verwendet, oder einen benutzerdefinierten Berechtigungssatz, der bis zu 10 AWS verwaltete oder vom Kunden verwaltete Richtlinien und eine Inline-Richtlinie verwendet. Sie können in der Service Quotas Quotas-Konsole für IAM eine Anpassung der maximalen Anzahl von 10 Richtlinien beantragen.

Sie können einen Berechtigungssatz in der IAM Identity Center-Konsole erstellen.

So erstellen Sie einen Berechtigungssatz

1. Öffnen Sie die IAM Identity Center-Konsole.

2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie Create permission set (Berechtigungssatz erstellen) aus.
4. Wählen Sie auf der Seite Berechtigungssatztyp auswählen unter Typ des Berechtigungssatzes einen Berechtigungssatztyp aus.
5. Wählen Sie je nach Typ des Berechtigungssatzes eine oder mehrere Richtlinien aus, die Sie für den Berechtigungssatz verwenden möchten:

   - Vordefinierter Berechtigungssatz

     1. Wählen Sie unter Richtlinie für vordefinierten Berechtigungssatz eine der IAM-Job-Funktionsrichtlinien oder Allgemeine Berechtigungsrichtlinien in der Liste aus, und klicken Sie dann auf Weiter. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Aufgabenfunktionen und AWS Verwaltete Richtlinien im AWS Identity and Access Management Benutzerhandbuch.
     2. Fahren Sie mit Schritt 6 fort, um die Seite mit den Details zum Berechtigungssatz angeben auszufüllen.

   - Benutzerdefinierter Berechtigungssatz

     1. Wählen Sie Weiter aus.
     2. Wählen Sie auf der Seite Richtlinien und Berechtigungsgrenzen angeben die Typen von IAM-Richtlinien aus, die Sie auf Ihren neuen Berechtigungssatz anwenden möchten. Standardmäßig können Sie Ihrem Berechtigungssatz eine beliebige Kombination aus bis zu 10 AWS verwalteten Richtlinien und vom Kunden verwalteten Richtlinien hinzufügen. Dieses Kontingent wird von IAM festgelegt. Um ihn zu erhöhen, fordern Sie eine Erhöhung des IAM-Kontingents an. Verwaltete Richtlinien, die mit einer IAM-Rolle verknüpft sind, in der Konsole Service Quotas in allen Bereichen, AWS-Konto denen Sie den Berechtigungssatz zuweisen möchten.

        - Erweitern Sie die AWS verwalteten Richtlinien um Richtlinien von IAM, das AWS erstellt und verwaltet wird. Weitere Informationen finden Sie unter AWS verwaltete Richtlinien.

          a. Suchen Sie im Berechtigungssatz nach AWS verwalteten Richtlinien, die Sie auf Ihre Benutzer anwenden möchten, und wählen Sie sie aus.

          b. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie den entsprechenden Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.

- Erweitern Sie Kundenverwaltete Richtlinien, um Richtlinien aus IAM hinzuzufügen, die Sie erstellen und verwalten. Weitere Informationen finden Sie unter Kundenverwaltete Richtlinien.
  a. Wählen Sie Richtlinien anhängen und geben Sie den Namen einer Richtlinie ein, die Sie Ihrem Berechtigungssatz hinzufügen möchten. Erstellen Sie in jedem Konto, dem Sie den Berechtigungssatz zuweisen möchten, eine Richtlinie mit dem von Ihnen eingegebenen Namen. Es hat sich bewährt, der Richtlinie in jedem Konto dieselben Berechtigungen zuzuweisen.
  b. Wählen Sie Weitere hinzufügen, um eine weitere Richtlinie hinzuzufügen.
  c. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie den entsprechenden Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.
- Erweitern Sie Inline-Richtlinie, um benutzerdefinierten Richtlinientext im JSON-Format hinzuzufügen. Inline-Richtlinien entsprechen nicht vorhandenen IAM-Ressourcen. Um eine Inline-Richtlinie zu erstellen, geben Sie die benutzerdefinierte Richtliniensprache in das bereitgestellte Formular ein. IAM Identity Center fügt die Richtlinie zu den IAM-Ressourcen hinzu, die es in Ihren Mitgliedskonten erstellt. Weitere Informationen finden Sie unter Eingebundene Richtlinien.
  a. Fügen Sie Ihre gewünschten Aktionen und Ressourcen im interaktiven Editor zu Ihrer Inline-Richtlinie hinzu. Zusätzliche Kontoauszüge können mit Neue Aussage hinzufügen hinzugefügt werden.
  b. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie dessen Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.
- Erweitern Sie die Berechtigungsgrenze, um eine AWS verwaltete oder vom Kunden verwaltete IAM-Richtlinie als maximale Anzahl von Berechtigungen hinzuzufügen, die Ihre anderen Richtlinien im Berechtigungssatz zuweisen können. Weitere Informationen finden Sie unter Berechtigungsgrenzen.
  a. Wählen Sie „Berechtigungsgrenze verwenden“, um die maximalen Berechtigungen festzulegen.
  b. Wählen Sie „AWS Verwaltete Richtlinie“, um eine Richtlinie von IAM festzulegen, die als Ihre Berechtigungsgrenze AWSerstellt und verwaltet wird. Wählen Sie vom Kunden

verwaltete Richtlinien aus, um eine Richtlinie von IAM festzulegen, die Sie als Ihre Rechtegrenze erstellen und verwalten.

c. Wenn Sie einen anderen Richtlinientyp hinzufügen möchten, wählen Sie den entsprechenden Container aus und treffen Sie Ihre Auswahl. Wählen Sie Weiter, wenn Sie alle Richtlinien ausgewählt haben, die Sie anwenden möchten. Fahren Sie mit Schritt 6 fort, um die Seite „Details zum Berechtigungssatz angeben“ abzuschließen.

6. Gehen Sie auf der Seite „Details zum Berechtigungssatz angeben“ wie folgt vor:

   1. Geben Sie unter Name des Berechtigungssatzes einen Namen ein, um diesen Berechtigungssatz in IAM Identity Center zu identifizieren. Der Name, den Sie für diesen Berechtigungssatz angeben, wird im AWS Zugriffsportal als verfügbare Rolle angezeigt. Benutzer melden sich beim AWS Access-Portal an, wählen eine AWS-Konto und dann die Rolle aus.
   2. (Optional) Sie können auch eine Beschreibung eingeben. Die Beschreibung wird nur in der IAM Identity Center-Konsole angezeigt, nicht im AWS Zugriffsportal.
   3. (Optional) Geben Sie den Wert für die Sitzungsdauer an. Dieser Wert bestimmt, wie lange ein Benutzer angemeldet sein kann, bevor die Konsole ihn von seiner Sitzung abmeldet. Weitere Informationen finden Sie unter Legen Sie die Sitzungsdauer fest.
   4. (Optional) Geben Sie den Wert für den Relay-Status an. Dieser Wert wird im Verbundprozess verwendet, um Benutzer innerhalb des Kontos umzuleiten. Weitere Informationen finden Sie unter Stellen Sie den Relay-Status ein.

      > **Note**
      >
      > Die Relay-State-URL muss sich innerhalb von befinden AWS Management Console. Beispielsweise:
      > **`https://console.aws.amazon.com/ec2/`**

   5. Erweitern Sie Tags (optional), wählen Sie Tag hinzufügen aus, und geben Sie dann Werte für Schlüssel und Wert an (optional).

      Informationen zu Tags siehe Markieren von AWS IAM Identity Center-Ressourcen.

   6. Wählen Sie Weiter aus.

7. Überprüfen Sie auf der Seite Überprüfen und erstellen die von Ihnen getroffenen Auswahlen und wählen Sie dann Erstellen aus.

8. Wenn Sie einen Berechtigungssatz erstellen, wird der Berechtigungssatz standardmäßig nicht bereitgestellt (in keinem AWS-Konten verwendet). Um einen Berechtigungssatz in einem bereitzustellen AWS-Konto, müssen Sie Benutzern und Gruppen im Konto IAM Identity Center-Zugriff zuweisen und dann den Berechtigungssatz auf diese Benutzer und Gruppen anwenden. Weitere Informationen finden Sie unter Single Sign-On-Zugriff auf AWS-Konten.

Delegieren Sie die Verwaltung des Berechtigungssatzes

Mit IAM Identity Center können Sie die Verwaltung von Berechtigungssätzen und Zuweisungen in Konten delegieren, indem Sie IAM-Richtlinien erstellen, die auf die Amazon-Ressourcennamen (ARNs) von IAM Identity Center-Ressourcen verweisen. Sie können beispielsweise Richtlinien erstellen, die es verschiedenen Administratoren ermöglichen, Zuweisungen in bestimmten Konten für Berechtigungssätze mit bestimmten Tags zu verwalten.

Sie können eine der folgenden Methoden verwenden, um diese Arten von Richtlinien zu erstellen.

- (Empfohlen) Erstellen Sie in IAM Identity Center Berechtigungssätze mit jeweils unterschiedlichen Richtlinien und weisen Sie die Berechtigungssätze verschiedenen Benutzern oder Gruppen zu. Auf diese Weise können Sie Administratorberechtigungen für Benutzer verwalten, die sich mit der von Ihnen ausgewählten IAM Identity Center-Identitätsquelle anmelden.
- Erstellen Sie benutzerdefinierte Richtlinien in IAM und fügen Sie sie dann den IAM-Rollen hinzu, die Ihre Administratoren übernehmen. Informationen zu Rollen finden Sie unter IAM-Rollen, um die ihnen zugewiesenen IAM Identity Center-Administratorberechtigungen zu erhalten.

> **Important**
>
> Bei den ARNs für IAM Identity Center-Ressourcen wird zwischen Groß- und Kleinschreibung unterschieden.

Im Folgenden wird die korrekte Schreibweise für den Verweis auf den IAM Identity Center-Berechtigungssatz und die Kontoressourcentypen dargestellt.

Ressourcentypen	ARN	Kontextschlüssel
PermissionSet	`arn:${Partition}:sso:::permissionSet`	`aws:ResourceTag/${TagKey}`

Ressourcentypen	ARN	Kontextschlüssel
	`/${InstanceId}/${PermissionSetId}`	
Account	`arn:${Partition}:sso:::account/${AccountId}`	Nicht zutreffend

Verwenden Sie IAM-Richtlinien in Berechtigungssätzen

In haben Sie gelerntBerechtigungssatz erstellen, wie Sie einem Berechtigungssatz Richtlinien hinzufügen, einschließlich kundenverwalteter Richtlinien und Berechtigungsgrenzen. Wenn Sie einem Berechtigungssatz vom Kunden verwaltete Richtlinien und Berechtigungen hinzufügen, erstellt IAM Identity Center in keinem Fall AWS-Konten eine Richtlinie. Stattdessen müssen Sie diese Richtlinien im Voraus in jedem Konto erstellen, dem Sie Ihren Berechtigungssatz zuweisen möchten, und sie mit den Namens- und Pfadangaben Ihres Berechtigungssatzes abgleichen. Wenn Sie einem AWS-Konto in Ihrer Organisation einen Berechtigungssatz zuweisen, erstellt IAM Identity Center eine AWS Identity and Access Management (IAM-) Rolle und ordnet Ihre IAM-Richtlinien dieser Rolle zu.

> **Note**
>
> Bevor Sie Ihrem Berechtigungssatz IAM-Richtlinien zuordnen, müssen Sie Ihr Mitgliedskonto vorbereiten. Der Name einer IAM-Richtlinie in Ihrem Mitgliedskonto muss unter Berücksichtigung der Groß- und Kleinschreibung mit dem Namen der Richtlinie in Ihrem Verwaltungskonto übereinstimmen. IAM Identity Center kann den Berechtigungssatz nicht zuweisen, wenn die Richtlinie in Ihrem Mitgliedskonto nicht vorhanden ist.
> Die Berechtigungen, die die Richtlinie gewährt, müssen den Konten nicht exakt entsprechen.

Um einem Berechtigungssatz eine IAM-Richtlinie zuzuweisen

1. Erstellen Sie in jedem Bereich, in AWS-Konten dem Sie den Berechtigungssatz zuweisen möchten, eine IAM-Richtlinie.
2. Weisen Sie der IAM-Richtlinie Berechtigungen zu. Sie können verschiedenen Konten unterschiedliche Berechtigungen zuweisen. Für ein einheitliches Nutzererlebnis sollten Sie in jeder Richtlinie identische Berechtigungen konfigurieren und verwalten. Sie können

Automatisierungsressourcen verwenden AWS CloudFormation StackSets , um beispielsweise Kopien einer IAM-Richtlinie mit demselben Namen und denselben Berechtigungen in jedem Mitgliedskonto zu erstellen. Weitere Informationen zu CloudFormation StackSets finden Sie unter Arbeiten mit AWS CloudFormation StackSets im AWS CloudFormation Benutzerhandbuch.

3. Erstellen Sie einen Berechtigungssatz in Ihrem Verwaltungskonto und fügen Sie Ihre IAM-Richtlinie unter Vom Kunden verwaltete Richtlinien oder Rechtegrenze hinzu. Weitere Informationen zum Erstellen eines Berechtigungssatzes finden Sie unterBerechtigungssatz erstellen.
4. Fügen Sie alle Inline-Richtlinien, AWS verwalteten Richtlinien oder zusätzlichen IAM-Richtlinien hinzu, die Sie vorbereitet haben.
5. Erstellen Sie Ihren Berechtigungssatz und weisen Sie ihn zu.

Löschen Sie Berechtigungssätze

Informationen zum Widerrufen einer aktiven Sitzung mit Berechtigungssätzen finden Sie unterWiderrufen Sie aktive IAM-Rollensitzungen, die mit Berechtigungssätzen erstellt wurden.

Bevor Sie einen Berechtigungssatz aus IAM Identity Center löschen können, müssen Sie ihn aus allen entfernen, AWS-Konten die den Berechtigungssatz verwenden. Informationen zum Überprüfen vorhandener Benutzer- und Gruppenzugriffe finden Sie unterBenutzer- und Gruppenzuweisungen anzeigen.

So entfernen Sie einen Berechtigungssatz aus einem AWS-Konto

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option. AWS-Konten
3. Auf der AWS-KontenSeite wird eine Strukturansicht Ihrer Organisation angezeigt. Wählen Sie den Namen des Berechtigungssatzes AWS-Konto aus, aus dem Sie den Berechtigungssatz entfernen möchten.
4. Wählen Sie auf der Übersichtsseite für die die AWS-Konto die Registerkarte Berechtigungssätze aus.
5. Aktivieren Sie das Kontrollkästchen neben dem Berechtigungssatz, den Sie entfernen möchten, und wählen Sie dann Entfernen aus.
6. Vergewissern Sie sich im Dialogfeld Berechtigungssatz entfernen, dass der richtige Berechtigungssatz ausgewählt ist, geben Sie einen Text ein, **`Delete`** um das Entfernen zu bestätigen, und wählen Sie dann Zugriff entfernen aus.

Gehen Sie wie folgt vor, um einen oder mehrere Berechtigungssätze zu löschen, sodass sie von niemandem AWS-Konto in der Organisation mehr verwendet werden können.

> **Note**
>
> Alle Benutzer und Gruppen, denen dieser Berechtigungssatz zugewiesen wurde, können AWS-Konto sich nicht mehr anmelden, unabhängig davon, wer ihn verwendet. Informationen zum Überprüfen vorhandener Benutzer- und Gruppenzugriffe finden Sie unterBenutzer- und Gruppenzuweisungen anzeigen.

So löschen Sie einen Berechtigungssatz aus einem AWS-Konto

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie den Berechtigungssatz aus, den Sie löschen möchten, und wählen Sie dann Löschen aus.
4. Geben Sie im Dialogfeld Berechtigungssatz löschen den Namen des Berechtigungssatzes ein, um das Löschen zu bestätigen, und wählen Sie dann Löschen aus. Der Name berücksichtigt Groß- und Kleinschreibung.

Konfigurieren Sie die Eigenschaften des Berechtigungssatzes

In IAM Identity Center können Sie die Benutzererfahrung anpassen, indem Sie die folgenden Eigenschaften des Berechtigungssatzes konfigurieren.

Themen

- Legen Sie die Sitzungsdauer fest
- Stellen Sie den Relay-Status ein
- Verwenden Sie eine Ablehnungsrichtlinie, um aktiven Benutzerberechtigungen zu entziehen

Legen Sie die Sitzungsdauer fest

Für jeden Berechtigungssatz können Sie eine Sitzungsdauer angeben, um zu steuern, wie lange ein Benutzer angemeldet sein kann AWS-Konto. Wenn die angegebene Dauer abgelaufen ist, wird der AWS Benutzer von der Sitzung abgemeldet.

Wenn Sie einen neuen Berechtigungssatz erstellen, ist die Sitzungsdauer standardmäßig auf 1 Stunde (in Sekunden) festgelegt. Die Mindestsitzungsdauer beträgt 1 Stunde und kann auf maximal 12 Stunden festgelegt werden. IAM Identity Center erstellt automatisch IAM-Rollen in jedem zugewiesenen Konto für jeden Berechtigungssatz und konfiguriert diese Rollen mit einer maximalen Sitzungsdauer von 12 Stunden.

Wenn Benutzer sich mit ihrer AWS-Konto Konsole verbinden oder wenn AWS Command Line Interface (AWS CLI) verwendet wird, verwendet IAM Identity Center die Einstellung für die Sitzungsdauer im Berechtigungssatz, um die Dauer der Sitzung zu steuern. Standardmäßig können von IAM Identity Center für Berechtigungssätze generierte IAM-Rollen nur von IAM Identity Center-Benutzern übernommen werden. Dadurch wird sichergestellt, dass die im IAM Identity Center-Berechtigungssatz angegebene Sitzungsdauer durchgesetzt wird.

> **Important**
>
> Als bewährte Sicherheitsmaßnahme empfehlen wir Ihnen, die Sitzungsdauer nicht länger als für die Ausführung der Rolle nötig festzulegen.

Nachdem Sie einen Berechtigungssatz erstellt haben, können Sie ihn aktualisieren, um eine neue Sitzungsdauer anzuwenden. Gehen Sie wie folgt vor, um die Sitzungsdauer für einen Berechtigungssatz zu ändern.

So legen Sie die Sitzungsdauer fest

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie den Namen des Berechtigungssatzes aus, für den Sie die Sitzungsdauer ändern möchten.
4. Wählen Sie auf der Detailseite für den Berechtigungssatz rechts neben der Überschrift Allgemeine Einstellungen die Option Bearbeiten aus.
5. Wählen Sie auf der Seite Allgemeine Einstellungen für den Berechtigungssatz bearbeiten einen neuen Wert für die Sitzungsdauer aus.
6. Wenn der Berechtigungssatz in einem beliebigen Verzeichnis bereitgestellt wurde AWS-Konten, werden die Namen der Konten unter Automatische AWS-Konten erneute Bereitstellung angezeigt. Nachdem der Wert für die Sitzungsdauer für den Berechtigungssatz aktualisiert wurde, werden alle, AWS-Konten die den Berechtigungssatz verwenden, erneut bereitgestellt.

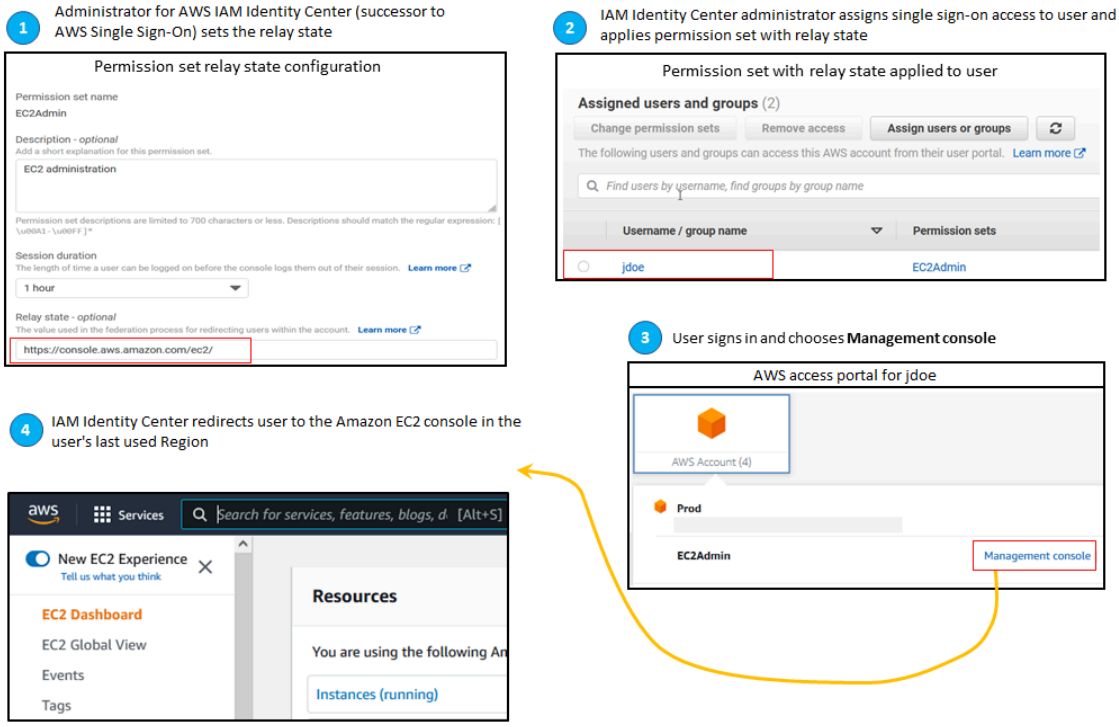
Das bedeutet, dass der neue Wert für diese Einstellung auf alle angewendet wird AWS-Konten , die den Berechtigungssatz verwenden.

7. Wählen Sie Änderungen speichern aus.
8. Oben auf der AWS-KontenSeite wird eine Benachrichtigung angezeigt.

   - Wenn der Berechtigungssatz in einem oder mehreren Fällen bereitgestellt wurde AWS-Konten, bestätigt die Benachrichtigung, dass die erneute Bereitstellung erfolgreich AWS-Konten war und dass der aktualisierte Berechtigungssatz auf die Konten angewendet wurde.
   - Wenn der Berechtigungssatz nicht in einem bereitgestellt wurde, bestätigt die Benachrichtigung AWS-Konto, dass die Einstellungen für den Berechtigungssatz aktualisiert wurden.

Stellen Sie den Relay-Status ein

Wenn sich ein Benutzer beim AWS Zugriffsportal anmeldet, ein Konto auswählt und dann die Rolle auswählt, die aus dem zugewiesenen Berechtigungssatz AWS erstellt wird, leitet IAM Identity Center den Browser des Benutzers standardmäßig an den AWS Management Console weiter. Sie können dieses Verhalten ändern, indem Sie den Relay-Status auf eine andere Konsolen-URL setzen. Wenn Sie den Relay-Status festlegen, können Sie dem Benutzer schnellen Zugriff auf die Konsole gewähren, die für seine Rolle am besten geeignet ist. Sie können den Relay-Status beispielsweise auf die Amazon EC2 EC2-Konsolen-URL (**`https://console.aws.amazon.com/ec2/`**) setzen, um den Benutzer zu dieser Konsole umzuleiten, wenn er die Amazon EC2 EC2-Administratorrolle auswählt. Während der Umleitung zur Standard-URL oder Relay-State-URL leitet IAM Identity Center den Browser des Benutzers an den Konsolenendpunkt weiter, den der Benutzer zuletzt AWS-Region verwendet hat. Wenn ein Benutzer beispielsweise seine letzte Konsolensitzung in der Region Europa (Stockholm) (eu-north-1) beendet hat, wird der Benutzer zur Amazon EC2 EC2-Konsole in dieser Region umgeleitet.



Um IAM Identity Center so zu konfigurieren, dass der Benutzer zu einer Konsole in einem bestimmten Bereich weitergeleitet wird AWS-Region, fügen Sie die Regionsspezifikation als Teil der URL hinzu. Um den Benutzer beispielsweise zur Amazon EC2 EC2-Konsole in der Region USA Ost (Ohio) (us-east-2) umzuleiten, geben Sie die URL für die Amazon EC2 EC2-Konsole in dieser Region an (). **`https://us-east-2.console.aws.amazon.com/ec2/`** Wenn Sie IAM Identity Center in der Region USA West (Oregon) (us-west-2) aktiviert haben und Sie den Benutzer zu dieser Region weiterleiten möchten, geben Sie Folgendes an. **`https://us-west-2.console.aws.amazon.com`**

Gehen Sie wie folgt vor, um die Relay-Status-URL für einen Berechtigungssatz zu konfigurieren.

Um den Relay-Status zu konfigurieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie unter Berechtigungen für mehrere Konten die Option Berechtigungssätze aus.
3. Wählen Sie den Namen des Berechtigungssatzes aus, für den Sie die neue Relay-Status-URL festlegen möchten.
4. Wählen Sie auf der Detailseite für den Berechtigungssatz rechts neben der Überschrift Allgemeine Einstellungen die Option Bearbeiten aus.

5. Geben Sie auf der Seite Allgemeine Berechtigungssatz-Einstellungen bearbeiten unter Relay-Status eine Konsolen-URL für einen der AWS Dienste ein. Beispielsweise:

   `https://console.aws.amazon.com/ec2/`

   > **Note**
   >
   > Die Relay-Status-URL muss sich innerhalb von befinden AWS Management Console.

6. Wenn der Berechtigungssatz in einem beliebigen Verzeichnis bereitgestellt wurde AWS-Konten, werden die Namen der Konten unter AWS-Konten „Automatische Neubereitstellung“ angezeigt. Nachdem die Relay-Status-URL für den Berechtigungssatz aktualisiert wurde, werden alle, AWS-Konten die den Berechtigungssatz verwenden, erneut bereitgestellt. Das bedeutet, dass der neue Wert für diese Einstellung auf alle angewendet wird AWS-Konten , die den Berechtigungssatz verwenden.
7. Wählen Sie Änderungen speichern aus.
8. Oben auf der AWS Organisationsseite wird eine Benachrichtigung angezeigt.

   - Wenn der Berechtigungssatz in einem oder mehreren Fällen bereitgestellt wurde AWS-Konten, bestätigt die Benachrichtigung, dass die erneute Bereitstellung erfolgreich AWS-Konten war und dass der aktualisierte Berechtigungssatz auf die Konten angewendet wurde.
   - Wenn der Berechtigungssatz nicht in einem bereitgestellt wurde, bestätigt die Benachrichtigung AWS-Konto, dass die Einstellungen für den Berechtigungssatz aktualisiert wurden.

> **Note**
>
> Sie können diesen Prozess automatisieren, indem Sie die AWS API, ein AWS SDK oder die AWS Command Line Interface(AWS CLI) verwenden. Weitere Informationen finden Sie hier:
>
> - Die `UpdatePermissionSet` Aktionen `CreatePermissionSet` oder in der IAM Identity Center API-Referenz
> - Die `update-permission-set` Befehle `create-permission-set` oder im sso-adminAbschnitt der AWS CLI Befehlsreferenz.

Verwenden Sie eine Ablehnungsrichtlinie, um aktiven Benutzerberechtigungen zu entziehen

Möglicherweise müssen Sie einem IAM Identity Center-Benutzer den Zugriff entziehen, AWS-Konten solange der Benutzer aktiv einen Berechtigungssatz verwendet. Sie können ihnen die Nutzung ihrer aktiven IAM-Rollensitzungen entziehen, indem Sie im Voraus eine Ablehnungsrichtlinie für einen nicht spezifizierten Benutzer implementieren. Anschließend können Sie die Verweigerungsrichtlinie bei Bedarf aktualisieren, um den Benutzer anzugeben, dessen Zugriff Sie blockieren möchten. In diesem Thema wird erklärt, wie eine Ablehnungsrichtlinie erstellt wird, und es werden Überlegungen zur Implementierung der Richtlinie angestellt.

Bereiten Sie sich darauf vor, eine aktive IAM-Rollensitzung zu widerrufen, die mit einem Berechtigungssatz erstellt wurde

Sie können verhindern, dass der Benutzer mit einer IAM-Rolle, die er aktiv verwendet, Aktionen ausführt, indem Sie mithilfe einer Service Control-Richtlinie eine „Alle verweigern“ -Richtlinie für einen bestimmten Benutzer anwenden. Sie können auch verhindern, dass ein Benutzer einen beliebigen Berechtigungssatz verwendet, bis Sie sein Passwort ändern, wodurch ein böswilliger Akteur, der gestohlene Anmeldeinformationen aktiv missbraucht, entfernt wird. Wenn Sie den Zugriff generell verweigern und verhindern möchten, dass ein Benutzer erneut einen Berechtigungssatz eingibt oder auf andere Berechtigungssätze zugreift, können Sie auch den gesamten Benutzerzugriff entfernen, die aktive AWS Access-Portalsitzung beenden und die Benutzeranmeldung deaktivieren. Weitere Informationen Widerrufen Sie aktive IAM-Rollensitzungen, die mit Berechtigungssätzen erstellt wurden zur Verwendung der Richtlinie „Verweigern“ in Verbindung mit zusätzlichen Aktionen für eine umfassendere Sperrung des Zugriffs finden Sie unter.

Richtlinie verweigern

Sie können eine Ablehnungsrichtlinie mit einer Bedingung verwenden, die mit der Bedingung des Benutzers `UserID` aus dem IAM Identity Center-Identitätsspeicher übereinstimmt, um weitere Aktionen einer IAM-Rolle zu verhindern, die der Benutzer aktiv verwendet. Durch die Verwendung dieser Richtlinie werden Auswirkungen auf andere Benutzer vermieden, die bei der Bereitstellung der Ablehnungsrichtlinie möglicherweise denselben Berechtigungssatz verwenden. Diese Richtlinie verwendet die Platzhalter-Benutzer-ID *`Add user ID here`*,, für `"identitystore:userId"` die Sie die Benutzer-ID aktualisieren, für die Sie den Zugriff widerrufen möchten.

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

```
        {
            "Effect": "Deny",
            "Action": [
                "*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "identitystore:userId": "Add user ID here"
                }
            }
        }
    ]
}
```

Sie könnten zwar einen anderen Bedingungsschlüssel wie“`aws:userId`”, verwenden, “`identitystore:userId`” ist aber sicher, weil es sich um einen global eindeutigen Wert handelt, der einer Person zugeordnet ist. Die Verwendung “`aws:userId`” in der Bedingung kann davon abhängen, wie Benutzerattribute anhand Ihrer Identitätsquelle synchronisiert werden, und kann sich ändern, wenn sich der Benutzername oder die E-Mail-Adresse des Benutzers ändert.

In der IAM Identity Center-Konsole können Sie nach Benutzern suchen, `identitystore:userId` indem Sie zu Benutzer navigieren, anhand des Namens nach dem Benutzer suchen, den Abschnitt Allgemeine Informationen erweitern und die Benutzer-ID kopieren. Es ist auch praktisch, die AWS Access-Portal-Sitzung eines Benutzers zu beenden und seinen Anmeldezugriff im selben Abschnitt zu deaktivieren, während Sie nach der Benutzer-ID suchen. Sie können den Prozess zur Erstellung einer Ablehnungsrichtlinie automatisieren, indem Sie die Benutzer-ID des Benutzers durch Abfragen der Identitätsspeicher-APIs abrufen.

Bereitstellen der Ablehnungsrichtlinie

Sie können eine ungültige Platzhalter-Benutzer-ID verwenden, z. B. *`Add user ID here`* um die Ablehnungsrichtlinie im Voraus mithilfe einer Service Control Policy (SCP) bereitzustellen, die Sie an die AWS-Konten Benutzer anhängen, auf die sie möglicherweise Zugriff haben. Dieser Ansatz wird aufgrund seiner einfachen und schnellen Wirkung empfohlen. Wenn Sie einem Benutzer den Zugriff mit der Richtlinie „Verweigern“ entziehen, bearbeiten Sie die Richtlinie so, dass die Platzhalter-Benutzer-ID durch die Benutzer-ID der Person ersetzt wird, deren Zugriff Sie widerrufen möchten. Dadurch wird verhindert, dass der Benutzer mit beliebigen Berechtigungen in jedem Konto, das Sie dem SCP zuordnen, Aktionen ausführt. Es blockiert die Aktionen des Benutzers, auch wenn er seine Active AWS Access-Portal-Sitzung verwendet, um zu verschiedenen Konten zu navigieren

und verschiedene Rollen anzunehmen. Wenn der Zugriff des Benutzers durch den SCP vollständig gesperrt ist, können Sie ihm dann die Möglichkeit nehmen, sich anzumelden, seine Zuweisungen zu widerrufen und seine AWS Access-Portal-Sitzung bei Bedarf zu beenden.

Als Alternative zur Verwendung von SCPs können Sie die Richtlinie „Verweigern“ auch in die Inline-Richtlinie für Berechtigungssätze und in vom Kunden verwaltete Richtlinien aufnehmen, die von den Berechtigungssätzen verwendet werden, auf die der Benutzer zugreifen kann.

Wenn Sie den Zugriff für mehr als eine Person widerrufen müssen, können Sie eine Werteliste im Bedingungsblock verwenden, z. B.:

```
        "Condition": {
                "StringEquals": {
                    "identitystore:userId": [" user1 userId", "user2 userId"...]
                    }
    }
```

> **Important**
>
> Unabhängig von der Methode (n), die Sie verwenden, müssen Sie alle anderen Korrekturmaßnahmen ergreifen und die Benutzer-ID des Benutzers mindestens 12 Stunden lang in der Richtlinie behalten. Danach laufen alle Rollen ab, die der Benutzer angenommen hat, und Sie können seine Benutzer-ID dann aus der Ablehnungsrichtlinie entfernen.

Referenzieren von Berechtigungssätzen in Ressourcenrichtlinien, Amazon EKS und AWS KMS

Wenn Sie einem AWS Konto einen Berechtigungssatz zuweisen, erstellt IAM Identity Center eine Rolle mit einem Namen, der mit beginnt. `AWSReservedSSO_`

Der vollständige Name und der Amazon-Ressourcenname (ARN) für die Rolle verwenden das folgende Format:

Name	ARN
`AWSReservedSSO_` *`permission-set-name_unique-suffix`*	`arn:aws:iam::` *`aws-account-ID`*`:role/aws-reserved/sso.amaz`

Name	ARN
	onaws.com/ *aws-region* /AWSReservedSSO_ *permission-set-name_unique-suffix*

Wenn Sie beispielsweise einen Berechtigungssatz erstellen, der Datenbankadministratoren AWS Kontozugriff gewährt, wird eine entsprechende Rolle mit dem folgenden Namen und ARN erstellt:

Name	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

Wenn Sie alle Zuweisungen zu diesem Berechtigungssatz im AWS Konto löschen, wird die entsprechende Rolle, die IAM Identity Center erstellt hat, ebenfalls gelöscht. Wenn Sie demselben Berechtigungssatz später eine neue Zuweisung zuweisen, erstellt IAM Identity Center eine neue Rolle für den Berechtigungssatz. Der Name und der ARN der neuen Rolle enthalten ein anderes, eindeutiges Suffix. In diesem Beispiel lautet das eindeutige Suffix abcdef0123456789.

Name	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

Die Änderung des Suffixes im neuen Namen und ARN für die Rolle hat zur Folge, dass alle Richtlinien, die auf den ursprünglichen Namen und den ARN verweisen, unverändert bleiben out-of-date, wodurch der Zugriff für Personen, die den entsprechenden Berechtigungssatz verwenden, unterbrochen wird. Beispielsweise wird durch eine Änderung des ARN für die Rolle der Zugriff für

Benutzer des Berechtigungssatzes unterbrochen, wenn in den folgenden Konfigurationen auf den ursprünglichen ARN verwiesen wird:

- In der `aws-auth ConfigMap` Datei für Amazon Elastic Kubernetes Service (Amazon EKS)
- In einer ressourcenbasierten Richtlinie für einen AWS Key Management Service () -Schlüssel.AWS KMS Diese Richtlinie wird auch als Schlüsselrichtlinie bezeichnet.

Sie können zwar ressourcenbasierte Richtlinien für die meisten AWS Services aktualisieren, um auf einen neuen ARN für eine Rolle zu verweisen, die einem Berechtigungssatz entspricht, aber Sie müssen über eine Backup-Rolle verfügen, die Sie in IAM für Amazon EKS erstellen und AWS KMS falls sich der ARN ändert. Für Amazon EKS muss die Backup-IAM-Rolle in der `aws-auth ConfigMap` vorhanden sein. Denn AWS KMS sie muss in Ihren wichtigsten Richtlinien enthalten sein. Wenn Sie in beiden Fällen keine Backup-IAM-Rolle haben, müssen Sie sich an uns wenden AWS Support.

Empfehlungen zur Vermeidung von Zugriffsunterbrechungen

Um Zugriffsunterbrechungen aufgrund von Änderungen im ARN für eine Rolle zu vermeiden, die einem Berechtigungssatz entspricht, empfehlen wir Ihnen, wie folgt vorzugehen.

- Behalten Sie mindestens eine Berechtigungssatzzuweisung bei.

  Behalten Sie diese Zuweisung in den AWS Konten bei, die die Rollen enthalten, auf die Sie in den `aws-auth ConfigMap` für Amazon EKS, in den wichtigsten Richtlinien in AWS KMS oder in den ressourcenbasierten Richtlinien für andere verweisen. AWS-Services

  Wenn Sie beispielsweise einen `EKSAccess` Berechtigungssatz erstellen und auf den entsprechenden Rollen-ARN aus dem AWS Konto verweisen`111122223333`, weisen Sie dem Berechtigungssatz in diesem Konto dauerhaft eine administrative Gruppe zu. Da die Zuweisung dauerhaft ist, löscht IAM Identity Center die entsprechende Rolle nicht, wodurch das Risiko einer Umbenennung entfällt. Die administrative Gruppe hat immer Zugriff, ohne dass das Risiko einer Rechteerweiterung besteht.
- Für Amazon EKS und AWS KMS: Fügen Sie eine in IAM erstellte Rolle hinzu.

  Wenn Sie auf Rollen-ARNs für Berechtigungssätze in einem `aws-auth ConfigMap` Amazon EKS-Cluster oder in Schlüsselrichtlinien für AWS KMS Schlüssel verweisen, empfehlen wir, dass Sie auch mindestens eine Rolle angeben, die Sie in IAM erstellen. Die Rolle muss Ihnen den Zugriff auf den Amazon EKS-Cluster oder die Verwaltung der AWS KMS Schlüsselrichtlinie

ermöglichen. Der Berechtigungssatz muss in der Lage sein, diese Rolle anzunehmen. Auf diese Weise können Sie den Verweis auf den ARN in der AWS KMS Schlüsselrichtlinie `aws-auth ConfigMap` oder aktualisieren, wenn sich der Rollen-ARN für einen Berechtigungssatz ändert. Der nächste Abschnitt enthält ein Beispiel dafür, wie Sie eine Vertrauensrichtlinie für eine Rolle erstellen können, die in IAM erstellt wurde. Die Rolle kann nur durch einen `AdministratorAccess` Berechtigungssatz übernommen werden.

Beispiel für eine benutzerdefinierte Vertrauensrichtlinie

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Vertrauensrichtlinie, die einem `AdministratorAccess` Berechtigungssatz Zugriff auf eine in IAM erstellte Rolle gewährt. Zu den wichtigsten Elementen dieser Richtlinie gehören:

- Das Hauptelement dieser Vertrauensrichtlinie legt einen AWS Kontohauptmann fest. In dieser Richtlinie können Prinzipale im AWS Konto `111122223333` mit `sts:AssumeRole` Berechtigungen die Rolle übernehmen, die in IAM erstellt wurde.
- Diese Vertrauensrichtlinie legt zusätzliche Anforderungen für Prinzipale fest, die die in IAM erstellte Rolle übernehmen können. `Condition element` In dieser Richtlinie kann der Berechtigungssatz mit der folgenden Rolle ARN die Rolle übernehmen.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> Das `Condition` Element enthält den `ArnLike` Bedingungsoperator und verwendet einen Platzhalter am Ende des ARN der Berechtigungssatzrolle anstelle eines eindeutigen Suffixes. Das bedeutet, dass die Richtlinie es dem Berechtigungssatz ermöglicht, die in IAM erstellte Rolle anzunehmen, auch wenn sich der Rollen-ARN für den Berechtigungssatz ändert.

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

```
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

Wenn Sie eine Rolle, die Sie in IAM erstellen, in eine solche Richtlinie aufnehmen, erhalten Sie Notfallzugriff auf Ihre Amazon EKS-Cluster oder andere AWS Ressourcen AWS KMS keys, falls ein Berechtigungssatz oder alle Zuweisungen zum Berechtigungssatz versehentlich gelöscht und neu erstellt werden.

Attributbasierte Zugriffskontrolle

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. Sie können IAM Identity Center verwenden, um den Zugriff auf Ihre AWS Ressourcen über mehrere hinweg zu verwalten, indem Sie Benutzerattribute AWS-Konten verwenden, die aus einer beliebigen IAM Identity Center-Identitätsquelle stammen. In AWS werden diese Attribute als Tags bezeichnet. Durch die Verwendung von Benutzerattributen als Stichwörter können Sie den Prozess der Erstellung detaillierter Berechtigungen vereinfachen AWS und sicherstellen, dass Ihre Mitarbeiter nur auf die AWS Ressourcen zugreifen können, die über die entsprechenden Tags verfügen. AWS

Sie können beispielsweise den Entwicklern Bob und Sally, die aus zwei verschiedenen Teams stammen, demselben Berechtigungssatz in IAM Identity Center zuweisen und dann das Teamnamenattribut für die Zugriffskontrolle auswählen. Wenn Bob und Sally sich bei ihrem anmelden AWS-Konten, sendet IAM Identity Center ihr Teamnamenattribut in der AWS Sitzung, sodass Bob und Sally nur dann auf AWS Projektressourcen zugreifen können, wenn ihr Teamnamenattribut mit dem Teamnamen-Tag auf der Projektressource übereinstimmt. Wenn Bob in future zu Sallys Team wechselt, können Sie seinen Zugriff ändern, indem Sie einfach sein Teamnamenattribut im Unternehmensverzeichnis aktualisieren. Wenn Bob sich das nächste Mal anmeldet, erhält er

automatisch Zugriff auf die Projektressourcen seines neuen Teams, ohne dass die Berechtigungen aktualisiert werden müssen. AWS

Dieser Ansatz trägt auch dazu bei, die Anzahl der unterschiedlichen Berechtigungen zu reduzieren, die Sie in IAM Identity Center erstellen und verwalten müssen, da Benutzer, denen dieselben Berechtigungssätze zugeordnet sind, nun anhand ihrer Attribute über eindeutige Berechtigungen verfügen können. Sie können diese Benutzerattribute in IAM Identity Center-Berechtigungssätzen und ressourcenbasierten Richtlinien verwenden, um ABAC für AWS Ressourcen zu implementieren und die Berechtigungsverwaltung in großem Umfang zu vereinfachen.

Vorteile

Im Folgenden sind weitere Vorteile der Verwendung von ABAC in IAM Identity Center aufgeführt.

- ABAC benötigt weniger Berechtigungssätze — Da Sie nicht unterschiedliche Richtlinien für verschiedene Jobfunktionen erstellen müssen, erstellen Sie weniger Berechtigungssätze. Dies reduziert die Komplexität Ihrer Berechtigungsverwaltung.
- Mit ABAC können sich Teams schnell ändern und wachsen — Berechtigungen für neue Ressourcen werden automatisch auf der Grundlage von Attributen erteilt, wenn Ressourcen bei der Erstellung entsprechend gekennzeichnet werden.
- Verwenden Sie Mitarbeiterattribute aus Ihrem Unternehmensverzeichnis mit ABAC — Sie können vorhandene Mitarbeiterattribute aus jeder in IAM Identity Center konfigurierten Identitätsquelle verwenden, um Entscheidungen zur Zugriffskontrolle in zu treffen. AWS
- Nachverfolgen, wer auf Ressourcen zugreift — Sicherheitsadministratoren können die Identität einer Sitzung auf einfache Weise ermitteln, indem sie die Benutzerattribute überprüfen, um die Benutzeraktivitäten in AWS CloudTrail zu verfolgen. AWS

Informationen zur Konfiguration von ABAC mithilfe der IAM Identity Center-Konsole finden Sie unter. Attribute für Zugriffskontrolle Informationen zur Aktivierung und Konfiguration von ABAC mithilfe der IAM Identity Center-APIs finden Sie CreateInstanceAccessControlAttributeConfigurationim IAM Identity Center API-Referenzhandbuch.

Themen

- Checkliste: Konfiguration von ABAC mithilfe von IAM Identity Center AWS
- Attribute für Zugriffskontrolle

Checkliste: Konfiguration von ABAC mithilfe von IAM Identity Center AWS

Diese Checkliste enthält die Konfigurationsaufgaben, die zur Vorbereitung Ihrer AWS Ressourcen und zur Einrichtung von IAM Identity Center für den ABAC-Zugriff erforderlich sind. Führen Sie die Aufgaben in dieser Checkliste der Reihe nach aus. Wenn Sie über einen Referenzlink zu einem Thema gelangen, kehren Sie zu diesem Thema zurück, damit Sie mit den verbleibenden Aufgaben in dieser Checkliste fortfahren können.

Schritt	Aufgabe	Referenz
1	Lesen Sie, wie Sie Tags zu all Ihren AWS Ressourcen hinzufügen können. Um ABAC in IAM Identity Center zu implementieren, müssen Sie zunächst Tags zu all Ihren AWS Ressourcen hinzufügen, für die Sie ABAC implementieren möchten.	• Ressourcen taggen AWS
2	Erfahren Sie, wie Sie Ihre Identitätsquelle in IAM Identity Center mit den zugehörigen Benutzeridentitäten und Attributen in Ihrem Identitätsspeicher konfigurieren. Mit IAM Identity Center können Sie Benutzerattribute aus jeder unterstützten IAM Identity Center-Identitätsquelle für ABAC in verwenden. AWS	• Verwalte deine Identitätsquelle
3	Ermitteln Sie anhand der folgenden Kriterien, welche Attribute Sie für Entscheidungen zur Zugriffskontrolle verwenden möchten, AWS und senden Sie sie an IAM Identity Center.	• Erste Schritte
	• Wenn Sie einen externen Identitätsanbieter (IdP) verwenden, entscheiden Sie, ob Sie vom IdP übergebene Attribute verwenden oder Attribute aus IAM Identity Center auswählen möchten.	• Auswahl von Attributen, wenn Sie einen externen Identitätsanbieter als Identitätsquelle verwenden
	• Wenn Sie festlegen, dass Ihr IdP Attribute sendet, konfigurieren Sie Ihren IdP so, dass er die Attribute in SAML-Assertionen überträgt. Sehen Sie sich die `Optional` Abschnitte im Tutorial für Ihren spezifischen IdP an.	• Erste Schritte mit Tutorials

Schritt	Aufgabe	Referenz
	• Wenn Sie einen IdP als Identitätsquelle verwenden und Attribute in IAM Identity Center auswählen , sollten Sie untersuchen, wie SCIM konfiguriert werden kann, sodass die Attributwerte von Ihrem IdP stammen. Wenn Sie SCIM nicht mit Ihrem IdP verwenden können, fügen Sie die Benutzer und ihre Attribute über die Benutzerseite der IAM Identity Center-Konsole hinzu.	• Automatische Bereitstellung • Unterstützte externe Identitätsanbieterattribute
	• Wenn Sie Active Directory oder IAM Identity Center als Identitätsquelle verwenden oder einen IdP verwenden und Attribute in IAM Identity Center auswählen, überprüfen Sie die verfügbaren Attribute , die Sie konfigurieren können. Fahren Sie dann sofort mit Schritt 4 fort, um mit der Konfiguration Ihrer ABAC-Attribute über die IAM Identity Center-Konsole zu beginnen.	• Auswahl von Attribute n, wenn Sie IAM Identity Center als Identitätsquelle verwenden • Auswahl von Attributen bei Verwendung AWS Managed Microsoft AD als Identität squelle • Standardzuordnungen
4	Wählen Sie auf der Seite „Attribute für die Zugriffsk ontrolle“ in der IAM Identity Center-Konsole die Attribute aus, die für ABAC verwendet werden sollen. Auf dieser Seite können Sie Attribute für die Zugriffskontrolle aus der Identitätsquelle auswählen, die Sie in Schritt 2 konfiguriert haben. Nachdem sich Ihre Identitäten und ihre Attribute im IAM Identity Center befinden, müssen Sie Schlüssel-Wert-Paare (Zuordnungen) erstellen, die Ihnen AWS-Konten zur Verwendung bei Entscheid ungen zur Zugriffskontrolle übergeben werden.	• Aktivieren und konfigurieren Sie Attribute für die Zugriffsk ontrolle

Schritt	Aufgabe	Referenz
5	Erstellen Sie benutzerdefinierte Berechtigungsrichtlinien innerhalb Ihres Berechtigungssatzes und verwenden Sie Zugriffskontrollattribute, um ABAC-Regeln zu erstellen, sodass Benutzer nur auf Ressourcen mit passenden Tags zugreifen können. Benutzerattribute, die Sie in Schritt 4 konfiguriert haben, werden als Tags AWS für Entscheidungen zur Zugriffskontrolle verwendet. Mithilfe der `aws:PrincipalTag/key` Bedingung können Sie auf die Attribute der Zugriffsk ontrolle in der Berechtigungsrichtlinie verweisen.	• Erstellen Sie im IAM Identity Center Berechtigungsricht linien für ABAC
6	Weisen Sie in Ihren verschiedenen AWS-Konten Fällen Benutzer den in Schritt 5 erstellten Berechtigungssätze n zu. Auf diese Weise wird sichergestellt, dass sie, wenn sie sich mit ihren Konten verbinden und auf AWS Ressourcen zugreifen, nur auf der Grundlage übereinst immender Stichwörter Zugriff erhalten.	• Weisen Sie Benutzerzugriff zu AWS-Konten

Nachdem Sie diese Schritte abgeschlossen haben, erhalten Benutzer, die Single Sign-On AWS-Konto verwenden, Zugriff auf ihre AWS Ressourcen, basierend auf den entsprechenden Attributen.

Attribute für Zugriffskontrolle

Attribute für die Zugriffskontrolle ist der Name der Seite in der IAM Identity Center-Konsole, auf der Sie Benutzerattribute auswählen, die Sie in Richtlinien zur Steuerung des Zugriffs auf Ressourcen verwenden möchten. Sie können Benutzer Workloads auf der AWS Grundlage vorhandener Attribute in der Identitätsquelle der Benutzer zuweisen.

Nehmen wir beispielsweise an, Sie möchten den Zugriff auf S3-Buckets anhand von Abteilungsnamen zuweisen. Auf der Seite „Attribute für die Zugriffskontrolle“ wählen Sie das Benutzerattribut „Abteilung“ für die Verwendung mit der attributebasierten Zugriffskontrolle (ABAC) aus. Im IAM Identity Center-Berechtigungssatz schreiben Sie dann eine Richtlinie, die Benutzern nur dann Zugriff gewährt, wenn das Abteilungsattribut mit dem Abteilungs-Tag übereinstimmt, das Sie Ihren S3-Buckets zugewiesen haben. IAM Identity Center übergibt das Abteilungsattribut des Benutzers an das Konto, auf das zugegriffen wird. Das Attribut wird dann verwendet, um den

Zugriff auf der Grundlage der Richtlinie zu bestimmen. Weitere Informationen zu ABAC finden Sie unterAttributbasierte Zugriffskontrolle.

Erste Schritte

Wie Sie mit der Konfiguration von Attributen für die Zugriffskontrolle beginnen, hängt davon ab, welche Identitätsquelle Sie verwenden. Unabhängig von der ausgewählten Identitätsquelle müssen Sie, nachdem Sie Ihre Attribute ausgewählt haben, Richtlinien für Berechtigungssätze erstellen oder bearbeiten. Diese Richtlinien müssen Benutzeridentitäten Zugriff auf AWS Ressourcen gewähren.

Auswahl von Attributen, wenn Sie IAM Identity Center als Identitätsquelle verwenden

Wenn Sie IAM Identity Center als Identitätsquelle konfigurieren, fügen Sie zunächst Benutzer hinzu und konfigurieren deren Attribute. Navigieren Sie anschließend zur Seite „Attribute für die Zugriffskontrolle“ und wählen Sie die Attribute aus, die Sie in Richtlinien verwenden möchten. Navigieren Sie abschließend zu der AWS-KontenSeite, auf der Sie Berechtigungssätze für die Verwendung der Attribute für ABAC erstellen oder bearbeiten können.

Auswahl von Attributen bei Verwendung AWS Managed Microsoft AD als Identitätsquelle

Wenn Sie IAM Identity Center AWS Managed Microsoft AD als Identitätsquelle konfigurieren, ordnen Sie zunächst eine Reihe von Attributen aus Active Directory den Benutzerattributen in IAM Identity Center zu. Navigieren Sie anschließend zur Seite „Attribute für die Zugriffskontrolle“. Wählen Sie dann auf der Grundlage des vorhandenen Satzes von SSO-Attributen, die aus Active Directory zugeordnet wurden, aus, welche Attribute in Ihrer ABAC-Konfiguration verwendet werden sollen. Verfassen Sie abschließend ABAC-Regeln mithilfe der Zugriffskontrollattribute in Berechtigungssätzen, um Benutzeridentitäten Zugriff auf Ressourcen zu gewähren. AWS Eine Liste der Standardzuordnungen von Benutzerattributen in IAM Identity Center zu den Benutzerattributen in Ihrem Verzeichnis finden Sie unter. AWS Managed Microsoft AD Standardzuordnungen

Auswahl von Attributen, wenn Sie einen externen Identitätsanbieter als Identitätsquelle verwenden

Wenn Sie IAM Identity Center mit einem externen Identitätsanbieter (IdP) als Identitätsquelle konfigurieren, gibt es zwei Möglichkeiten, Attribute für ABAC zu verwenden.

- Sie können Ihren IdP so konfigurieren, dass er die Attribute über SAML-Assertionen sendet. In diesem Fall leitet IAM Identity Center den Attributnamen und den Wert vom IdP zur Richtlinienbewertung weiter.

> **Note**
>
> Attribute in SAML-Assertionen sind für Sie auf der Seite „Attribute für die Zugriffskontrolle“ nicht sichtbar. Sie müssen diese Attribute im Voraus kennen und sie zu den Zugriffskontrollregeln hinzufügen, wenn Sie Richtlinien erstellen. Wenn Sie sich dafür entscheiden, Ihren externen IdPs Attributen zu vertrauen, werden diese Attribute immer weitergegeben, wenn sich Benutzer AWS-Konten zusammenschließen. In Szenarien, in denen dieselben Attribute über SAML und SCIM in IAM Identity Center übertragen werden, hat der Wert der SAML-Attribute bei Entscheidungen zur Zugriffskontrolle Vorrang.

- Sie können auf der Seite Attribute für die Zugriffskontrolle in der IAM Identity Center-Konsole konfigurieren, welche Attribute Sie verwenden. Die Attributwerte, die Sie hier auswählen, ersetzen die Werte für alle passenden Attribute, die über eine Assertion von einem IdP stammen. Je nachdem, ob Sie SCIM verwenden, sollten Sie Folgendes beachten:
  - Bei Verwendung von SCIM synchronisiert der IdP die Attributwerte automatisch mit dem IAM Identity Center. Zusätzliche Attribute, die für die Zugriffskontrolle erforderlich sind, sind möglicherweise nicht in der Liste der SCIM-Attribute enthalten. In diesem Fall sollten Sie in Erwägung ziehen, mit dem IT-Administrator in Ihrem IdP zusammenzuarbeiten, um solche Attribute über SAML-Assertionen mit dem erforderlichen Präfix an das IAM Identity Center zu senden. `https://aws.amazon.com/SAML/Attributes/AccessControl:` Informationen zur Konfiguration von Benutzerattributen für die Zugriffskontrolle in Ihrem IdP zum Senden über SAML-Assertionen finden Sie unter Erste Schritte mit Tutorials Für Ihren IdP.
  - Wenn Sie SCIM nicht verwenden, müssen Sie die Benutzer manuell hinzufügen und ihre Attribute so festlegen, als ob Sie IAM Identity Center als Identitätsquelle verwenden würden. Navigieren Sie als Nächstes zur Seite „Attribute für die Zugriffskontrolle“ und wählen Sie die Attribute aus, die Sie in Richtlinien verwenden möchten.

Eine vollständige Liste der unterstützten Attribute für Benutzerattribute in IAM Identity Center für die Benutzerattribute in Ihrem externen IdPs System finden Sie unterUnterstützte externe Identitätsanbieterattribute.

Informationen zu den ersten Schritten mit ABAC in IAM Identity Center finden Sie in den folgenden Themen.

Themen

- Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle

- Erstellen Sie im IAM Identity Center Berechtigungsrichtlinien für ABAC

Aktivieren und konfigurieren Sie Attribute für die Zugriffskontrolle

Um ABAC in allen Fällen verwenden zu können, müssen Sie ABAC zunächst über die IAM Identity Center-Konsole oder die IAM Identity Center-API aktivieren. Wenn Sie IAM Identity Center zur Auswahl von Attributen verwenden möchten, verwenden Sie die Seite „Attribute für die Zugriffskontrolle“ in der IAM Identity Center-Konsole oder die IAM Identity Center-API. Wenn Sie einen externen Identitätsanbieter (IdP) als Identitätsquelle verwenden und sich dafür entscheiden, Attribute über die SAML-Assertionen zu senden, konfigurieren Sie Ihren IdP so, dass er die Attribute weitergibt. Wenn eine SAML-Zusicherung eins dieser Attribute übergibt, ersetzt IAM Identity Center den Attributwert durch den Wert aus dem IAM Identity Center-Identitätsspeicher. Nur in IAM Identity Center konfigurierte Attribute werden gesendet, um Entscheidungen zur Zugriffskontrolle zu treffen, wenn Benutzer sich zu ihren Konten zusammenschließen.

> **Note**
>
> Sie können die von einem externen IdP konfigurierten und gesendeten Attribute nicht auf der Seite Attribute für die Zugriffskontrolle in der IAM Identity Center-Konsole anzeigen. Wenn Sie Zugriffskontrollattribute in den SAML-Assertionen von Ihrem externen IdP übergeben, werden diese Attribute direkt an den gesendet, AWS-Konto wenn sich Benutzer zusammenschließen. Die Attribute werden in IAM Identity Center nicht für die Zuordnung verfügbar sein.

Aktivieren Sie Attribute für die Zugriffskontrolle

Gehen Sie wie folgt vor, um die Funktion zur Steuerung der Attribute für den Zugriff (ABAC) mithilfe der IAM Identity Center-Konsole zu aktivieren.

> **Note**
>
> Wenn Sie bereits über Berechtigungssätze verfügen und ABAC in Ihrer IAM Identity Center-Instance aktivieren möchten, müssen Sie für zusätzliche Sicherheitseinschränkungen zunächst über die Richtlinie verfügen. `iam:UpdateAssumeRolePolicy` Diese zusätzlichen Sicherheitseinschränkungen sind nicht erforderlich, wenn Sie in Ihrem Konto keine Berechtigungssätze erstellt haben.

Um Attribute für die Zugriffskontrolle zu aktivieren

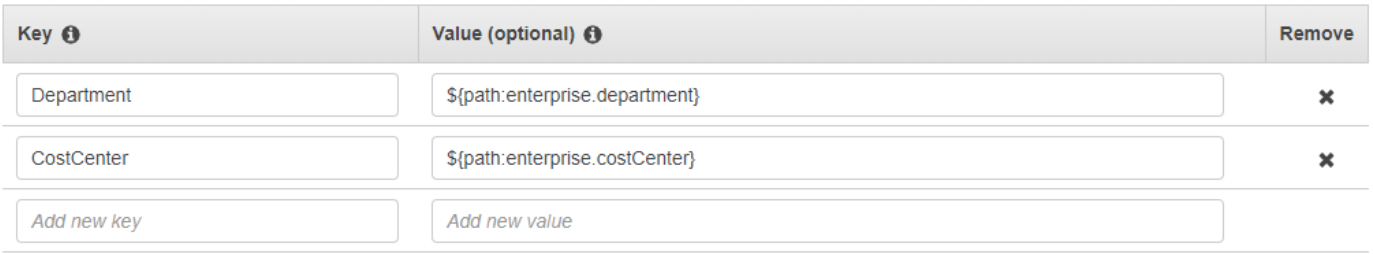
1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Einstellungen
3. Suchen Sie auf der Seite Einstellungen das Informationsfeld Attribute für die Zugriffskontrolle und wählen Sie dann Aktivieren aus. Fahren Sie mit dem nächsten Verfahren fort, um es zu konfigurieren.

Wählen Sie Ihre Attribute

Gehen Sie wie folgt vor, um Attribute für Ihre ABAC-Konfiguration einzurichten.

So wählen Sie Ihre Attribute mit der IAM Identity Center-Konsole aus

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Einstellungen
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Attribute für die Zugriffskontrolle und dann Attribute verwalten aus.
4. Wählen Sie auf der Seite „Attribute für die Zugriffskontrolle“ die Option „Attribut hinzufügen“ und geben Sie die Schlüssel - und Wertdetails ein. Hier ordnen Sie das aus Ihrer Identitätsquelle stammende Attribut einem Attribut zu, das IAM Identity Center als Sitzungs-Tag weitergibt.



   Key steht für den Namen, den Sie dem Attribut zur Verwendung in Richtlinien geben. Dies kann ein beliebiger Name sein, aber Sie müssen diesen genauen Namen in den Richtlinien angeben, die Sie für die Zugriffskontrolle erstellen. Nehmen wir zum Beispiel an, dass Sie Okta (einen externen IdP) als Identitätsquelle verwenden und die Kostenstellendaten Ihrer Organisation als Sitzungs-Tags weitergeben müssen. Im Feld Schlüssel würden Sie einen ähnlich passenden Namen CostCenterwie Ihren Schlüsselnamen eingeben. Es ist wichtig zu beachten, dass unabhängig davon, welchen Namen Sie hier wählen, er auch in Ihrem Namen `aws:PrincipalTag-Bedingungsschlüssel` (das heißt,`"ec2:ResourceTag/`

`CostCenter": "${aws:PrincipalTag/CostCenter}"`) exakt den gleichen Namen haben muss.

> **Note**
>
> Verwenden Sie ein Attribut mit einem einzigen Wert für Ihren Schlüssel, zum Beispiel. **`Manager`** IAM Identity Center unterstützt keine mehrwertigen Attribute für ABAC, zum Beispiel. **`Manager, IT Systems`**

Der Wert steht für den Inhalt des Attributs, das aus Ihrer konfigurierten Identitätsquelle stammt. Hier können Sie einen beliebigen Wert aus der entsprechenden Identitätsquellentabelle eingeben, die unter aufgeführt istAttributzuordnungen für AWS Managed Microsoft AD das Verzeichnis. Wenn Sie beispielsweise den Kontext aus dem oben genannten Beispiel verwenden, überprüfen Sie die Liste der unterstützten IdP-Attribute und stellen fest, dass ein unterstütztes Attribut am ehesten übereinstimmt, **`${path:enterprise.costCenter}`**und geben Sie es dann in das Feld Wert ein. Sehen Sie sich den obigen Screenshot als Referenz an. Beachten Sie, dass Sie externe IdP-Attributwerte außerhalb dieser Liste für ABAC nicht verwenden können, es sei denn, Sie verwenden die Option, Attribute über die SAML-Assertion zu übergeben.

5. Wählen Sie Änderungen speichern aus.

Nachdem Sie die Zuordnung Ihrer Zugriffskontrollattribute konfiguriert haben, müssen Sie den ABAC-Konfigurationsprozess abschließen. Erstellen Sie dazu Ihre ABAC-Regeln und fügen Sie sie Ihren Berechtigungssätzen und/oder ressourcenbasierten Richtlinien hinzu. Dies ist erforderlich, damit Sie Benutzeridentitäten Zugriff auf Ressourcen gewähren können. AWS Weitere Informationen finden Sie unter Erstellen Sie im IAM Identity Center Berechtigungsrichtlinien für ABAC.

Attribute für die Zugriffskontrolle deaktivieren

Gehen Sie wie folgt vor, um die ABAC-Funktion zu deaktivieren und alle konfigurierten Attributzuordnungen zu löschen.

Um Attribute für die Zugriffskontrolle zu deaktivieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Einstellungen

3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Attribute für die Zugriffskontrolle“ und dann „Deaktivieren“.
4. Überprüfen Sie im Dialogfeld „Attribute für Zugriffskontrolle deaktivieren“ die Informationen, geben Sie LÖSCHEN ein, und klicken Sie dann auf Bestätigen.

> **Important**
>
> In diesem Schritt werden alle konfigurierten Attribute gelöscht. Nach dem Löschen werden alle Attribute, die von einer Identitätsquelle empfangen wurden, und alle benutzerdefinierten Attribute, die Sie zuvor konfiguriert haben, nicht weitergegeben.

Erstellen Sie im IAM Identity Center Berechtigungsrichtlinien für ABAC

Sie können Berechtigungsrichtlinien erstellen, die anhand des konfigurierten Attributwerts festlegen, wer auf Ihre AWS Ressourcen zugreifen kann. Wenn Sie ABAC aktivieren und Attribute angeben, übergibt IAM Identity Center den Attributwert des authentifizierten Benutzers zur Verwendung bei der Richtlinienbewertung an IAM.

aws:PrincipalTag-Bedingungsschlüssel

Mithilfe des Bedingungsschlüssels können Sie Zugriffskontrollattribute in Ihren Berechtigungssätzen verwenden, um `aws:PrincipalTag` Zugriffskontrollregeln zu erstellen. In der folgenden Vertrauensrichtlinie können Sie beispielsweise alle Ressourcen in Ihrer Organisation mit ihren jeweiligen Kostenstellen kennzeichnen. Sie können auch einen einzigen Berechtigungssatz verwenden, der Entwicklern Zugriff auf ihre Kostenstellenressourcen gewährt. Wenn Entwickler sich nun mithilfe von Single Sign-On und ihrem Kostenstellenattribut mit dem Konto verbinden, erhalten sie nur Zugriff auf die Ressourcen in ihren jeweiligen Kostenstellen. Wenn das Team mehr Entwickler und Ressourcen zu seinem Projekt hinzufügt, müssen Sie nur Ressourcen mit der richtigen Kostenstelle taggen. Anschließend geben Sie Informationen zur Kostenstelle in der AWS Sitzung weiter, in der sich die Entwickler AWS-Konten zusammenschließen. Wenn das Unternehmen der Kostenstelle neue Ressourcen und Entwickler hinzufügt, können Entwickler Ressourcen entsprechend ihren Kostenstellen verwalten, ohne dass Genehmigungen aktualisiert werden müssen.

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter aws:PrincipalTagund EC2: Starten oder Stoppen von Instances auf der Grundlage übereinstimmender Principal- und Resource-Tags im IAM-Benutzerhandbuch.

Wenn Richtlinien ungültige Attribute in ihren Bedingungen enthalten, schlägt die Richtlinienbedingung fehl und der Zugriff wird verweigert. Weitere Informationen finden Sie unter Fehler „Ein unerwarteter Fehler ist aufgetreten“, wenn ein Benutzer versucht, sich mit einem externen Identitätsanbieter anzumelden.

IAM-Identitätsanbieter

Wenn Sie Single Sign-On-Zugriff zu einem hinzufügen AWS-Konto, erstellt IAM Identity Center in jedem einen IAM-Identitätsanbieter. AWS-Konto Ein IAM-Identitätsanbieter trägt zu Ihrer AWS-Konto Sicherheit bei, da Sie keine langfristigen Sicherheitsanmeldedaten wie Zugriffsschlüssel verteilen oder in Ihre Anwendung einbetten müssen.

Reparieren Sie den IAM-Identitätsanbieter

Wenn Sie Ihren Identitätsanbieter versehentlich löschen oder ändern, müssen Sie Ihre Benutzer- und Gruppenzuweisungen manuell erneut anwenden. Durch erneutes Anwenden Ihrer Benutzer- und Gruppenzuweisungen wird der Identity Provider neu erstellt. Weitere Informationen finden Sie hier:

- Zugriff verwalten auf AWS-Konten
- Zugriff auf Anwendungen verwalten

Service-verknüpfte Rollen

Dienstbezogene Rollen sind vordefinierte IAM-Berechtigungen, die es IAM Identity Center ermöglichen, zu delegieren und durchzusetzen, auf welche Benutzer in Ihrem Unternehmen Single Sign-On-Zugriff haben. AWS-Konten AWS Organizations Der Service ermöglicht diese Funktionalität, indem er in jeder Rolle innerhalb der Organisation eine dienstbezogene Rolle bereitstellt. AWS-Konto Der Dienst ermöglicht es dann anderen AWS Diensten wie IAM Identity Center, diese Rollen zur Ausführung dienstbezogener Aufgaben zu nutzen. Weitere Informationen finden Sie unter Rollen im Zusammenhang mit AWS Organizations Diensten.

Wenn Sie IAM Identity Center aktivieren, erstellt IAM Identity Center eine dienstverknüpfte Rolle für alle Konten innerhalb der Organisation in. AWS Organizations IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen. Weitere Informationen finden Sie unter Zugriff verwalten auf AWS-Konten.

Mit Diensten verknüpfte Rollen, die in den einzelnen Rollen erstellt werden, AWS-Konto sind benannt. `AWSServiceRoleForSSO` Weitere Informationen finden Sie unter Verwendung von serviceverknüpften Rollen für IAM Identity Center.

Zugriff auf Anwendungen verwalten

Mit können Sie steuern AWS IAM Identity Center, wer Single Sign-On-Zugriff auf Ihre Anwendungen haben kann. Benutzer erhalten nahtlosen Zugriff auf diese Anwendungen, nachdem sie sich mit ihren Verzeichnisanmeldedaten angemeldet haben.

IAM Identity Center kommuniziert sicher mit diesen Anwendungen über eine vertrauenswürdige Beziehung zwischen IAM Identity Center und dem Dienstanbieter der Anwendung. Dieses Vertrauen kann je nach Anwendungstyp auf unterschiedliche Weise hergestellt werden.

IAM Identity Center unterstützt zwei Anwendungstypen: AWS verwaltete Anwendungen und vom Kunden verwaltete Anwendungen. AWS verwaltete Anwendungen werden direkt in den entsprechenden Anwendungskonsolen oder über die Anwendungs-APIs konfiguriert. Vom Kunden verwaltete Anwendungen müssen der IAM Identity Center-Konsole hinzugefügt und mit den entsprechenden Metadaten sowohl für IAM Identity Center als auch für den Service Provider konfiguriert werden.

Nachdem Sie die Anwendungen für die Zusammenarbeit mit IAM Identity Center konfiguriert haben, können Sie verwalten, welche Benutzer oder Gruppen auf die Anwendungen zugreifen. Standardmäßig sind Anwendungen keine Benutzer zugewiesen.

Sie können Ihren Mitarbeitern auch Zugriff auf die AWS Management Console für Ihre Organisation bestimmten AWS-Konto Daten gewähren. Weitere Informationen finden Sie unter Zugriff verwalten auf AWS-Konten.

Themen

AWS verwaltete Anwendungen

AWS verwaltete Anwendungen lassen sich in IAM Identity Center integrieren und können es für Authentifizierungs- und Verzeichnisdienste verwenden.

Durch die Integration AWS verwalteter Anwendungen mit IAM Identity Center können Sie Benutzerzugriff einfacher zuweisen, ohne dass Sie für jede Anwendung einen separaten Verbund oder eine Benutzer- und Gruppensynchronisierung einrichten müssen. Sie können die Identitätsquelle, die Sie für die Authentifizierung verwenden möchten, einmal verbinden, und Sie erhalten eine zentrale Ansicht der Benutzer- und Gruppenzuweisungen. Administratoren von Anwendungen, die die Verbreitung vertrauenswürdiger Identitäten ermöglichen, können den Zugriff auf ihre Anwendungsressourcen auf der Grundlage der Mitgliedschaft eines Benutzers oder seiner Gruppe definieren und prüfen, ohne sie IAM-Rollen zuordnen zu müssen.

AWS Verwaltete Anwendungen bieten eine administrative Benutzeroberfläche, mit der Sie den Zugriff auf Anwendungsressourcen verwalten können. Beispielsweise können QuickSight Administratoren Benutzern auf der Grundlage ihrer Gruppenmitgliedschaft den Zugriff auf Dashboards zuweisen. Die meisten AWS verwalteten Anwendungen bieten auch eine AWS Management Console Benutzeroberfläche, mit der Sie der Anwendung Benutzer zuweisen können. Die Konsolenoberfläche für diese Anwendungen kann beide Funktionen integrieren, um Funktionen zur Benutzerzuweisung mit der Fähigkeit zu kombinieren, den Zugriff auf Anwendungsressourcen zu verwalten.

AWS Zu den verwalteten Anwendungen, die in IAM Identity Center integriert sind, gehören:

AWS verwaltete Anwendungen, die in IAM Identity Center integriert sind

AWS verwaltete Anwendung	Integriert in die Organisationsinstanz von IAM Identity Center	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center
Amazon Athena SQL	 Ja	 Ja	 Ja

AWS verwaltete Anwendung	Integriert in die Organisationsinstanz von IAM Identity Center	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center
Amazon CodeCatalyst	 Ja	 Ja	 Nein
Amazon EMR-Notizbücher	 Ja	 N	 Nein
Amazon EMR auf Amazon EC2	 Ja	 Ja	 Ja
Amazon EMR Studio	 Ja	 Ja	 Ja
Amazon Kendra	 Ja	 N	 Nein
Amazon Managed Grafana	 Ja	 N	 Nein
Amazon Monitron	 Ja	 N	 Nein

AWS verwaltete Anwendung	Integriert in die Organisationsinstanz von IAM Identity Center	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center
Amazon Nimble Studio	 Ja	 N	 Nein
Amazon Pinpoint	 Ja	 N	 Nein
Amazon Q Business	 Ja	 Ja	 Nein
Amazon Q-Entwickler	 Ja	 Ja *	 Nein
Amazon QuickSight	 Ja	 Ja	 Ja
Amazon-Redshift	 Ja	 Ja	 Ja
Amazon S3 S3-Zugriffsberechtigungen	 Ja	 Ja	 Ja

AWS verwaltete Anwendung	Integriert in die Organisationsinstanz von IAM Identity Center	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center
Amazon SageMaker Studio	 Ja	 Nein	 Nein
Amazon WorkSpaces Web	 Ja	 Nein	 Nein
AWS CLI	 Ja	 Nein	 Nein
AWS Deadline Cloud	 Ja	 Ja	 Nein
AWS IoT Events	 Ja	 Nein	 Nein
AWS IoT Fleet Hub	 Ja	 Nein	 Nein
AWS IoT SiteWise	 Ja	 Nein	 Nein

AWS verwaltete Anwendung	Integriert in die Organisationsinstanz von IAM Identity Center	Integriert in Kontoinstanzen von IAM Identity Center	Ermöglicht die Verbreitung vertrauenswürdiger Identitäten über IAM Identity Center
AWS Lake Formation	 Ja	 Ja	 Ja
AWS Supply Chain	 Ja	 Nein	 Nein
AWS Systems Manager	 Ja	 Nein	 Nein
AWS Verified Access	 Ja	 Nein	 Nein

* Kontoinstanzen von IAM Identity Center werden unterstützt, es sei denn, Ihre Benutzer benötigen Zugriff auf Amazon Q in der AWS Konsole.

Themen

- Steuern des Zugriffs
- Koordination administrativer Aufgaben
- Konfiguration von IAM Identity Center für die gemeinsame Nutzung von Identitätsinformationen
- Überlegungen zum Teilen von Identitätsinformationen in AWS-Konten
- Aktivierung identitätsbewusster Konsolensitzungen
- Einschränkung der Nutzung verwalteter Anwendungen AWS
- Details zu einer AWS verwalteten Anwendung anzeigen

- Eine AWS verwaltete Anwendung deaktivieren

Steuern des Zugriffs

Der Zugriff auf AWS verwaltete Anwendungen wird auf zwei Arten gesteuert:

- Erster Zugriff auf die Anwendung — IAM Identity Center verwaltet diesen Zugriff über Zuweisungen an die Anwendung. Standardmäßig sind Zuweisungen für AWS verwaltete Anwendungen erforderlich.
- Zugriff auf Anwendungsressourcen — Die Anwendung verwaltet dies über unabhängige Ressourcenzuweisungen, die sie kontrolliert.

Koordination administrativer Aufgaben

Wenn Sie ein Anwendungsadministrator sind, können Sie wählen, ob Sie Zuweisungen zu einer Anwendung benötigen. Wenn Zuweisungen erforderlich sind, können bei der Anmeldung von Benutzern im AWS Access Portal nur Benutzer, die der Anwendung direkt oder über eine Gruppenzuweisung zugewiesen wurden, die Anwendungskachel anzeigen. Wenn keine Zuweisungen erforderlich sind, können Sie alternativ allen IAM Identity Center-Benutzern den Zugriff auf die Anwendung gestatten. In diesem Fall verwaltet die Anwendung den Zugriff auf Ressourcen und die Anwendungskachel ist für alle Benutzer sichtbar, die das AWS Zugriffsportal besuchen.

Wenn Sie ein IAM Identity Center-Administrator sind, können Sie die IAM Identity Center-Konsole verwenden, um Zuweisungen zu AWS verwalteten Anwendungen zu entfernen. Bevor Sie Zuweisungen entfernen, empfehlen wir, dass Sie sich mit dem Anwendungsadministrator abstimmen. Sie sollten sich auch mit dem Anwendungsadministrator abstimmen, wenn Sie beabsichtigen, die Einstellung zu ändern, die bestimmt, ob Zuweisungen erforderlich sind, oder Anwendungszuweisungen zu automatisieren.

Konfiguration von IAM Identity Center für die gemeinsame Nutzung von Identitätsinformationen

IAM Identity Center bietet einen Identitätsspeicher, der Benutzer- und Gruppenattribute mit Ausnahme von Anmeldeinformationen enthält. Sie können eine der folgenden Methoden verwenden, um die Benutzer und Gruppen in Ihrem IAM Identity Center-Identitätsspeicher auf dem neuesten Stand zu halten:

- Verwenden Sie den IAM Identity Center-Identitätsspeicher als Hauptidentitätsquelle. Wenn Sie diese Methode wählen, verwalten Sie Ihre Benutzer, ihre Anmeldeinformationen und Gruppen von der IAM Identity Center-Konsole aus oder AWS Command Line Interface ().AWS CLI Weitere Informationen finden Sie unter Identitäten im IAM Identity Center verwalten.
- Richten Sie die Bereitstellung (Synchronisation) von Benutzern und Gruppen aus einer der folgenden Identitätsquellen für Ihren IAM Identity Center-Identitätsspeicher ein:
  - Active Directory — Weitere Informationen finden Sie unter. Herstellen einer Verbindung mit einem Microsoft AD Verzeichnis
  - Externer Identitätsanbieter — Weitere Informationen finden Sie unterStellen Sie eine Connect zu einem externen Identitätsanbieter her.

  Wenn Sie diese Bereitstellungsmethode wählen, verwalten Sie Ihre Benutzer und Gruppen weiterhin von Ihrer Identitätsquelle aus, und diese Änderungen werden mit dem IAM Identity Center-Identitätsspeicher synchronisiert.

Für welche Identitätsquelle Sie sich auch entscheiden, IAM Identity Center kann die Benutzer- und Gruppeninformationen mit verwalteten Anwendungen teilen. AWS Auf diese Weise können Sie eine Identitätsquelle einmal mit dem IAM Identity Center verbinden und dann Identitätsinformationen mit mehreren Anwendungen in der teilen. AWS Cloud Dadurch entfällt die Notwendigkeit, für jede Anwendung den Verbund und die Bereitstellung von Identitäten unabhängig voneinander einzurichten. Diese Funktion zur gemeinsamen Nutzung macht es auch einfach, Ihren Benutzern Zugriff auf viele Anwendungen in verschiedenen AWS-Konten Bereichen zu gewähren.

Überlegungen zum Teilen von Identitätsinformationen in AWS-Konten

IAM Identity Center unterstützt die am häufigsten verwendeten Attribute in allen Anwendungen. Zu diesen Attributen gehören Vor- und Nachname, Telefonnummer, E-Mail-Adresse, Adresse und bevorzugte Sprache. Überlegen Sie sorgfältig, welche Anwendungen und welche Konten diese personenbezogenen Daten verwenden können.

Sie können den Zugriff auf diese Informationen auf eine der folgenden Arten kontrollieren. Sie können wählen, ob Sie den Zugriff nur für das AWS Organizations Verwaltungskonto oder für alle Konten in aktivieren möchten AWS Organizations. Oder Sie können mithilfe von Service Control Policies (SCPs) steuern, welche Anwendungen auf die Informationen in welchen Konten zugreifen können. AWS Organizations Wenn Sie beispielsweise den Zugriff nur im AWS Organizations Verwaltungskonto aktivieren, haben Anwendungen in Mitgliedskonten keinen Zugriff auf die Informationen. Wenn Sie jedoch den Zugriff für alle Konten aktivieren, können Sie SCPs verwenden,

um allen Anwendungen den Zugriff zu verbieten, mit Ausnahme derjenigen, die Sie zulassen möchten.

Aktivierung identitätsbewusster Konsolensitzungen

Eine identitätsbewusste Sitzung für die Konsole verbessert die Konsolensitzung eines Benutzers AWS , indem sie zusätzlichen Benutzerkontext bereitstellt, um die Benutzererfahrung zu personalisieren. Diese Funktion wird derzeit für Benutzer von Amazon Q in der AWS Konsole unterstützt.

Sie können Konsolensitzungen mit identitätsbezogener Identität aktivieren, ohne Änderungen an den bestehenden Zugriffsmustern oder dem Verbund in der AWS Konsole vornehmen zu müssen. Wenn sich Ihre Benutzer mit IAM an der AWS Konsole anmelden (z. B. wenn sie sich als IAM-Benutzer oder über Verbundzugriff mit IAM anmelden), können sie diese Methoden weiterhin verwenden. Wenn sich Ihre Benutzer beim AWS Zugriffsportal anmelden, können sie weiterhin ihre IAM Identity Center-Benutzeranmeldedaten verwenden.

Themen

Voraussetzungen und Überlegungen

Bevor Sie identitätsbewusste Konsolensitzungen aktivieren, sollten Sie die folgenden Voraussetzungen und Überlegungen überprüfen:

- Sie müssen identitätsbewusste Konsolensitzungen für Benutzer aktivieren, die Zugriff auf Amazon Q in der AWS Konsole benötigen.
- Identitätssensitive Konsolensitzungen werden derzeit nur für die Verwendung mit Amazon Q in der AWS Konsole unterstützt.
- Konsolensitzungen mit Identitätsbewusstsein erfordern eine Organisationsinstanz von IAM Identity Center.
- Die Integration mit Amazon Q wird nicht unterstützt, wenn Sie IAM Identity Center in einem AWS-Region Opt-In aktivieren.
- Nachdem Sie identitätsbewusste Konsolensitzungen aktiviert haben, können Sie diese Funktion nicht mehr deaktivieren.

- Um identitätsbewusste Konsolensitzungen zu aktivieren, benötigen Sie die folgenden Berechtigungen:
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`
  - `sso:PutApplicationGrant`
  - `sso:PutApplicationAccessScope`
  - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
  - `signin:ListTrustedIdentityPropagationApplicationForConsole`
  -
- Um Ihren Benutzern die Verwendung identitätsbewusster Konsolensitzungen zu ermöglichen, müssen Sie ihnen die entsprechenden `sts:setContext` Berechtigungen in einer identitätsbasierten Richtlinie erteilen. Weitere Informationen finden Sie unter Benutzern Berechtigungen zur Nutzung identitätsbewusster Konsolensitzungen gewähren.

Wie aktiviert man Sitzungen identity-aware-console

Sie können identitätsbewusste Konsolensitzungen in der Amazon Q-Konsole oder in der IAM Identity Center-Konsole aktivieren.

Aktivieren Sie identitätsbewusste Konsolensitzungen in der Amazon Q-Konsole

Bevor Sie identitätsbewusste Konsolensitzungen aktivieren können, müssen Sie über eine Organisationsinstanz von IAM Identity Center verfügen, an die eine Identitätsquelle angeschlossen ist. Wenn Sie IAM Identity Center bereits konfiguriert haben, fahren Sie mit Schritt 3 fort.

1. Öffnen Sie die IAM Identity Center-Konsole. Wählen Sie Aktivieren und erstellen Sie eine Organisationsinstanz von IAM Identity Center. Weitere Informationen finden Sie unter Aktivieren AWS IAM Identity Center.
2. Connect Ihre Identitätsquelle mit IAM Identity Center und stellen Sie Benutzern Zugriff auf IAM Identity Center zur Verfügung. Sie können das standardmäßige IAM Identity Center-Verzeichnis als Identitätsquelle wählen oder einen anderen Identitätsanbieter verwenden. Weitere Informationen finden Sie unter Erste Schritte mit Tutorials.

3. Nachdem Sie das IAM Identity Center eingerichtet haben, öffnen Sie die Amazon Q-Konsole und folgen Sie den Schritten unter Abonnements im Amazon Q Developer User Guide. Stellen Sie sicher, dass Sie identitätsbewusste Konsolensitzungen aktivieren.

> **Note**
>
> Wenn Sie nicht über ausreichende Berechtigungen verfügen, um identitätsbewusste Konsolensitzungen zu aktivieren, müssen Sie möglicherweise einen IAM Identity Center-Administrator bitten, diese Aufgabe in der IAM Identity Center-Konsole für Sie auszuführen. Weitere Informationen finden Sie im nächsten Verfahren .

Aktivieren Sie identitätsbewusste Konsolensitzungen in der IAM Identity Center-Konsole

Wenn Sie ein IAM Identity Center-Administrator sind, werden Sie möglicherweise von einem anderen Administrator aufgefordert, identitätsbewusste Konsolensitzungen in der IAM Identity Center-Konsole zu aktivieren.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen).
3. Wählen Sie unter „Identitätssensitive Sitzungen aktivieren“ die Option Aktivieren aus.
4. Wählen Sie in der zweiten Nachricht die Option Aktivieren aus.
5. Nachdem Sie die Aktivierung identitätsbewusster Konsolensitzungen abgeschlossen haben, wird oben auf der Einstellungsseite eine Bestätigungsmeldung angezeigt.
6. Im Abschnitt „Details“ lautet der Status für identitätssensitive Sitzungen „Aktiviert“.

So funktionieren identitätsbewusste Konsolensitzungen

Bei identitätsbewussten Konsolensitzungen können sich Benutzer von Amazon Q in der AWS Konsole anmelden AWS, die AWS Management Console oder eine andere AWS Website öffnen, das Amazon Q-Symbol wählen und einen Chat starten oder andere unterstützte Funktionen nutzen. Weitere Informationen finden Sie im Amazon Q Developer User Guide.

IAM Identity Center erweitert die aktuelle Konsolensitzung eines Benutzers um die ID des aktiven IAM Identity Center-Benutzers und die IAM Identity Center-Sitzungs-ID.

Konsolensitzungen, bei denen Identität berücksichtigt wird, beinhalten die folgenden drei Werte:

- Benutzer-ID des Identitätsspeichers (Identitätsspeicher: UserId) — Dieser Wert wird verwendet, um einen Benutzer in der Identitätsquelle, die mit IAM Identity Center verbunden ist, eindeutig zu identifizieren.
- Identitätsspeicher-Verzeichnis ARN (Identitätsspeicher: IdentityStoreArn) — Dieser Wert ist der ARN des Identitätsspeichers, der mit IAM Identity Center verbunden ist und für `identitystore:UserId` den Sie nach Attributen suchen können.
- IAM Identity Center-Sitzungs-ID — Dieser Wert gibt an, ob die IAM Identity Center-Sitzung des Benutzers noch gültig ist.

Die Werte sind identisch, werden jedoch auf unterschiedliche Weise abgerufen und zu unterschiedlichen Zeitpunkten des Vorgangs hinzugefügt, je nachdem, wie sich der Benutzer anmeldet:

- IAM Identity Center (AWS Zugriffsportal): In diesem Fall werden die Benutzer-ID und die ARN-Werte des Identitätsspeichers des Benutzers bereits in der aktiven IAM Identity Center-Sitzung bereitgestellt. IAM Identity Center erweitert die aktuelle Sitzung, indem nur die Sitzungs-ID hinzugefügt wird.
- Andere Anmeldemethoden: Wenn sich der Benutzer AWS als IAM-Benutzer, mit einer IAM-Rolle oder als Verbundbenutzer mit IAM anmeldet, wird keiner dieser Werte bereitgestellt. IAM Identity Center erweitert die aktuelle Sitzung um die Benutzer-ID des Identitätsspeichers, den ARN des Identitätsspeicher-Verzeichnisses und die Sitzungs-ID.

Einschränkung der Nutzung verwalteter Anwendungen AWS

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, AWS können AWS verwaltete Anwendungen automatisch in allen Konten in verwendet werden. AWS Organizations Um Anwendungen einzuschränken, müssen Sie SCPs implementieren. Sie können SCPs verwenden, um den Zugriff auf die Benutzer- und Gruppeninformationen von IAM Identity Center zu blockieren und zu verhindern, dass die Anwendung gestartet wird, außer in bestimmten Konten.

Details zu einer AWS verwalteten Anwendung anzeigen

Nachdem Sie eine AWS verwaltete Anwendung mithilfe der Konsole oder der APIs für die Anwendung mit IAM Identity Center verbunden haben, wird die Anwendung bei IAM Identity Center registriert. Nachdem eine Anwendung bei IAM Identity Center registriert wurde, können Sie detaillierte Informationen über die Anwendung in der IAM Identity Center-Konsole einsehen.

Um Informationen zu einer AWS verwalteten Anwendung in der IAM Identity Center-Konsole anzuzeigen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „AWS Verwaltete Anwendungen“.
4. Wählen Sie in der Liste der Anwendungen den Namen der Anwendung aus, für die Sie detaillierte Informationen anzeigen möchten.
5. Zu den Informationen über das Programm gehören, ob Benutzer- und Gruppenzuweisungen erforderlich sind, sowie gegebenenfalls die zugewiesenen Benutzer und Gruppen sowie vertrauenswürdige Anwendungen für die Weitergabe von Identitäten. Hinweise zur Weitergabe vertrauenswürdiger Identitäten finden Sie unterVertrauenswürdige Identitätsverteilung zwischen Anwendungen.

Eine AWS verwaltete Anwendung deaktivieren

Um zu verhindern, dass sich Benutzer bei einer AWS verwalteten Anwendung authentifizieren, können Sie die Anwendung in der IAM Identity Center-Konsole deaktivieren.

> **Warning**
>
> Durch das Deaktivieren einer Anwendung werden alle Benutzerberechtigungen für diese Anwendung gelöscht, die Anwendung wird vom IAM Identity Center getrennt und der Zugriff auf die Anwendung ist nicht mehr möglich. Wenn Sie ein IAM Identity Center-Administrator sind, empfehlen wir, dass Sie sich mit dem Anwendungsadministrator abstimmen, bevor Sie diese Aufgabe ausführen.

Um eine AWS verwaltete Anwendung zu deaktivieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie auf der Seite Anwendungen unter AWS Verwaltete Anwendungen die Anwendung aus, die Sie deaktivieren möchten.
4. Wählen Sie bei ausgewählter Anwendung Aktionen und anschließend Deaktivieren aus.
5. Wählen Sie im Dialogfeld „Anwendung sperren“ die Option „Sperren“.

6. In der Liste der AWS verwalteten Anwendungen wird der Anwendungsstatus als Inaktiv angezeigt.

Vom Kunden verwaltete Anwendungen

Mit IAM Identity Center können Sie Workforce-Benutzer erstellen oder verbinden und deren Zugriff auf all ihre AWS-Konten Anwendungen zentral verwalten. IAM Identity Center fungiert als zentraler Identitätsdienst und bietet verschiedene Möglichkeiten zur Authentifizierung Ihrer Benutzer. Wenn Sie bereits einen Identitätsanbieter (IdP) verwenden, kann IAM Identity Center in Ihren IdP integriert werden, sodass Sie Ihre Benutzer und Gruppen in IAM Identity Center bereitstellen und Ihren IdP für die Authentifizierung verwenden können.

Wenn Sie vom Kunden verwaltete Anwendungen verwenden, die SAML 2.0 unterstützen, können Sie Ihren IdP über SAML 2.0 mit IAM Identity Center verbinden und IAM Identity Center verwenden, um den Benutzerzugriff auf diese Anwendungen zu verwalten. IAM Identity Center bietet einen Katalog häufig verwendeter Anwendungen, die SAML 2.0 unterstützen, wie Salesforce und Microsoft 365. Dieser Katalog ist in der IAM Identity Center-Konsole verfügbar. Sie können auch Ihre eigenen SAML 2.0-Anwendungen einrichten.

> **Note**
>
> Wenn Sie vom Kunden verwaltete Anwendungen haben, die OAuth 2.0 unterstützen, und Ihre Benutzer von diesen Anwendungen aus Zugriff auf AWS Dienste benötigen, können Sie Trusted Identity Propagation verwenden. Mit Trusted Identity Propagation kann sich ein Benutzer bei einer Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Zugriff auf Daten in AWS Diensten weitergeben. Weitere Informationen finden Sie unter Verwendung von Trusted Identity Propagation mit vom Kunden verwalteten Anwendungen.

Themen

- SAML 2.0 und OAuth 2.0
- Einrichtung von vom Kunden verwalteten SAML 2.0-Anwendungen

SAML 2.0 und OAuth 2.0

Mit IAM Identity Center können Sie Ihren Benutzern Single Sign-On-Zugriff auf SAML 2.0- oder OAuth 2.0-Anwendungen gewähren. Die folgenden Themen bieten einen allgemeinen Überblick über SAML 2.0 und OAuth 2.0.

Themen

- SAML 2.0
- OAuth 2.0

SAML 2.0

SAML 2.0 ist ein Industriestandard, der für den sicheren Austausch von SAML-Assertions verwendet wird, die Informationen über einen Benutzer zwischen einer SAML-Behörde (als Identitätsanbieter oder IdP bezeichnet) und einem SAML 2.0-Verbraucher (als Service Provider oder SP bezeichnet) weitergeben. IAM Identity Center verwendet diese Informationen, um Benutzern, die berechtigt sind, Anwendungen innerhalb des Zugriffsportals zu verwenden, einen föderierten Single Sign-On-Zugriff bereitzustellen. AWS

OAuth 2.0

OAuth 2.0 ist ein Protokoll, mit dem Anwendungen sicher auf Benutzerdaten zugreifen und diese teilen können, ohne Passwörter weitergeben zu müssen. Diese Funktion bietet Benutzern eine sichere und standardisierte Möglichkeit, Anwendungen den Zugriff auf ihre Ressourcen zu gewähren. Der Zugriff wird durch verschiedene OAuth 2.0-Zuschüsse erleichtert.

Mit IAM Identity Center können Anwendungen, die auf öffentlichen Clients ausgeführt werden, temporäre Anmeldeinformationen für den Zugriff AWS-Konten und die Dienste programmgesteuert im Namen ihrer Benutzer abrufen. Öffentliche Clients sind in der Regel Desktops, Laptops oder andere mobile Geräte, die zur lokalen Ausführung von Anwendungen verwendet werden. Beispiele für AWS Anwendungen, die auf öffentlichen Clients ausgeführt werden, sind die AWS Command Line Interface (AWS CLI) AWS Toolkit, und AWS Software Development Kits (SDKs). Damit diese Anwendungen Anmeldeinformationen abrufen können, unterstützt IAM Identity Center Teile der folgenden OAuth 2.0-Flows:

- Autorisierungscode mit Proof Key for Code Exchange (PKCE) (RFC 6749 und RFC 7636)
- Erteilung der Geräteautorisierung (RFC 8628)

> **Note**
>
> Diese Arten von Zuschüssen können nur verwendet werden, wenn sie AWS-Services diese Funktion unterstützen. Diese Dienste unterstützen diesen Zuschusstyp möglicherweise nicht vollständig AWS-Regionen. Informationen zu den regionalen Unterschieden finden Sie in der Dokumentation. AWS-Services

OpenID Connect (OIDC) ist ein Authentifizierungsprotokoll, das auf dem OAuth 2.0 Framework basiert. OIDC spezifiziert, wie OAuth 2.0 für die Authentifizierung verwendet wird. Über die IAM Identity Center OIDC-Dienst-APIs registriert eine Anwendung einen OAuth 2.0-Client und verwendet einen dieser Abläufe, um ein Zugriffstoken zu erhalten, das Berechtigungen für durch IAM Identity Center geschützte APIs gewährt. Eine Anwendung spezifiziert Zugriffsbereiche, um ihren beabsichtigten API-Benutzer zu deklarieren. Nachdem Sie als IAM Identity Center-Administrator Ihre Identitätsquelle konfiguriert haben, müssen Ihre Anwendungsendbenutzer einen Anmeldevorgang abschließen, sofern sie dies noch nicht getan haben. Ihre Endbenutzer müssen dann ihre Zustimmung geben, damit die Anwendung API-Aufrufe tätigen darf. Diese API-Aufrufe werden unter Verwendung der Benutzerberechtigungen getätigt. Als Antwort gibt IAM Identity Center ein Zugriffstoken an die Anwendung zurück, das die Zugriffsbereiche enthält, denen die Benutzer zugestimmt haben.

Es wird ein OAuth 2.0-Grant-Flow verwendet

OAuth 2.0-Grant-Flows sind nur über AWS verwaltete Anwendungen verfügbar, die diese Flows unterstützen. Um einen OAuth 2.0-Flow verwenden zu können, müssen Ihre Instanz von IAM Identity Center und alle unterstützten AWS verwalteten Anwendungen, die Sie verwenden, in einer einzigen Instanz bereitgestellt werden. AWS-Region Die regionale Verfügbarkeit der AWS verwalteten Anwendungen und AWS-Service die IAM Identity Center-Instanz, die Sie verwenden möchten, finden Sie in der jeweiligen Dokumentation.

Um eine Anwendung zu verwenden, die einen OAuth 2.0-Flow verwendet, muss der Endbenutzer die URL eingeben, unter der die Anwendung eine Verbindung herstellt und sich bei Ihrer IAM Identity Center-Instanz registriert. Je nach Anwendung müssen Sie als Administrator Ihren Benutzern die URL des AWS Zugriffsportals oder die Aussteller-URL Ihrer IAM Identity Center-Instanz zur Verfügung stellen. Sie finden diese beiden Einstellungen auf der Einstellungsseite der IAM Identity Center-Konsole. Weitere Informationen zur Konfiguration einer Client-Anwendung finden Sie in der Dokumentation der jeweiligen Anwendung.

Wie der Endbenutzer sich bei einer Anwendung anmeldet und seine Zustimmung erteilt, hängt davon ab, ob die Anwendung das Erteilung des Autorisierungscodes mit PKCE Oder verwendetGeräteautorisierung gewähren.

Erteilung des Autorisierungscodes mit PKCE

Dieser Ablauf wird von Anwendungen verwendet, die auf einem Gerät ausgeführt werden, das über einen Browser verfügt.

1. Ein Browserfenster wird geöffnet.
2. Wenn sich der Benutzer nicht authentifiziert hat, leitet ihn der Browser weiter, um die Benutzerauthentifizierung abzuschließen.
3. Nach der Authentifizierung wird dem Benutzer ein Zustimmungsbildschirm angezeigt, auf dem die folgenden Informationen angezeigt werden:
   - Der Name der Anwendung
   - Die Zugriffsbereiche, für deren Verwendung die Anwendung um Zustimmung bittet
4. Der Benutzer kann den Einwilligungsprozess abbrechen oder seine Zustimmung geben und der Antrag setzt den Zugriff auf der Grundlage der Benutzerberechtigungen fort.

Geräteautorisierung gewähren

Dieser Flow kann von Anwendungen verwendet werden, die auf einem Gerät mit oder ohne Browser ausgeführt werden. Wenn die Anwendung den Flow initiiert, präsentiert die Anwendung eine URL und einen Benutzercode, die der Benutzer später im Flow überprüfen muss. Der Benutzercode ist erforderlich, da die Anwendung, die den Flow initiiert, möglicherweise auf einem anderen Gerät läuft als dem Gerät, auf dem der Benutzer seine Zustimmung erteilt. Der Code stellt sicher, dass der Benutzer dem Flow zustimmt, den er auf dem anderen Gerät initiiert hat.

1. Wenn der Flow von einem Gerät mit einem Browser aus initiiert wird, wird ein Browserfenster geöffnet. Wenn der Flow von einem Gerät ohne Browser aus initiiert wird, muss der Benutzer einen Browser auf einem anderen Gerät öffnen und zu der URL wechseln, die von der Anwendung angezeigt wurde.
2. In beiden Fällen leitet der Browser den Benutzer weiter, um die Benutzerauthentifizierung abzuschließen, wenn er sich nicht authentifiziert hat.
3. Nach der Authentifizierung wird dem Benutzer ein Zustimmungsbildschirm angezeigt, auf dem die folgenden Informationen angezeigt werden:

- Der Name der Anwendung
- Die Zugriffsbereiche, für deren Verwendung die Anwendung um Zustimmung bittet
- Der Benutzercode, den die Anwendung dem Benutzer präsentiert hat

4. Der Benutzer kann den Einwilligungsprozess abbrechen oder seine Zustimmung geben, sodass die Anwendung auf der Grundlage der Benutzerberechtigungen mit dem Zugriff fortfährt.

Bereiche des Zugriffs

Ein Bereich definiert den Zugriff für einen Dienst auf einen Dienst, auf den über einen OAuth 2.0-Flow zugegriffen werden kann. Bereiche sind eine Möglichkeit für den Dienst, der auch als Ressourcenserver bezeichnet wird, Berechtigungen in Bezug auf Aktionen und die Dienstressourcen zu gruppieren. Sie spezifizieren die groben Operationen, die OAuth 2.0-Clients anfordern können. Wenn sich ein OAuth 2.0-Client beim IAM Identity Center OIDC-Dienst registriert, gibt der Client die Bereiche an, in denen die beabsichtigten Aktionen deklariert werden, für die der Benutzer seine Zustimmung geben muss.

OAuth 2.0-Clients verwenden `scope` Werte, die in Abschnitt 3.3 von OAuth 2.0 (RFC 6749) definiert sind, um anzugeben, welche Berechtigungen für ein Zugriffstoken angefordert werden. Clients können maximal 25 Bereiche angeben, wenn sie ein Zugriffstoken anfordern. Wenn ein Benutzer im Rahmen einer Autorisierungscode-Gewährung mit PKCE oder Device Authorization Grant seine Zustimmung erteilt, codiert IAM Identity Center die Bereiche in das zurückgegebene Zugriffstoken.

AWS fügt dem IAM Identity Center Bereiche für unterstützte Bereiche hinzu. AWS-Services In der folgenden Tabelle sind die Bereiche aufgeführt, die der IAM Identity Center OIDC-Dienst unterstützt, wenn Sie einen öffentlichen Client registrieren.

Greifen Sie bei der Registrierung eines öffentlichen Clients auf Bereiche zu, die vom IAM Identity Center OIDC-Dienst unterstützt werden

Scope	Beschreibung	Dienste, die unterstützt werden von
`sso:account:access`	Greifen Sie auf verwaltete Konten und Berechtigungssätze von IAM Identity Center zu.	IAM Identity Center
`codewhisperer:analysis`	Ermöglichen Sie den Zugriff auf die Amazon Q Developer-Codeanalyse.	AWS Builder ID und IAM Identity Center

Scope	Beschreibung	Dienste, die unterstützt werden von
`codewhisperer:completions`	Aktivieren Sie den Zugriff auf Amazon Q-Inline-Code-Vorschläge.	AWS Builder ID und IAM Identity Center
`codewhisperer:conversations`	Aktivieren Sie den Zugriff auf den Amazon Q-Chat.	AWS Builder ID und IAM Identity Center
`codewhisperer:taskassist`	Ermöglichen Sie den Zugriff auf Amazon Q Developer Agent für die Softwareentwicklung.	AWS Builder ID und IAM Identity Center
`codewhisperer:transformations`	Aktivieren Sie den Zugriff auf Amazon Q Developer Agent für die Codetransformation.	AWS Builder ID und IAM Identity Center
`codecatalyst:read_write`	Lesen und Schreiben in Ihre CodeCatalyst Amazon-Ressourcen, sodass Sie auf all Ihre vorhandenen Ressourcen zugreifen können.	AWS Builder ID und IAM Identity Center

Einrichtung von vom Kunden verwalteten SAML 2.0-Anwendungen

Wenn Sie vom Kunden verwaltete Anwendungen verwenden, die SAML 2.0 unterstützen, können Sie Ihren IdP über SAML 2.0 mit IAM Identity Center verbinden und IAM Identity Center verwenden, um den Benutzerzugriff auf diese Anwendungen zu verwalten. Sie können eine SAML 2.0-Anwendung aus einem Katalog häufig verwendeter Anwendungen in der IAM Identity Center-Konsole auswählen oder Ihre eigene SAML 2.0-Anwendung einrichten.

> **Note**
>
> Wenn Sie vom Kunden verwaltete Anwendungen haben, die OAuth 2.0 unterstützen, und Ihre Benutzer von diesen Anwendungen aus Zugriff auf AWS Dienste benötigen, können Sie Trusted Identity Propagation verwenden. Mit Trusted Identity Propagation kann sich ein Benutzer bei einer Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Zugriff auf Daten in AWS Diensten weitergeben. Weitere

Informationen finden Sie unter Verwendung von Trusted Identity Propagation mit vom Kunden verwalteten Anwendungen.

Themen

IAM Identity Center-Anwendungskatalog

Sie können den Anwendungskatalog in der IAM Identity Center-Konsole verwenden, um viele häufig verwendete SAML 2.0-Anwendungen hinzuzufügen, die mit IAM Identity Center funktionieren. Beispiele hierfür sind Salesforce, Box und Microsoft 365.

Die meisten Anwendungen bieten detaillierte Informationen darüber, wie die Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter der Anwendung eingerichtet wird. Diese Informationen sind auf der Konfigurationsseite für die Anwendung verfügbar, nachdem Sie die Anwendung im Katalog ausgewählt haben. Nachdem Sie die Anwendung konfiguriert haben, können Sie Benutzern oder Gruppen in IAM Identity Center nach Bedarf Zugriff zuweisen.

Themen

Richten Sie eine Anwendung aus dem Anwendungskatalog ein

Gehen Sie wie folgt vor, um eine SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer Anwendung einzurichten.

Bevor Sie mit diesem Verfahren beginnen, ist es hilfreich, die Metadaten-Austauschdatei des Dienstanbieters zur Verfügung zu haben, damit Sie die Vertrauensstellung effizienter einrichten können. Wenn Sie nicht über diese Datei verfügen, können Sie dieses Verfahren trotzdem verwenden, um die Vertrauensstellung manuell zu konfigurieren.

Um eine Anwendung aus dem Anwendungskatalog hinzuzufügen und zu konfigurieren

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).

3. Wählen Sie die Registerkarte „Vom Kunden verwaltet“.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Einstellungen die Option Ich möchte eine Anwendung aus dem Katalog auswählen aus.
6. Geben Sie unter Anwendungskatalog den Namen der Anwendung, die Sie hinzufügen möchten, in das Suchfeld ein.
7. Wählen Sie den Namen der Anwendung aus der Liste aus, wenn er in den Suchergebnissen angezeigt wird, und klicken Sie dann auf Weiter.
8. Auf der Seite „Anwendung konfigurieren“ sind die Felder Anzeigename und Beschreibung bereits mit relevanten Details für die Anwendung gefüllt. Sie können diese Informationen bearbeiten.
9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:

    a. Wählen Sie unter IAM Identity Center SAML-Metadatendatei die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.

    b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Zertifikat herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

    > **Note**
    >
    > Sie benötigen diese Dateien später, wenn Sie die Anwendung auf der Website des Dienstanbieters einrichten. Befolgen Sie die Anweisungen des Anbieters.

10. (Optional) Unter Anwendungseigenschaften können Sie die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendungseigenschaften in der IAM Identity Center-Konsole.
11. Führen Sie unter Anwendungsmetadaten einen der folgenden Schritte aus:

    a. Wenn Sie über eine Metadatendatei verfügen, wählen Sie SAML-Metadatendatei für die Anwendung hochladen aus. Wählen Sie dann Datei auswählen, nach der die Metadatendatei gesucht werden soll, und wählen Sie sie aus.

    b. Wenn Sie keine Metadatendatei haben, wählen Sie Manuelles Eingeben Ihrer Metadatenwerte und geben Sie dann die ACS-URL der Anwendung und die SAML-Zielgruppenwerte für die Anwendung an.

12. Wählen Sie Absenden aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Richten Sie Ihre eigene SAML 2.0-Anwendung ein

Sie können Ihre eigenen Anwendungen einrichten, die einen Identitätsverbund mit SAML 2.0 ermöglichen, und sie zu IAM Identity Center hinzufügen. Die meisten Schritte zum Einrichten Ihrer eigenen SAML 2.0-Anwendungen entsprechen dem Einrichten einer SAML 2.0-Anwendung aus dem Anwendungskatalog in der IAM Identity Center-Konsole. Sie müssen jedoch auch zusätzliche SAML-Attributzuordnungen für Ihre eigenen SAML 2.0-Anwendungen bereitstellen. Diese Zuordnungen ermöglichen es IAM Identity Center, die SAML 2.0-Assertion für Ihre Anwendung korrekt auszufüllen. Sie können diese zusätzliche SAML-Attributzuordnung bereitstellen, wenn Sie die Anwendung zum ersten Mal einrichten. Sie können SAML 2.0-Attributzuordnungen auch auf der Seite mit den Anwendungsdetails in der IAM Identity Center-Konsole angeben.

Gehen Sie wie folgt vor, um eine SAML 2.0-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer SAML 2.0-Anwendung einzurichten. Bevor Sie damit beginnen, stellen Sie sicher, dass Sie die Zertifikatsdatei sowie die Austauschdatei mit den Metadaten des Service-Anbieters haben, damit Sie die Einrichtung der Vertrauensstellung abschließen können.

So richten Sie Ihre eigene SAML 2.0-Anwendung ein

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „Vom Kunden verwaltet“.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Einstellungen die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
6. Wählen Sie unter Anwendungstyp die Option SAML 2.0 aus.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Anwendung konfigurieren unter Anwendung konfigurieren einen Anzeigenamen für die Anwendung ein, z. B. **`MyApp`** Geben Sie dann eine Beschreibung ein.
9. Gehen Sie unter IAM Identity Center-Metadaten wie folgt vor:

    a. Wählen Sie unter SAML-Metadatendatei für IAM Identity Center die Option Herunterladen aus, um die Metadaten des Identitätsanbieters herunterzuladen.

    b. Wählen Sie unter IAM Identity Center-Zertifikat die Option Herunterladen aus, um das Identitätsanbieter-Zertifikat herunterzuladen.

> **Note**
>
> Sie benötigen diese Dateien später, wenn Sie die benutzerdefinierte Anwendung über die Website des Service-Anbieters einrichten.

10. (Optional) Unter Anwendungseigenschaften können Sie auch die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer angeben. Weitere Informationen finden Sie unter Konfigurieren Sie die Anwendungseigenschaften in der IAM Identity Center-Konsole.
11. Wählen Sie unter Anwendungsmetadaten die Option Manuelles Eingeben Ihrer Metadatenwerte aus. Geben Sie dann die ACS-URL der Anwendung und die Zielgruppenwerte für die SAML-Anwendung ein.
12. Wählen Sie Absenden aus. Sie werden zur Detailseite der Anwendung weitergeleitet, die Sie gerade hinzugefügt haben.

Vertrauenswürdige Identitätsverteilung zwischen Anwendungen

Die Verbreitung vertrauenswürdiger Identitäten ermöglicht es AWS Diensten, Folgendes zu tun:

- Autorisieren Sie den Zugriff auf AWS Ressourcen auf der Grundlage des Identitätskontextes des Benutzers.
- Teilen Sie den Identitätskontext des Benutzers auf sichere Weise mit anderen AWS Diensten.

Mit diesen Funktionen kann der Benutzerzugriff einfacher definiert, gewährt und protokolliert werden.

Mit Trusted Identity Propagation kann sich ein Benutzer bei einer Anwendung anmelden, und diese Anwendung kann den Identitätskontext des Benutzers bei Anfragen zum Zugriff auf Daten in AWS Diensten weitergeben. Da der Zugriff auf der Identität eines Benutzers basiert, müssen Benutzer keine lokalen Benutzeranmeldedaten für die Datenbank verwenden oder eine IAM-Rolle übernehmen, um auf Daten zuzugreifen.

Themen

- Überblick über die Verbreitung vertrauenswürdiger Identitäten
- Anwendungsfälle für die Verbreitung vertrauenswürdiger Identitäten
- Richten Sie die Verbreitung vertrauenswürdiger Identitäten ein

- Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten

Überblick über die Verbreitung vertrauenswürdiger Identitäten

Mit Trusted Identity Propagation kann der Benutzerzugriff auf AWS Ressourcen einfacher definiert, gewährt und protokolliert werden. Trusted Identity Propagation basiert auf dem OAuth 2.0 Authorization Framework, das es Anwendungen ermöglicht, sicher auf Benutzerdaten zuzugreifen und diese gemeinsam zu nutzen, ohne Passwörter weitergeben zu müssen. OAuth 2.0 bietet sicheren delegierten Zugriff auf Anwendungsressourcen. Der Zugriff wird delegiert, weil der Ressourcenadministrator die Anwendung, bei der sich der Benutzer anmeldet, genehmigt oder delegiert, um auf die andere Anwendung zuzugreifen.

Um zu verhindern, dass Benutzerkennwörter weitergegeben werden, verwendet Trusted Identity Propagation Token. Mit Tokens kann eine vertrauenswürdige Anwendung standardmäßig behaupten, wer der Benutzer ist und welche Anfragen zwischen zwei Anwendungen zulässig sind. AWS verwaltete Anwendungen, die in die Verbreitung vertrauenswürdiger Identitäten integriert sind, erhalten Token direkt vom IAM Identity Center. IAM Identity Center bietet Anwendungen auch die Möglichkeit, Identitätstoken auszutauschen und auf Token zuzugreifen, die von einem externen OAuth 2.0-Autorisierungsserver stammen. Auf diese Weise kann sich eine Anwendung außerhalb von authentifizieren und Token abrufen AWS, das Token gegen ein IAM Identity Center-Token austauschen und das neue Token verwenden, um Anfragen an Dienste zu stellen. AWS Weitere Informationen finden Sie unter Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten.

Der OAuth 2.0-Prozess beginnt, wenn sich ein Benutzer bei einer Anwendung anmeldet. Die Anwendung, bei der sich der Benutzer anmeldet, initiiert eine Anfrage für den Zugriff auf die Ressourcen der anderen Anwendung. Die initiierende (anfordernde) Anwendung kann im Namen des Benutzers auf die empfangende Anwendung zugreifen, indem sie ein Token vom Autorisierungsserver anfordert. Der Autorisierungsserver gibt das Token zurück, und die initiierende Anwendung leitet dieses Token zusammen mit einer Zugriffsanforderung an die empfangende Anwendung weiter.

Anwendungsfälle für die Verbreitung vertrauenswürdiger Identitäten

Als IAM Identity Center-Administrator werden Sie möglicherweise gebeten, bei der Konfiguration der vertrauenswürdigen Identitätsverbreitung zwischen den folgenden initiierenden Anwendungen, die diese Funktion unterstützen, und verbundenen AWS Diensten zu helfen. In den folgenden

Abschnitten finden Sie weitere Informationen zu den spezifischen Anwendungsfällen, die von Anwendungen unterstützt werden, die die Verbreitung vertrauenswürdiger Identitäten initiieren können.

Themen

Amazon EMR

Sie können Amazon EMR als initiierende Anwendung für die folgenden Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten verwenden.

Beschreibung	Andere genutzte Dienste AWS	Weitere Informationen
Führen Sie interaktive Analysen mit Apache Spark auf Amazon EMR auf Amazon EC2 EC2-Clusternen über Amazon EMR Studio durch. Wenden Sie für Catalog Through eine Zugriffskontrolle an, die auf den Identitäten der Belegschaft und den zugehörigen Attributen basiert. AWS Glue AWS Lake Formation	Amazon EMR auf Amazon EC2 AWS Lake Formation, autorisiert über Amazon S3 Access Grants, Amazon S3, AWS Service Catalog Note • Erfordert Zugriff über Amazon EMR Studio. • Nur Zugriffskontrolle auf Tabellenebene.	• Integrieren Sie Amazon EMR mit IAM Identity Center im Amazon EMR Management Guide. • Amazon S3 Access Grants und Unternehmensverzeichnisidentitäten im Amazon Simple Storage Service-Benutzerhandbuch. • Verbindung AWS Lake Formation mit IAM Identity Center herstellen im Entwicklerhandbuch AWS Lake Formation • Verwenden Sie Ihre Unternehmensidentitäten für Analysen mit

Beschreibung	Andere genutzte Dienste AWS	Weitere Informationen
	• Apache Hive, PrestoSQL /Trino und EMR Serverless werden nicht unterstützt.	Amazon EMR und IAM Identity Center im AWS Big Data-Blog
Führen Sie Ad-hoc-Analysen mit Trino on Athena über Amazon EMR Studio durch. Wenden Sie für Catalog Through eine Zugriffskontrolle an, die auf den Identitäten der Mitarbeiter und den zugehörigen Attribute n basiert. AWS Glue AWS Lake Formation Sichern Sie den Zugriff auf einen Bucket mit Athena-Ab frageergebnissen in Amazon S3 mithilfe von Amazon S3 Access Grants.	Athena autorisiert durch AWS Lake Formation Amazon S3 Access Grants Note Erfordert Zugriff über Amazon EMR Studio. Direkter Zugriff von der Amazon Athena Konsole aus wird nicht unterstützt.	• Integrieren Sie Amazon EMR mit IAM Identity Center im Amazon EMR Management Guide. • Die Verwendung von IAM Identity Center aktivierten Athena-Arbeitsgruppen im Amazon Athena Athena-Be nutzerhandbuch. • Amazon S3 Access Grants und Unternehmensverzeichnisiden titäten im Amazon Simple Storage Service-Benutzerha ndbuch. • Herstellen AWS Lake Formation einer Verbindun g mit IAM Identity Center im AWS Lake Formation Entwickle rhandbuch. • Bringen Sie im AWS Big Data-Blog Ihre Mitarbeiteridentität in Amazon EMR Studio und Athena ein.

Amazon QuickSight

Sie können Amazon QuickSight als initiierende Anwendung für die folgenden Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten verwenden.

Beschreibung	Andere genutzte AWS Dienste	Weitere Informationen
QuickSight Amazon-Benutzer können Amazon Redshift-Daten abfragen. Der Datenzugriff wird in Amazon Redshift von einem Amazon Redshift Redshift-Administrator gewährt.	Amazon-Redshift	• Connect Redshift mit IAM Identity Center, um Benutzern eine einmalige Anmeldung im Amazon Redshift Management Guide zu bieten. • Connect Amazon Redshift mit IAM Identity Center über Amazon QuickSight im Amazon Redshift Management Guide.
QuickSight Amazon-Benutzer können Amazon Redshift Spectrum nach strukturierten Daten in Amazon S3 abfragen, wobei der Zugriff von einem AWS Lake Formation Administrator autorisiert wurde.	Amazon Redshift Spectrum, Amazon S3 strukturierte Daten *Über Amazon Redshift Spectrum autorisie rt durch AWS Lake Formation	• Connect Redshift mit IAM Identity Center, um Benutzern eine einmalige Anmeldung im Amazon Redshift Management Guide zu bieten. • Connect Amazon Redshift mit IAM Identity Center über Amazon QuickSight im Amazon Redshift Management Guide. • Eine Verbindung AWS Lake Formation mit IAM Identity Center herstellen finden Sie im Entwicklerhandbuch.AWS Lake Formation • Vereinfachen Sie die Zugriffsv erwaltung mit Amazon Redshift und AWS Lake Formation für Benutzer in einem externen

Beschreibung	Andere genutzte AWS Dienste	Weitere Informationen
		Identitätsanbieter im AWS Big Data-Blog.
QuickSight Amazon-Benutzer können Amazon Redshift-Datenfreigaben nach strukturierten Daten in Amazon S3 abfragen, wobei der Zugriff von einem Administrator autorisiert wurde. AWS Lake Formation	Amazon Redshift Redshift-Datenfreigaben, Amazon S3 S3-strukturierte Daten *Über Amazon Redshift autorisiert durch AWS Lake Formation	• Connect Amazon Redshift mit IAM Identity Center über Amazon QuickSight im Amazon Redshift Management Guide. • Eine Verbindung AWS Lake Formation mit IAM Identity Center herstellen finden Sie im Entwicklerhandbuch.AWS Lake Formation • Vereinfachen Sie die Zugriffsverwaltung mit Amazon Redshift und AWS Lake Formation für Benutzer in einem externen Identitätsanbieter im AWS Big Data-Blog.

Amazon-Redshift-Abfrage-Editor v2

Sie können den Amazon Redshift Query Editor v2 als initiierende Anwendung für die folgenden Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten verwenden.

Beschreibung	Andere verwendete Dienste AWS	Weitere Informationen
Benutzer des Amazon Redshift Redshift-Abfrage-Editors v2 können Amazon Redshift Redshift-Daten abfragen. Der Datenzugriff wird in Amazon Redshift von einem Amazon	Amazon-Redshift	• Connect Redshift mit IAM Identity Center, um Benutzern eine einmalige Anmeldung im Amazon Redshift Management Guide zu bieten.

Beschreibung	Andere verwendete Dienste AWS	Weitere Informationen
Redshift Redshift-Administrator gewährt.		• Stellen Sie im Amazon Redshift Management Guide eine Connect zu einer Amazon Redshift Redshift-Datenbank her. • OktaIntegrieren Sie den Amazon Redshift Query Editor V2 AWS IAM Identity Center für ein nahtloses Single Sign-On im AWS Big Data-Blog.
Benutzer des Amazon Redshift Query Editor v2 können externe Amazon Redshift Spectrum-Tabellen nach strukturierten Daten in Amazon S3 abfragen, wobei der Zugriff von einem AWS Lake Formation Administrator autorisiert wurde.	Amazon Redshift Spectrum, Amazon S3 strukturierte Daten *Über Amazon Redshift Spectrum autorisie rt durch AWS Lake Formation	• Connect Redshift mit IAM Identity Center, um Benutzern eine einmalige Anmeldung im Amazon Redshift Management Guide zu bieten. • Stellen Sie im Amazon Redshift Management Guide eine Connect zu einer Amazon Redshift Redshift-Datenbank her. • Verbindung AWS Lake Formation mit IAM Identity Center herstellen im Entwickle rhandbuch.AWS Lake Formation

Beschreibung	Andere verwendete Dienste AWS	Weitere Informationen
Benutzer des Amazon Redshift Query Editor v2 können Amazon Redshift Redshift-Datenfreigaben mit einem von einem Administrator autorisierten Zugriff abfragen. AWS Lake Formation	Amazon Redshift Redshift-Datenfreigaben, AWS Lake Formation	• Stellen Sie im Amazon Redshift Management Guide eine Connect zu einer Amazon Redshift Redshift-Datenbank her. • Verbindung AWS Lake Formation mit IAM Identity Center herstellen im Entwicklerhandbuch.AWS Lake Formation

Business Intelligence-Anwendungen von Drittanbietern

Sie können eine Business Intelligence-Anwendung eines Drittanbieters wie Tableau als initiierende Anwendung für bestimmte Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten verwenden. Modifizierte Business Intelligence-Anwendungen von Drittanbietern können dem Amazon Redshift-Treiber die Identität eines Benutzers über OAuth-Identitätstoken oder Zugriffstoken übergeben, um Amazon Redshift nach Daten abzufragen, wobei der Zugriff von einem Amazon Redshift Redshift-Administrator autorisiert wurde.

Kundenspezifisch entwickelte Anwendungen

Sie können Ihre eigenen, maßgeschneiderten Anwendungen als Startanwendung für die folgenden Anwendungsfälle zur Verbreitung vertrauenswürdiger Identitäten verwenden.

Beschreibung	Andere verwendete Dienste AWS	Weitere Informationen
Erstellen Sie eine Anwendung, die Benutzer über einen OAuth-Autorisierungsserver authentifiziert, AWS IAM Identity Center und verwenden Sie dann und IAM, um identitätserweiterte IAM-	AWS IAM Identity Center, Amazon S3 S3-unstrukturierte Daten	• Amazon S3 Access Grants und Unternehmensverzeichnisidentitäten im Amazon Simple Storage Service-Benutzerhandbuch.

Beschreibung	Andere verwendete Dienste AWS	Weitere Informationen
Rollenanmeldeinformationen zu erhalten. Diese Anmeldeinformationen werden verwendet, um Zugriff auf unstrukturierte Daten in Amazon S3 anzufordern, wobei der Zugriff von einem Amazon S3 Access Grants-Administrator autorisiert wurde.	*Autorisiert durch Amazon S3 Access Grants	• Informationen zur Entwicklung einer benutzerorientierten Datenanwendung mit IAM Identity Center und Amazon S3 Access Grants (Teil 1) und (Teil 2) finden Sie im AWS Storage-Blog.
Erstellen Sie eine benutzerdefinierte Anwendung, die mit Amazon Q Business interagiert, um Benutzerfragen auf der Grundlage Ihrer eigenen Inhalte und der Benutzerberechtigungen zu beantworten.	IAM Identity Center, Amazon Q Business	• Aktivieren und konfigurieren Sie eine IAM Identity Center-Instance im Amazon Q Business User Guide. • So verwenden Sie AWS verwaltete Anwendungen mit IAM Identity Center: Aktivieren Sie Amazon Q, ohne bestehende IAM-Verbundabläufe zu migrieren, finden Sie im AWS Sicherheitsblog.

Richten Sie die Verbreitung vertrauenswürdiger Identitäten ein

Die Verbreitung vertrauenswürdiger Identitäten unterstützt verschiedene Methoden zur Authentifizierung von Anwendungen, sodass sie die Identität eines Benutzers an AWS Dienste weitergeben können. Die Einrichtung für die Weitergabe vertrauenswürdiger Identitäten hängt von den Anwendungstypen und der Art der Authentifizierung ab.

> **Note**
>
> Sie müssen einen vertrauenswürdigen Token-Aussteller einrichten, wenn Sie vom Kunden verwaltete Anwendungen haben, die Zugriff auf AWS verwaltete Anwendungen anfordern, aber keine AWS APIs für die Verbindung verwenden.

Themen

Voraussetzungen und Überlegungen

Bevor Sie Trusted Identity Propagation einrichten, sollten Sie sich mit den folgenden Voraussetzungen und Überlegungen vertraut machen.

Themen

Voraussetzungen

Um Trusted Identity Propagation zu verwenden, stellen Sie sicher, dass Ihre Umgebung die folgenden Voraussetzungen erfüllt.

- IAM Identity Center-Bereitstellung mit bereitgestellten Benutzern und Gruppen

  Um Trusted Identity Propagation zu verwenden, müssen Sie IAM Identity Center aktivieren und Benutzer und Gruppen bereitstellen. Weitere Informationen finden Sie unter Erste Schritte mit allgemeinen Aufgaben in IAM Identity Center.

  Organisationsinstanz empfohlen — Wir empfehlen, dass Sie eine Organisationsinstanz von IAM Identity Center verwenden, die Sie im Verwaltungskonto von AWS Organizations aktivieren. Wenn Sie beabsichtigen, Trusted Identity Propagation zu verwenden, um Benutzern den Zugriff auf AWS Dienste und zugehörige Ressourcen AWS-Konten innerhalb derselben Organisation zu ermöglichen, können Sie die Verwaltung Ihrer IAM Identity Center-Instanz an ein Mitgliedskonto delegieren.

  Wenn Sie planen, eine einzelne Kontoinstanz von IAM Identity Center zu verwenden, müssen sich alle AWS Dienste und Ressourcen, auf die Benutzer über die Verbreitung vertrauenswürdiger Identitäten zugreifen können AWS-Konto, in demselben eigenständigen Konto oder in demselben Mitgliedskonto in der Organisation befinden, in der Sie IAM Identity Center aktiviert haben. Weitere Informationen finden Sie unter Kontoinstanzen von IAM Identity Center.

- Für AWS verwaltete Anwendungen: Verbindung zum IAM Identity Center

  Um Trusted Identity Propagation nutzen zu können, müssen AWS verwaltete Anwendungen in IAM Identity Center integriert werden.

Weitere Überlegungen

Beachten Sie bei der Verwendung von Trusted Identity Propagation die folgenden zusätzlichen Überlegungen.

- Ändern Sie nicht die Einstellung „Zuweisungen erforderlich“ für AWS verwaltete Anwendungen

  AWS Verwaltete Anwendungen verfügen über eine Standardeinstellungskonfiguration, die bestimmt, ob Zuweisungen für Benutzer und Gruppen erforderlich sind. Es wird empfohlen, diese Einstellung nicht zu ändern. Selbst wenn Sie detaillierte Berechtigungen konfiguriert haben, die Benutzern den Zugriff auf bestimmte Ressourcen ermöglichen, kann das Ändern der Einstellung Zuweisungen erforderlich zu unerwartetem Verhalten führen, einschließlich einer Unterbrechung des Benutzerzugriffs auf diese Ressourcen.
- Berechtigungen für mehrere Konten (Berechtigungssätze) sind nicht erforderlich

  Für die Verbreitung vertrauenswürdiger Identitäten müssen Sie keine Berechtigungen für mehrere Konten (Berechtigungssätze) einrichten. Sie können IAM Identity Center aktivieren und es nur für die Verbreitung vertrauenswürdiger Identitäten verwenden.

Verwendung der Verbreitung vertrauenswürdiger Identitäten mit AWS verwalteten Anwendungen

Die Verbreitung vertrauenswürdiger Identitäten ermöglicht AWS es einer verwalteten Anwendung, im Namen eines Benutzers Zugriff auf Daten in AWS Diensten anzufordern. Die Verwaltung des Datenzugriffs basiert auf der Identität eines Benutzers, sodass Administratoren Zugriff auf der Grundlage der vorhandenen Benutzer- und Gruppenmitgliedschaften gewähren können. Die Identität des Benutzers, die in seinem Namen ausgeführten Aktionen und andere Ereignisse werden in dienstspezifischen Protokollen und CloudTrail Ereignissen aufgezeichnet.

Die Verbreitung vertrauenswürdiger Identitäten basiert auf dem OAuth 2.0-Standard. Um diese Funktion nutzen zu können, müssen AWS verwaltete Anwendungen in IAM Identity Center integriert werden. AWS Analysedienste können treiberbasierte Schnittstellen bereitstellen, die es einer kompatiblen Anwendung ermöglichen, vertrauenswürdige Identitätsverbreitung

zu nutzen. JDBC-, ODBC- und Python-Treiber ermöglichen es kompatiblen Abfragetools beispielsweise, vertrauenswürdige Identitätsverbreitung zu verwenden, ohne dass Sie zusätzliche Einrichtungsschritte ausführen müssen.

Themen

Richten Sie AWS verwaltete Anwendungen für die Verbreitung vertrauenswürdiger Identitäten ein

AWS Dienste, die die Verbreitung vertrauenswürdiger Identitäten unterstützen, bieten eine administrative Benutzeroberfläche und APIs, mit denen Sie diese Funktion einrichten können. Für diese Dienste ist keine Konfiguration innerhalb von IAM Identity Center erforderlich.

Im Folgenden wird der allgemeine Prozess zur Einrichtung eines AWS Dienstes für die Verbreitung vertrauenswürdiger Identitäten beschrieben. Die spezifischen Schritte hängen von der administrativen Oberfläche und den APIs ab, die von der Anwendung bereitgestellt werden.

1. Verwenden Sie die Anwendungskonsole oder APIs, um die Anwendung mit Ihrer Instanz von IAM Identity Center zu verbinden

   Verwenden Sie die Konsole für die AWS verwaltete Anwendung oder die Anwendungs-APIs, um die Anwendung mit Ihrer IAM Identity Center-Instanz zu verbinden. Wenn Sie die Konsole für die Anwendung verwenden, enthält die administrative Benutzeroberfläche ein Widget, das den Einrichtungs- und Verbindungsprozess optimiert.
2. Verwenden Sie die Anwendungskonsole oder APIs, um den Benutzerzugriff auf die Ressourcen der Anwendung einzurichten

   Führen Sie diesen Schritt aus, um zu autorisieren, auf welche Ressourcen oder Daten ein Benutzer zugreifen kann. Der Zugriff basiert auf der Identität des Benutzers oder der Gruppenmitgliedschaft. Das Autorisierungsmodell variiert je nach Anwendung.

> **Important**
>
> Sie müssen diesen Schritt abschließen, damit Benutzer auf die Ressourcen des AWS Dienstes zugreifen können. Andernfalls können Benutzer nicht auf Ressourcen zugreifen, selbst wenn die anfordernde Anwendung autorisiert ist, Zugriff auf den Dienst anzufordern.

Anfragen zur Weitergabe vertrauenswürdiger Identitäten werden für AWS verwaltete Anwendungen bereitgestellt

Alle Datenflüsse zur Weitergabe vertrauenswürdiger AWS Identitäten an verwaltete Anwendungen müssen mit einer Anwendung beginnen, die ein Token von IAM Identity Center erhält. Dieses Token ist erforderlich, da es einen Verweis auf einen Benutzer enthält, der dem IAM Identity Center und den Anwendungen, die bei IAM Identity Center registriert sind, bekannt ist.

In den folgenden Abschnitten wird beschrieben, wie eine AWS verwaltete Anwendung ein Token vom IAM Identity Center abrufen kann, um die Verbreitung vertrauenswürdiger Identitäten zu initiieren.

Themen

- Webbasierte IAM Identity Center-Authentifizierung
- Konsolenbasierte, vom Benutzer initiierte Authentifizierungsanfragen

Webbasierte IAM Identity Center-Authentifizierung

Für diesen Ablauf bietet die AWS verwaltete Anwendung ein webbasiertes Single Sign-On-Erlebnis mit IAM Identity Center zur Authentifizierung.

Wenn ein Benutzer eine AWS verwaltete Anwendung öffnet, wird ein Single Sign-On-Flow ausgelöst, der IAM Identity Center verwendet. Wenn es keine aktive Sitzung für den Benutzer in IAM Identity Center gibt, wird dem Benutzer eine Anmeldeseite angezeigt, die auf der von Ihnen angegebenen Identitätsquelle basiert, und IAM Identity Center erstellt eine Sitzung für den Benutzer.

IAM Identity Center stellt der AWS verwalteten Anwendung ein Token zur Verfügung, das die Identität des Benutzers und eine Liste von Zielgruppen (Auds) und zugehörigen Bereichen enthält, für deren Verwendung die Anwendung registriert ist. Die Anwendung kann das Token dann verwenden, um Anfragen an andere Empfangsdienste zu stellen. AWS

Konsolenbasierte, vom Benutzer initiierte Authentifizierungsanfragen

Für diesen Ablauf bietet die AWS verwaltete Anwendung ein Konsolenerlebnis, das Benutzer initiieren.

In diesem Fall wird die AWS verwaltete Anwendung von der AWS Managementkonsole aus aufgerufen, nachdem sie eine Rolle übernommen hat. Damit die Anwendung ein Token erhält, muss der Benutzer einen Prozess initiieren, der die Anwendung zur Authentifizierung des Benutzers auslöst. Dadurch wird die Authentifizierung mithilfe von IAM Identity Center initiiert, wodurch der Benutzer zu der von Ihnen konfigurierten Identitätsquelle weitergeleitet wird.

Nachdem eine Anwendung ein Token erhalten hat

Nachdem eine anfordernde Anwendung ein Token von IAM Identity Center erhalten hat, aktualisiert die Anwendung das Token regelmäßig, sodass es für die gesamte Dauer der Benutzersitzung verwendet werden kann. Während dieser Zeit kann die Anwendung:

- Rufen Sie weitere Informationen über das Token ab, um festzustellen, wer der Benutzer ist und welche Bereiche die Anwendung mit anderen AWS verwalteten Empfangsanwendungen verwenden kann.
- Übergeben Sie das Token in Aufrufen an andere AWS verwaltete Empfangsanwendungen, die die Verwendung von Token unterstützen.
- Besorgen Sie sich IAM-Rollensitzungen mit verbesserter Identität, die es verwenden kann, um Anfragen an andere AWS verwaltete Anwendungen zu stellen, die AWS Signature Version 4 verwenden.

  Eine IAM-Rollensitzung mit erweiterter Identität ist eine IAM-Rollensitzung, in der die weitergegebene Identität des Benutzers in einem vom IAM Identity Center erstellten Token gespeichert ist.

IAM-Rollensitzungen mit verbesserter Identität

Das AWS Security Token Service ermöglicht einer Anwendung, eine identitätserweiterte IAM-Rollensitzung abzurufen. AWS verwaltete Anwendungen, die den Benutzerkontext in einer Rollensitzung unterstützen, können die Identitätsinformationen verwenden, um den Zugriff auf der Grundlage des Benutzers zu autorisieren, der sich in der Rollensitzung befindet. Dieser neue Kontext ermöglicht es Anwendungen, Anfragen an AWS verwaltete Anwendungen zu stellen, die die Verbreitung vertrauenswürdiger Identitäten über AWS Signature Version 4-API-Anfragen unterstützen.

Wenn eine AWS verwaltete Anwendung eine identitätserweiterte IAM-Rollensitzung für den Zugriff auf eine Ressource verwendet, CloudTrail protokolliert sie die Identität des Benutzers (Benutzer-ID), die initiierende Sitzung und die ergriffene Aktion.

Wenn eine Anwendung mithilfe einer identitätsoptimierten IAM-Rollensitzung eine Anfrage an eine empfangende Anwendung stellt, fügt sie der Sitzung Kontext hinzu, sodass die empfangende Anwendung den Zugriff auf der Grundlage der Identität oder Gruppenmitgliedschaft des Benutzers oder der IAM-Rolle autorisieren kann. Beim Empfang von Anwendungen, die die Weitergabe vertrauenswürdiger Identitäten unterstützen, wird ein Fehler zurückgegeben, wenn die empfangende Anwendung oder die angeforderte Ressource nicht so konfiguriert ist, dass der Zugriff auf der Identität oder der Gruppenmitgliedschaft des Benutzers autorisiert wird.

Gehen Sie wie folgt vor, um dieses Problem zu vermeiden:

- Stellen Sie sicher, dass die empfangende Anwendung mit IAM Identity Center verbunden ist.
- Verwenden Sie die Konsole für die empfangende Anwendung oder die Anwendungs-APIs, um die Anwendung so einzurichten, dass der Zugriff auf Ressourcen auf der Grundlage der Identität oder der Gruppenmitgliedschaft des Benutzers autorisiert wird. Die diesbezüglichen Einrichtungsanforderungen variieren je nach Anwendung.

Weitere Informationen finden Sie in der Dokumentation der empfangenden AWS verwalteten Anwendung.

Arten von IAM-Rollensitzungen mit erweiterter Identität

Eine Anwendung ruft eine identitätserweiterte IAM-Rollensitzung ab, indem sie eine Anfrage an die AWS STS `AssumeRole` API sendet und im Parameter der Anfrage eine Kontext-Assertion übergibt. `ProvidedContexts` `AssumeRole` Die Kontext-Assertion wird aus dem `idToken` Anspruch abgerufen, der in der Antwort auf die Anfrage verfügbar ist. `SSO OIDC` `CreateTokenWithIAM`

AWS STS kann zwei verschiedene Typen von IAM-Rollensitzungen mit erweiterter Identität erstellen, je nachdem, welche Kontext-Assertion für die Anfrage bereitgestellt wurde: `AssumeRole`

- Sitzungen, in denen nur die Identität des Benutzers protokolliert wird. CloudTrail
- Sitzungen, die die Autorisierung auf der Grundlage der weitergegebenen Benutzeridentität ermöglichen und in denen diese protokolliert wird. CloudTrail

Um eine IAM-Rollensitzung mit erweiterter Identität zu erhalten AWS STS , die nur Auditinformationen bereitstellt, die in einem CloudTrail Trail registriert wurden, geben Sie den Wert des `sts:audit_context` Anspruchs in der Anfrage an. `AssumeRole` Um eine Sitzung zu erhalten, die es dem empfangenden AWS Dienst auch ermöglicht, den IAM Identity Center-Benutzer zur Ausführung einer Aktion zu autorisieren, geben Sie den Wert des Anspruchs für die Anfrage an. `sts:identity_context` `AssumeRole` Sie können nur einen Kontext angeben.

IAM-Rollensitzungen mit verbesserter Identität, erstellt mit **`sts:audit_context`**

Wenn mithilfe einer identitätsoptimierten IAM-Rollensitzung, die mit erstellt wurde, eine Anfrage an einen AWS Dienst gestellt wird`sts:audit_context`, wird das IAM Identity Center `userId` des Benutzers in dem Element angemeldet. CloudTrail `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Diese Sitzungen können nicht zur Autorisierung des Identity Center-Benutzers verwendet werden. Sie können weiterhin zur Autorisierung der IAM-Rolle verwendet werden.

Um diese Art von Rollensitzung abzurufen AWS STS, geben Sie den Wert des `sts:audit_context` Felds für die `AssumeRole` Anforderung im Anforderungsparameter `ProvidedContextsan`. Verwenden Sie `arn:aws:iam::aws:contextProvider/IdentityStore` als Wert für`ProviderArn`.

IAM-Rollensitzungen mit verbesserter Identität, erstellt mit **`sts:identity_context`**

Wenn ein Benutzer mithilfe einer identitätsoptimierten IAM-Rollensitzung, die mit erstellt wurde, eine Anfrage an einen AWS Dienst stellt`sts:identity_context`, wird das IAM Identity Center `userId` des Benutzers CloudTrail in dem on`Behalf0f` Element genauso angemeldet wie eine Sitzung, die mit erstellt wurde. `sts:audit_context`

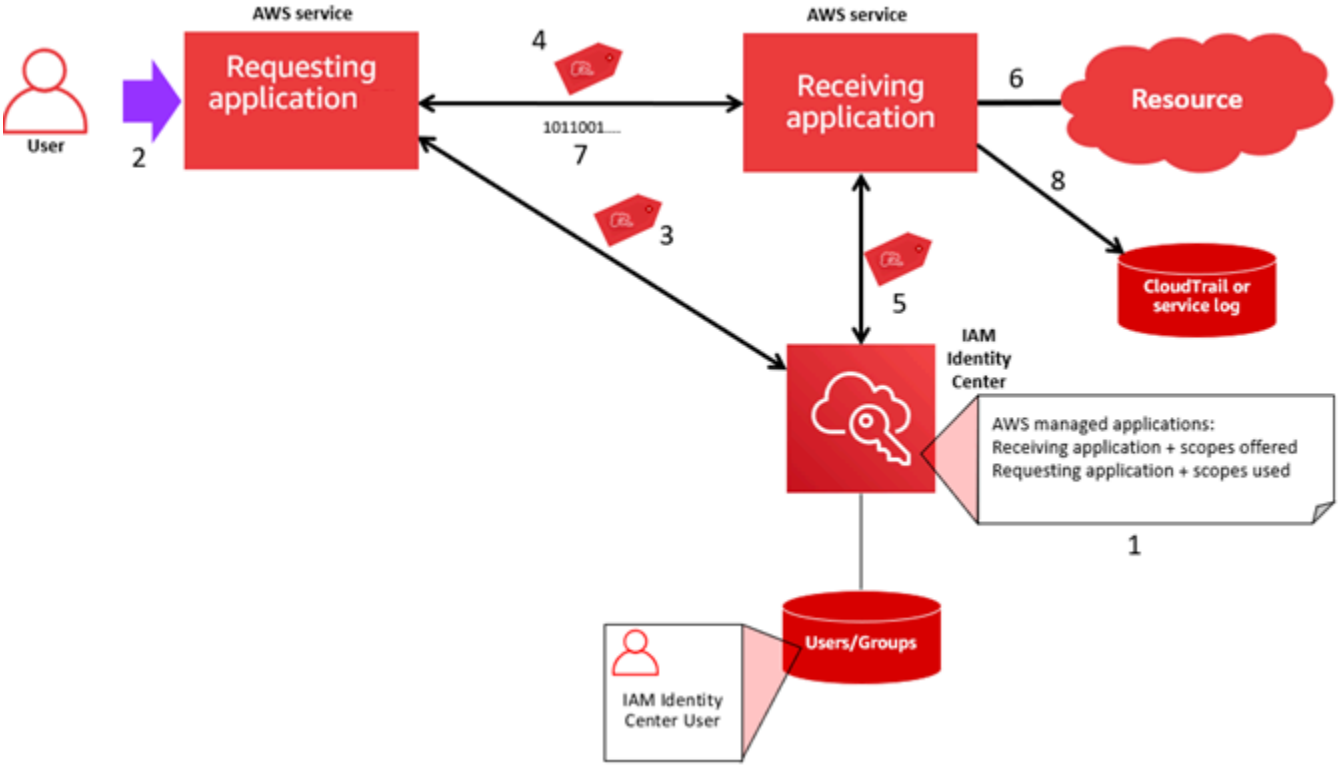
Dieser Sitzungstyp protokolliert nicht nur die Daten von IAM Identity Center-Benutzern CloudTrail, sondern wird auch von unterstützten APIs verwendet, `userId` um Aktionen auf der Grundlage der weitergegebenen Benutzeridentität zu autorisieren. Eine Liste der IAM-Aktionen für die unterstützten APIs finden Sie in der verwalteten Richtlinie. `AWSIAMIdentityCenterAllowListForIdentityContext` AWS Diese AWS verwaltete Richtlinie wird als Sitzungsrichtlinie bereitgestellt, wenn eine identitätserweiterte IAM-Rollensitzung mit erstellt wird. `sts:identity_context` Die Richtlinie verhindert, dass Sie die Rollensitzung mit nicht unterstützten Diensten verwenden. AWS

Um diese Art von Rollensitzung abzurufen AWS STS, geben Sie den Wert des `sts:identity_context` Felds für die `AssumeRole` Anforderung im Anforderungsparameter `ProvidedContexts an`. Verwenden Sie `arn:aws:iam::aws:contextProvider/IdentityStore` als Wert für`ProviderArn`.

Einrichtungsprozess und Anforderungsablauf für AWS verwaltete Anwendungen

In diesem Abschnitt werden der Einrichtungsprozess und der Anforderungsablauf für AWS verwaltete Anwendungen beschrieben, die Trusted Identity Propagation verwenden und ein webbasiertes Single Sign-On-Erlebnis bieten.

Das folgende Diagramm bietet einen Überblick über diesen Prozess.



Die folgenden Schritte bieten zusätzliche Informationen zu diesem Prozess.

1. Verwenden Sie die Konsole für die AWS verwaltete Anwendung oder die Anwendungs-APIs, um Folgendes zu tun:
   a. Connect die Anwendung mit Ihrer Instanz von IAM Identity Center.
   b. Richten Sie Berechtigungen ein, um zu autorisieren, auf welche Anwendungsressourcen ein Benutzer zugreifen kann.
2. Der Anforderungsablauf beginnt, wenn ein Benutzer eine AWS verwaltete Anwendung öffnet, die Zugriff auf Ressourcen anfordern kann (eine anfordernde Anwendung).
3. Um ein Token für den Zugriff auf die empfangende AWS verwaltete Anwendung zu erhalten, initiiert die anfordernde AWS verwaltete Anwendung eine Anmeldeanforderung beim IAM Identity Center.

   Wenn der Benutzer nicht angemeldet ist, löst IAM Identity Center eine Benutzerauthentifizierung an die von Ihnen angegebene Identitätsquelle aus. Dadurch wird eine neue AWS Access-Portal-Sitzung für den Benutzer mit der Dauer erstellt, die Sie in IAM Identity Center konfiguriert haben. IAM Identity Center generiert dann ein Token, das der Sitzung zugeordnet ist, und die Anwendung kann für die verbleibende Dauer der AWS Zugriffsportalsitzung des Benutzers ausgeführt werden.

Wenn sich der Benutzer von seiner Anwendung abmeldet oder wenn Sie seine Sitzung löschen, endet die Sitzung automatisch innerhalb von zwei Stunden.

4. Die AWS verwaltete Anwendung initiiert eine Anfrage an die empfangende Anwendung und stellt ihr Token bereit.
5. Die empfangende Anwendung ruft das IAM Identity Center auf, um die Identität des Benutzers und die im Token codierten Bereiche abzurufen. Die empfangende Anwendung kann auch Anfragen zum Abrufen von Benutzerattributen oder Gruppenmitgliedschaften des Benutzers aus dem Identity Center-Verzeichnis stellen.
6. Die empfangende Anwendung verwendet ihre Autorisierungskonfiguration, um festzustellen, ob der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen.
7. Wenn der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen, beantwortet die empfangende Anwendung die Anfrage.
8. Die Identität des Benutzers, die in seinem Namen ausgeführten Aktionen und andere Ereignisse, die in den Protokollen und AWS CloudTrail Ereignissen der empfangenden Anwendung aufgezeichnet wurden. Die spezifische Art und Weise, wie diese Informationen protokolliert werden, ist je nach Anwendung unterschiedlich.

Verwendung von Trusted Identity Propagation mit vom Kunden verwalteten Anwendungen

Durch die Weitergabe vertrauenswürdiger Identitäten kann eine vom Kunden verwaltete Anwendung im Namen eines Benutzers Zugriff auf Daten in AWS Diensten anfordern. Die Datenzugriffsverwaltung basiert auf der Identität eines Benutzers, sodass Administratoren den Zugriff auf der Grundlage der bestehenden Benutzer- und Gruppenmitgliedschaften der Benutzer gewähren können. Die Identität des Benutzers, die in seinem Namen ausgeführten Aktionen und andere Ereignisse werden in dienstspezifischen Protokollen und CloudTrail Ereignissen aufgezeichnet.

Bei der Weitergabe vertrauenswürdiger Identitäten kann sich ein Benutzer bei einer vom Kunden verwalteten Anwendung anmelden, und diese Anwendung kann die Identität des Benutzers bei Anfragen zum Zugriff auf Daten in AWS Diensten weitergeben.

> **Important**
>
> Um auf einen AWS Service zugreifen zu können, müssen vom Kunden verwaltete Anwendungen ein Token von einem vertrauenswürdigen Token-Aussteller erhalten, der sich außerhalb von IAM Identity Center befindet. Ein vertrauenswürdiger Token-Aussteller ist

ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Anfragen für den Zugriff auf AWS Dienste initiieren (Anwendungen empfangen). Weitere Informationen finden Sie unter Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten.

Themen

- Richten Sie vom Kunden verwaltete OAuth 2.0-Anwendungen für die Verbreitung vertrauenswürdiger Identitäten ein
- Geben Sie vertrauenswürdige Anwendungen an

Richten Sie vom Kunden verwaltete OAuth 2.0-Anwendungen für die Verbreitung vertrauenswürdiger Identitäten ein

Um eine vom Kunden verwaltete OAuth 2.0-Anwendung für die Verbreitung vertrauenswürdiger Identitäten einzurichten, müssen Sie sie zunächst zu IAM Identity Center hinzufügen. Gehen Sie wie folgt vor, um Ihre Anwendung zu IAM Identity Center hinzuzufügen.

Themen

- Schritt 1: Wählen Sie den Anwendungstyp
- Schritt 2: Geben Sie die Anwendungsdetails an
- Schritt 3: Geben Sie die Authentifizierungseinstellungen an
- Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an
- Schritt 5: Überprüfen und konfigurieren

Schritt 1: Wählen Sie den Anwendungstyp

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „Vom Kunden verwaltet“.
4. Wählen Sie Anwendung hinzufügen.
5. Wählen Sie auf der Seite Anwendungstyp auswählen unter Setup-Einstellungen die Option Ich habe eine Anwendung, die ich einrichten möchte aus.
6. Wählen Sie unter Anwendungstyp die Option OAuth 2.0 aus.

7. Wählen Sie Weiter, um zur nächsten Seite zu gelangen. Schritt 2: Geben Sie die Anwendungsdetails an

Schritt 2: Geben Sie die Anwendungsdetails an

1. Geben Sie auf der Seite Anwendungsdetails angeben unter Anwendungsname und Beschreibung einen Anzeigenamen für die Anwendung ein, z. **`MyApp`** B. Geben Sie dann eine Beschreibung ein.
2. Wählen Sie unter Zuweisungsmethode für Benutzer und Gruppen eine der folgenden Optionen aus:

   - Zuweisungen erforderlich — Erlauben Sie nur Benutzern und Gruppen von IAM Identity Center, die dieser Anwendung zugewiesen sind, Zugriff auf die Anwendung.

     Sichtbarkeit der Anwendungskachel — Nur Benutzer, die der Anwendung direkt oder über eine Gruppenzuweisung zugewiesen wurden, können die Anwendungskachel im AWS Access Portal anzeigen, sofern die Anwendungssichtbarkeit im AWS Access Portal auf Sichtbar gesetzt ist.
   - Keine Zuweisungen erforderlich — Erlauben Sie allen autorisierten IAM Identity Center-Benutzern und -Gruppen den Zugriff auf diese Anwendung.

     Sichtbarkeit der Anwendungskachel — Die Anwendungskachel ist für alle Benutzer sichtbar, die sich beim AWS Access Portal anmelden, es sei denn, die Sichtbarkeit der Anwendung im AWS Access Portal ist auf Nicht sichtbar gesetzt.
3. Geben Sie unter AWS Zugriffsportal die URL ein, über die Benutzer auf die Anwendung zugreifen können, und geben Sie an, ob die Anwendungskachel im AWS Zugriffsportal sichtbar sein soll oder nicht. Wenn Sie Nicht sichtbar wählen, können nicht einmal zugewiesene Benutzer die Anwendungskachel sehen.
4. Wählen Sie unter Tags (optional) die Option Neues Tag hinzufügen aus und geben Sie dann Werte für Schlüssel und Wert an (optional).

   Informationen zu Tags siehe Markieren von AWS IAM Identity Center-Ressourcen.
5. Wählen Sie Weiter und fahren Sie mit der nächsten Seite fortSchritt 3: Geben Sie die Authentifizierungseinstellungen an.

Schritt 3: Geben Sie die Authentifizierungseinstellungen an

Um eine vom Kunden verwaltete Anwendung, die OAuth 2.0 unterstützt, zu IAM Identity Center hinzuzufügen, müssen Sie einen vertrauenswürdigen Token-Aussteller angeben. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Anfragen (Anfragen) für den Zugriff auf AWS verwaltete Anwendungen (Empfangen von Anwendungen) initiieren.

1. Führen Sie auf der Seite Authentifizierungseinstellungen angeben unter Vertrauenswürdige Token-Aussteller einen der folgenden Schritte aus:

   - So verwenden Sie einen vorhandenen vertrauenswürdigen Token-Aussteller:

     Aktivieren Sie das Kontrollkästchen neben dem Namen des vertrauenswürdigen Token-Ausstellers, den Sie verwenden möchten.

   - Um einen neuen vertrauenswürdigen Token-Emittenten hinzuzufügen:

     1. Wählen Sie Vertrauenswürdigen Token-Aussteller erstellen aus.
     2. Ein neuer Browser-Tab wird geöffnet. Folgen Sie den Schritten 5 bis 8 inWie füge ich einen vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzu.
     3. Nachdem Sie diese Schritte abgeschlossen haben, kehren Sie zu dem Browserfenster zurück, das Sie für die Einrichtung Ihrer Anwendung verwenden, und wählen Sie den vertrauenswürdigen Token-Aussteller aus, den Sie gerade hinzugefügt haben.
     4. Aktivieren Sie in der Liste der vertrauenswürdigen Token-Emittenten das Kontrollkästchen neben dem Namen des vertrauenswürdigen Token-Ausstellers, den Sie gerade hinzugefügt haben.

        Nachdem Sie einen vertrauenswürdigen Token-Aussteller ausgewählt haben, wird der Abschnitt Ausgewählte vertrauenswürdige Token-Aussteller konfigurieren angezeigt.

2. Geben Sie unter Ausgewählte vertrauenswürdige Token-Emittenten konfigurieren den Aud-Anspruch ein. Der Aud-Anspruch identifiziert die Zielgruppe (Empfänger) für das Token, das vom vertrauenswürdigen Token-Emittenten generiert wurde. Weitere Informationen finden Sie unter Ein Anspruch geltend machen.
3. Um zu verhindern, dass sich Ihre Benutzer erneut authentifizieren müssen, wenn sie diese Anwendung verwenden, wählen Sie Benutzerauthentifizierung für aktive Anwendungssitzung automatisch aktualisieren. Wenn diese Option ausgewählt ist, aktualisiert sie das Zugriffstoken für die Sitzung alle 60 Minuten, bis die Sitzung abläuft oder der Benutzer die Sitzung beendet.

4. Wählen Sie Weiter und fahren Sie mit der nächsten Seite fort. Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an

Schritt 4: Geben Sie die Anmeldeinformationen für die Anwendung an

Führen Sie die Schritte in diesem Verfahren aus, um die Anmeldeinformationen anzugeben, die Ihre Anwendung verwendet, um Token-Austauschaktionen mit vertrauenswürdigen Anwendungen durchzuführen. Diese Anmeldeinformationen werden in einer ressourcenbasierten Richtlinie verwendet. Die Richtlinie erfordert, dass Sie einen Prinzipal angeben, der berechtigt ist, die in der Richtlinie angegebenen Aktionen auszuführen. Sie müssen einen Prinzipal angeben, auch wenn sich die vertrauenswürdigen Anwendungen in derselben befinden AWS-Konto.

> **Note**
>
> Wenn Sie Berechtigungen mit Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen.

Diese Richtlinie erfordert die `sso-oauth:CreateTokenWithIAM` Aktion.

1. Führen Sie auf der Seite „Anmeldeinformationen für die Anwendung angeben“ einen der folgenden Schritte aus:

   - So geben Sie schnell eine oder mehrere IAM-Rollen an:

     1. Wählen Sie Eine oder mehrere IAM-Rollen eingeben aus.
     2. Geben Sie unter IAM-Rollen eingeben den Amazon-Ressourcennamen (ARN) einer vorhandenen IAM-Rolle an. Verwenden Sie die folgende Syntax, um den ARN anzugeben. Der Teil zur Angabe der Region im ARN ist leer, da IAM-Ressourcen globale Ressourcen sind.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Weitere Informationen finden Sie im Benutzerhandbuch unter Kontenübergreifender Zugriff mithilfe ressourcenbasierter Richtlinien und IAM-ARNs.AWS Identity and Access Management

- So bearbeiten Sie die Richtlinie manuell (erforderlich, wenn Sie keine Anmeldeinformationen angeben):AWS
  1. Wählen Sie Anwendungsrichtlinie bearbeiten aus.
  2. Ändern Sie Ihre Richtlinie, indem Sie Text in das JSON-Textfeld eingeben oder einfügen.
  3. Beheben Sie alle Sicherheitswarnungen, Fehler oder allgemeinen Warnungen, die während der Richtlinienvalidierung generiert wurden. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Überprüfen von IAM-Richtlinien.

2. Wählen Sie Weiter und fahren Sie mit der nächsten Seite fort,. Schritt 5: Überprüfen und konfigurieren

Schritt 5: Überprüfen und konfigurieren

1. Überprüfen Sie auf der Seite Überprüfen und konfigurieren die von Ihnen getroffenen Entscheidungen. Um Änderungen vorzunehmen, wählen Sie den gewünschten Konfigurationsabschnitt aus, wählen Sie Bearbeiten und nehmen Sie dann die erforderlichen Änderungen vor.
2. Wenn Sie fertig sind, wählen Sie Anwendung hinzufügen.
3. Die von Ihnen hinzugefügte Anwendung wird in der Liste der vom Kunden verwalteten Anwendungen angezeigt.
4. Nachdem Sie Ihre vom Kunden verwaltete Anwendung in IAM Identity Center eingerichtet haben, müssen Sie einen oder mehrere AWS Dienste oder vertrauenswürdige Anwendungen für die Identitätsweitergabe angeben. Auf diese Weise können sich Benutzer bei Ihrer vom Kunden verwalteten Anwendung anmelden und auf Daten in der vertrauenswürdigen Anwendung zugreifen.

   Weitere Informationen finden Sie unter Geben Sie vertrauenswürdige Anwendungen an .

Geben Sie vertrauenswürdige Anwendungen an

Nachdem Sie Ihre vom Kunden verwaltete Anwendung eingerichtet haben, müssen Sie einen oder mehrere vertrauenswürdige AWS Dienste oder vertrauenswürdige Anwendungen für die Identitätsweitergabe angeben. Geben Sie einen AWS Dienst an, der Daten enthält, auf die Benutzer Ihrer vom Kunden verwalteten Anwendungen zugreifen müssen. Wenn sich Ihre Benutzer bei Ihrer vom Kunden verwalteten Anwendung anmelden, gibt diese Anwendung die Identität Ihrer Benutzer an die vertrauenswürdige Anwendung weiter.

Gehen Sie wie folgt vor, um einen Dienst auszuwählen, und geben Sie dann einzelne Anwendungen an, denen Sie für diesen Dienst vertrauen möchten.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie die Registerkarte „Vom Kunden verwaltet“.
4. Wählen Sie in der Liste „Vom Kunden verwaltete Anwendungen“ die OAuth 2.0-Anwendung aus, für die Sie Zugriffsanfragen einleiten möchten. Dies ist die Anwendung, bei der sich Ihre Benutzer anmelden.
5. Wählen Sie auf der Detailseite unter Vertrauenswürdige Anwendungen für die Weitergabe von Identitäten die Option Vertrauenswürdige Anwendungen angeben aus.
6. Wählen Sie unter Setup-Typ die Option Einzelne Anwendungen aus, geben Sie den Zugriff an, und klicken Sie dann auf Weiter.
7. Wählen Sie auf der Seite Service auswählen den AWS Dienst aus, der über Anwendungen verfügt, denen Ihre vom Kunden verwaltete Anwendung bei der Identitätsweitergabe vertrauen kann, und klicken Sie dann auf Weiter.

   Der Dienst, den Sie auswählen, definiert die Anwendungen, denen vertraut werden kann. Im nächsten Schritt wählen Sie Anwendungen aus.
8. Wählen Sie auf der Seite „Anwendungen auswählen“ die Option Einzelne Anwendungen aus, aktivieren Sie das Kontrollkästchen für jede Anwendung, die Zugriffsanfragen empfangen kann, und klicken Sie dann auf Weiter.
9. Führen Sie auf der Seite Zugriff konfigurieren unter Konfigurationsmethode einen der folgenden Schritte aus:

   - Zugriff pro Anwendung auswählen — Wählen Sie diese Option, um für jede Anwendung unterschiedliche Zugriffsebenen zu konfigurieren. Wählen Sie die Anwendung aus, für die Sie die Zugriffsebene konfigurieren möchten, und klicken Sie dann auf Zugriff bearbeiten. Ändern Sie unter Zugriffsebene die Zugriffsebenen nach Bedarf und wählen Sie dann Änderungen speichern aus.
   - Gleiche Zugriffsebene auf alle Anwendungen anwenden — Wählen Sie diese Option, wenn Sie die Zugriffsebenen nicht pro Anwendung konfigurieren müssen.
10. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Konfiguration überprüfen die von Ihnen getroffenen Entscheidungen. Um Änderungen vorzunehmen, wählen Sie den gewünschten

Konfigurationsabschnitt aus, wählen Sie Zugriff bearbeiten und nehmen Sie dann die erforderlichen Änderungen vor.

12. Wenn Sie fertig sind, wählen Sie Anwendungen vertrauen aus.

Verwenden Sie Anwendungen mit einem vertrauenswürdigen Token-Emittenten

Vertrauenswürdige Token-Emittenten ermöglichen es Ihnen, Trusted Identity Propagation mit Anwendungen zu verwenden, die sich außerhalb von authentifizieren. AWS Mit vertrauenswürdigen Token-Emittenten können Sie diese Anwendungen autorisieren, im Namen ihrer Benutzer Anfragen für den Zugriff auf verwaltete Anwendungen zu stellen. AWS

Die folgenden Themen beschreiben, wie vertrauenswürdige Token-Emittenten funktionieren, und bieten Anleitungen zur Einrichtung.

Themen

Überblick über vertrauenswürdige Token-Emittenten

Die Verbreitung vertrauenswürdiger Identitäten bietet einen Mechanismus, mit dem Anwendungen, die AWS sich außerhalb von authentifizieren, mithilfe eines vertrauenswürdigen Token-Ausstellers Anfragen im Namen ihrer Benutzer stellen können. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der signierte Token erstellt. Diese Token autorisieren Anwendungen, die Anfragen (Anträge anfordern) für den Zugriff auf AWS Dienste (Empfangen von Anwendungen) initiieren. Anfordernde Anwendungen initiieren Zugriffsanfragen im Namen von Benutzern, die vom vertrauenswürdigen Token-Aussteller authentifiziert werden. Die Benutzer sind sowohl dem vertrauenswürdigen Token-Aussteller als auch dem IAM Identity Center bekannt.

AWS Dienste, die Anfragen erhalten, verwalten eine detaillierte Autorisierung ihrer Ressourcen auf der Grundlage ihrer Benutzer und Gruppenzugehörigkeit, wie sie im Identity Center-Verzeichnis

dargestellt sind. AWS Dienste können die Token des externen Token-Ausstellers nicht direkt verwenden.

Um dieses Problem zu lösen, bietet IAM Identity Center der anfragenden Anwendung oder einem AWS Treiber, den die anfordernde Anwendung verwendet, die Möglichkeit, das vom vertrauenswürdigen Token-Aussteller ausgegebene Token gegen ein von IAM Identity Center generiertes Token auszutauschen. Das von IAM Identity Center generierte Token bezieht sich auf den entsprechenden IAM Identity Center-Benutzer. Die anfordernde Anwendung oder der Treiber verwendet das neue Token, um eine Anfrage an die empfangende Anwendung zu initiieren. Da das neue Token auf den entsprechenden Benutzer in IAM Identity Center verweist, kann die empfangende Anwendung den angeforderten Zugriff auf der Grundlage der Benutzer- oder Gruppenmitgliedschaft, wie sie in IAM Identity Center dargestellt ist, autorisieren.

> **Important**
>
> Die Auswahl eines OAuth 2.0-Autorisierungsservers, der als vertrauenswürdiger Token-Aussteller hinzugefügt werden soll, ist eine Sicherheitsentscheidung, die sorgfältig geprüft werden muss. Wählen Sie nur vertrauenswürdige Token-Emittenten aus, denen Sie vertrauen, dass sie die folgenden Aufgaben ausführen:
>
> - Authentifizieren Sie den Benutzer, der im Token angegeben ist.
> - Autorisieren Sie den Zugriff dieses Benutzers auf die empfangende Anwendung.
> - Generieren Sie ein Token, das von IAM Identity Center gegen ein von IAM Identity Center erstelltes Token eingetauscht werden kann.

Voraussetzungen und Überlegungen für vertrauenswürdige Token-Emittenten

Bevor Sie einen vertrauenswürdigen Token-Emittenten einrichten, sollten Sie sich mit den folgenden Voraussetzungen und Überlegungen vertraut machen.

- Konfiguration eines vertrauenswürdigen Token-Ausstellers

  Sie müssen einen OAuth 2.0-Autorisierungsserver (den vertrauenswürdigen Token-Aussteller) konfigurieren. Obwohl der vertrauenswürdige Token-Aussteller in der Regel der Identitätsanbieter ist, den Sie als Identitätsquelle für IAM Identity Center verwenden, muss dies nicht der Fall sein. Informationen zur Einrichtung des vertrauenswürdigen Token-Ausstellers finden Sie in der Dokumentation des jeweiligen Identitätsanbieters.

> **Note**
>
> Sie können bis zu 10 vertrauenswürdige Token-Aussteller für die Verwendung mit IAM Identity Center konfigurieren, sofern Sie die Identität jedes Benutzers im vertrauenswürdigen Token-Aussteller einem entsprechenden Benutzer im IAM Identity Center zuordnen.

- Der OAuth 2.0-Autorisierungsserver (der vertrauenswürdige Token-Aussteller), der das Token erstellt, muss über einen OpenID Connect (OIDC) -Erkennungsendpunkt verfügen, über den IAM Identity Center öffentliche Schlüssel zur Überprüfung der Tokensignaturen abrufen kann. Weitere Informationen finden Sie unter URL des OIDC-Discovery-Endpunkts (Aussteller-URL).
- Vom vertrauenswürdigen Token-Emittenten ausgegebene Token

  Token des vertrauenswürdigen Token-Emittenten müssen die folgenden Anforderungen erfüllen:

  - Das Token muss signiert sein und im JSON-Web-Token-Format (JWT) den RS256-Algorithmus verwenden.
  - Das Token muss die folgenden Ansprüche enthalten:
    - Issuer (iss) — Die Entität, die das Token ausgestellt hat. Dieser Wert muss mit dem Wert übereinstimmen, der im OIDC-Erkennungsendpunkt (Aussteller-URL) des vertrauenswürdigen Token-Ausstellers konfiguriert ist.
    - Betreff (Sub) — Der authentifizierte Benutzer.
    - Zielgruppe (aud) — Der beabsichtigte Empfänger des Tokens. Dies ist der AWS Dienst, auf den zugegriffen wird, nachdem das Token gegen ein Token von IAM Identity Center ausgetauscht wurde. Weitere Informationen finden Sie unter Ein Anspruch geltend machen.
    - Ablaufzeit (exp) — Die Zeit, nach der das Token abläuft.
    -
  - Das Token kann ein Identitätstoken oder ein Zugriffstoken sein.
  - Das Token muss über ein Attribut verfügen, das eindeutig einem IAM Identity Center-Benutzer zugeordnet werden kann.
- Optionale Ansprüche

  IAM Identity Center unterstützt alle optionalen Ansprüche, die in RFC 7523 definiert sind. Weitere Informationen finden Sie in Abschnitt 3: JWT-Format und Verarbeitungsanforderungen dieses RFC.

Das Token kann beispielsweise einen JTI-Anspruch (JWT-ID) enthalten. Dieser Anspruch verhindert, sofern vorhanden, dass Token mit derselben JTI für den Tokenaustausch wiederverwendet werden. Weitere Informationen zu JTI-Ansprüchen finden Sie unter. Einzelheiten zum JTI-Anspruch

- IAM Identity Center-Konfiguration für die Zusammenarbeit mit einem vertrauenswürdigen Token-Aussteller

  Sie müssen außerdem IAM Identity Center aktivieren, die Identitätsquelle für IAM Identity Center konfigurieren und Benutzer bereitstellen, die den Benutzern im Verzeichnis des vertrauenswürdigen Token-Ausstellers entsprechen.

  Dazu müssen Sie einen der folgenden Schritte ausführen:

  - Synchronisieren Sie Benutzer mithilfe des SCIM 2.0-Protokolls (System for Cross-Domain Identity Management) mit dem IAM Identity Center.
  - Erstellen Sie die Benutzer direkt im IAM Identity Center.

> **Note**
>
> Vertrauenswürdige Token-Aussteller werden nicht unterstützt, wenn Sie den Active Directory-Domänendienst als Identitätsquelle verwenden.

Einzelheiten zum JTI-Anspruch

Wenn IAM Identity Center eine Anfrage zum Austausch eines Tokens erhält, das IAM Identity Center bereits ausgetauscht hat, schlägt die Anfrage fehl. Um die Wiederverwendung eines Tokens für den Token-Austausch zu erkennen und zu verhindern, können Sie einen JTI-Anspruch angeben. IAM Identity Center schützt vor der Wiederholung von Token, die auf den Ansprüchen im Token basieren.

Nicht alle OAuth 2.0-Autorisierungsserver fügen Tokens einen JTI-Anspruch hinzu. Bei einigen OAuth 2.0-Autorisierungsservern können Sie möglicherweise kein JTI als benutzerdefinierten Anspruch hinzufügen. OAuth 2.0-Autorisierungsserver, die die Verwendung eines JTI-Anspruchs unterstützen, fügen diesen Anspruch möglicherweise nur zu Identitätstoken, nur Zugriffstoken oder beiden hinzu. Weitere Informationen finden Sie in der Dokumentation zu Ihrem OAuth 2.0-Autorisierungsserver.

Informationen zum Erstellen von Anwendungen, die Token austauschen, finden Sie in der IAM Identity Center API-Dokumentation. Informationen zur Konfiguration einer vom Kunden verwalteten

Anwendung zum Abrufen und Austauschen der richtigen Token finden Sie in der Dokumentation zur Anwendung.

Konfigurationseinstellungen für vertrauenswürdigen Token-Emittenten

In den folgenden Abschnitten werden die Einstellungen beschrieben, die für die Einrichtung und Verwendung eines vertrauenswürdigen Token-Ausstellers erforderlich sind.

Themen

URL des OIDC-Discovery-Endpunkts (Aussteller-URL)

Wenn Sie der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzufügen, müssen Sie die URL des OIDC-Discovery-Endpunkts angeben. Auf diese URL wird üblicherweise mit ihrer relativen URL, verwiesen. `/.well-known/openid-configuration` In der IAM Identity Center-Konsole wird diese URL als Aussteller-URL bezeichnet.

> **Note**
>
> Sie müssen die URL des Discovery-Endpunkts bis und ohne einfügen. `.well-known/openid-configuration` Wenn sie in der URL enthalten `.well-known/openid-configuration` ist, funktioniert die Konfiguration des vertrauenswürdigen Token-Ausstellers nicht. Da IAM Identity Center diese URL nicht validiert, schlägt die Einrichtung des vertrauenswürdigen Token-Ausstellers ohne Benachrichtigung fehl, wenn die URL nicht korrekt formatiert ist.

IAM Identity Center verwendet diese URL, um zusätzliche Informationen über den vertrauenswürdigen Token-Aussteller abzurufen. Beispielsweise verwendet IAM Identity Center diese URL, um die Informationen abzurufen, die zur Überprüfung der vom vertrauenswürdigen Token-Emittenten generierten Token erforderlich sind. Wenn Sie einen vertrauenswürdigen Token-Aussteller zu IAM Identity Center hinzufügen, müssen Sie diese URL angeben. Die URL finden Sie in der Dokumentation des OAuth 2.0-Autorisierungsserver-Anbieters, den Sie zum Generieren von Tokens für Ihre Anwendung verwenden, oder wenden Sie sich direkt an den Anbieter, um Unterstützung zu erhalten.

Attributzuordnung

Mithilfe von Attributzuordnungen kann IAM Identity Center den Benutzer, der in einem von einem vertrauenswürdigen Token-Emittenten ausgegebenen Token repräsentiert wird, einem einzelnen Benutzer in IAM Identity Center zuordnen. Sie müssen die Attributzuordnung angeben, wenn Sie den vertrauenswürdigen Token-Aussteller zu IAM Identity Center hinzufügen. Diese Attributzuordnung wird in einem Anspruch in dem Token verwendet, das vom vertrauenswürdigen Token-Emittenten generiert wird. Der Wert im Anspruch wird für die Suche im IAM Identity Center verwendet. Bei der Suche wird das angegebene Attribut verwendet, um einen einzelnen Benutzer in IAM Identity Center abzurufen, der als Benutzer innerhalb von IAM Identity Center verwendet wird. AWS Der von Ihnen gewählte Anspruch muss einem Attribut in einer festen Liste verfügbarer Attribute im IAM Identity Center-Identitätsspeicher zugeordnet werden. Sie können eines der folgenden IAM Identity Center-Identitätsspeicher-Attribute wählen: Benutzername, E-Mail und externe ID. Der Wert für das Attribut, das Sie in IAM Identity Center angeben, muss für jeden Benutzer eindeutig sein.

Ein Anspruch geltend machen

Ein Aud-Antrag identifiziert die Zielgruppe (Empfänger), für die ein Token bestimmt ist. Wenn sich die Anwendung, die den Zugriff anfordert, über einen Identitätsanbieter authentifiziert, der nicht mit dem IAM Identity Center verbunden ist, muss dieser Identitätsanbieter als vertrauenswürdiger Token-Aussteller eingerichtet werden. Die Anwendung, die die Zugriffsanfrage empfängt (die empfangende Anwendung), muss das vom vertrauenswürdigen Token-Aussteller generierte Token gegen ein von IAM Identity Center generiertes Token austauschen.

Informationen darüber, wie Sie die Aud-Claim-Werte für die empfangende Anwendung abrufen können, da sie beim vertrauenswürdigen Token-Aussteller registriert sind, finden Sie in der Dokumentation Ihres vertrauenswürdigen Token-Ausstellers oder wenden Sie sich an den Administrator des vertrauenswürdigen Token-Ausstellers, um Unterstützung zu erhalten.

Einen vertrauenswürdigen Token-Emittenten einrichten

Um die Verbreitung vertrauenswürdiger Identitäten für eine Anwendung zu aktivieren, die sich extern bei IAM Identity Center authentifiziert, müssen ein oder mehrere Administratoren einen vertrauenswürdigen Token-Aussteller einrichten. Ein vertrauenswürdiger Token-Aussteller ist ein OAuth 2.0-Autorisierungsserver, der Token an Anwendungen ausgibt, die Anfragen initiieren (Anwendungen anfordern). Die Token autorisieren diese Anwendungen, im Namen ihrer Benutzer Anfragen an eine empfangende Anwendung (einen Dienst) zu stellen. AWS

Themen

- Koordinierung der administrativen Rollen und Zuständigkeiten
- Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Emittenten
- Wie füge ich einen vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzu
- Wie können Sie die Einstellungen für vertrauenswürdige Token-Aussteller in der IAM Identity Center-Konsole anzeigen oder bearbeiten
- Einrichtungsprozess und Anforderungsablauf für Anwendungen, die einen vertrauenswürdigen Token-Aussteller verwenden

Koordinierung der administrativen Rollen und Zuständigkeiten

In einigen Fällen kann ein einziger Administrator alle erforderlichen Aufgaben für die Einrichtung eines vertrauenswürdigen Token-Emittenten ausführen. Wenn mehrere Administratoren diese Aufgaben ausführen, ist eine enge Abstimmung erforderlich. In der folgenden Tabelle wird beschrieben, wie mehrere Administratoren gemeinsam einen vertrauenswürdigen Token-Aussteller einrichten und den AWS Dienst für dessen Verwendung konfigurieren können.

> **Note**
>
> Bei der Anwendung kann es sich um einen beliebigen AWS Dienst handeln, der in IAM Identity Center integriert ist und die Verbreitung vertrauenswürdiger Identitäten unterstützt.

Weitere Informationen finden Sie unter Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Emittenten.

Rolle	Führt diese Aufgaben aus	Koordiniert mit
IAM Identity Center-Administrator	Fügt den externen IdP als vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzu. Hilft bei der Einrichtung der korrekten Attributzuordnung zwischen IAM Identity Center und dem externen IdP.	Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller) AWS Dienstadministrator

Rolle	Führt diese Aufgaben aus	Koordiniert mit
	Benachrichtigt den AWS Dienstadministrator, wenn der vertrauenswürdige Token-Aussteller der IAM Identity Center-Konsole hinzugefügt wird.	
Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller)	Konfiguriert den externen IdP für die Ausgabe von Tokens. Hilft bei der Einrichtung der korrekten Attributzuordnung zwischen IAM Identity Center und dem externen IdP. Stellt dem Dienstadministrator den Namen der Zielgruppe (Aud-Anspruch) zur AWS Verfügung.	IAM Identity Center-Administrator AWS Dienstadministrator
AWS Dienstadministrator	Sucht in der AWS Servicekonsole nach dem vertrauenswürdigen Token-Aussteller. Der vertrauenswürdige Token-Aussteller wird in der AWS Servicekonsole angezeigt, nachdem der IAM Identity Center-Administrator ihn der IAM Identity Center-Konsole hinzugefügt hat. Konfiguriert den AWS Dienst für die Verwendung des vertrauenswürdigen Token-Ausstellers.	IAM Identity Center-Administrator Externer IdP-Administrator (vertrauenswürdiger Token-Aussteller)

Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Emittenten

Um einen vertrauenswürdigen Token-Aussteller einzurichten, müssen ein IAM Identity Center-Administrator, ein externer IdP-Administrator (vertrauenswürdiger Token-Aussteller) und ein Anwendungsadministrator die folgenden Aufgaben ausführen.

> **Note**
>
> Bei der Anwendung kann es sich um einen beliebigen AWS Dienst handeln, der in IAM Identity Center integriert ist und die Verbreitung vertrauenswürdiger Identitäten unterstützt.

1. Den vertrauenswürdigen Token-Aussteller zu IAM Identity Center hinzufügen — Der IAM Identity Center-Administrator fügt den vertrauenswürdigen Token-Aussteller mithilfe der IAM Identity Center-Konsole oder der APIs hinzu. Für diese Konfiguration müssen Sie Folgendes angeben:
   - Ein Name für den vertrauenswürdigen Token-Emittenten
   - Die URL des OIDC-Discovery-Endpunkts (in der IAM Identity Center-Konsole wird diese URL als Aussteller-URL bezeichnet).
   - Attributzuordnung für die Benutzersuche. Diese Attributzuordnung wird in einem Anspruch in dem Token verwendet, das vom vertrauenswürdigen Token-Emittenten generiert wird. Der Wert im Anspruch wird für die Suche im IAM Identity Center verwendet. Die Suche verwendet das angegebene Attribut, um einen einzelnen Benutzer in IAM Identity Center abzurufen.
2. Connect AWS Service mit IAM Identity Center verbinden — Der AWS Dienstadministrator muss die Anwendung über die Konsole für die Anwendung oder die Anwendungs-APIs mit dem IAM Identity Center verbinden.

   Nachdem der vertrauenswürdige Token-Aussteller der IAM Identity Center-Konsole hinzugefügt wurde, ist er auch in der AWS Servicekonsole sichtbar und kann vom Service-Administrator ausgewählt werden. AWS
3. Konfigurieren Sie die Verwendung des Token-Austauschs — In der AWS Servicekonsole konfiguriert AWS der AWS Service-Administrator den Service so, dass er vom vertrauenswürdigen Token-Aussteller ausgegebene Token akzeptiert. Diese Token werden gegen vom IAM Identity Center generierte Token ausgetauscht. Dazu müssen Sie den Namen des vertrauenswürdigen Token-Ausstellers aus Schritt 1 und den Aud-Claim-Wert angeben, der AWS dem Service entspricht.

   Der vertrauenswürdige Token-Emittent fügt den Aud-Anspruchswert in das von ihm ausgegebene Token ein, um anzuzeigen, dass das Token für die Verwendung durch den AWS Dienst vorgesehen ist. Um diesen Wert zu erhalten, wenden Sie sich an den Administrator des vertrauenswürdigen Token-Ausstellers.

Wie füge ich einen vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzu

In einer Organisation mit mehreren Administratoren wird diese Aufgabe von einem IAM Identity Center-Administrator ausgeführt. Wenn Sie der IAM Identity Center-Administrator sind, müssen Sie auswählen, welcher externe IdP als vertrauenswürdiger Token-Aussteller verwendet werden soll.

Um einen vertrauenswürdigen Token-Aussteller zur IAM Identity Center-Konsole hinzuzufügen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie unter Vertrauenswürdige Token-Aussteller die Option Vertrauenswürdigen Token-Aussteller erstellen aus.
5. Gehen Sie auf der Seite Einen externen IdP für die Ausgabe vertrauenswürdiger Token einrichten unter Informationen zum vertrauenswürdigen Token-Emittenten wie folgt vor:

   - Geben Sie für Issuer URL die OIDC-Discovery-URL des externen IdP an, der Token für die Verbreitung vertrauenswürdiger Identitäten ausstellt. Sie müssen die URL des Discovery-Endpunkts bis und danach angeben. `.well-known/openid-configuration` Der Administrator des externen IdP kann diese URL bereitstellen.

     > **Note**
     >
     > Hinweis: Diese URL muss mit der URL im Anspruch des Ausstellers (iss) in Tokens übereinstimmen, die für die Weitergabe vertrauenswürdiger Identitäten ausgegeben werden.

   - Geben Sie unter Name des vertrauenswürdigen Token-Ausstellers einen Namen ein, um diesen vertrauenswürdigen Token-Aussteller im IAM Identity Center und in der Anwendungskonsole zu identifizieren.
6. Gehen Sie unter Attribute zuordnen wie folgt vor:

   - Wählen Sie unter Identity Provider-Attribut ein Attribut aus der Liste aus, das einem Attribut im IAM Identity Center-Identitätsspeicher zugeordnet werden soll.
   - Wählen Sie für das IAM Identity Center-Attribut das entsprechende Attribut für die Attributzuordnung aus.

7. Wählen Sie unter Tags (optional) die Option Neues Tag hinzufügen aus, geben Sie einen Wert für Schlüssel und optional für Wert an.

   Informationen zu Tags siehe Markieren von AWS IAM Identity Center-Ressourcen.
8. Wählen Sie Vertrauenswürdigen Token-Aussteller erstellen aus.
9. Wenn Sie mit der Erstellung des vertrauenswürdigen Token-Ausstellers fertig sind, wenden Sie sich an den Anwendungsadministrator, um ihm den Namen des vertrauenswürdigen Token-Ausstellers mitzuteilen, damit er bestätigen kann, dass der vertrauenswürdige Token-Aussteller in der entsprechenden Konsole sichtbar ist.
10. Der Anwendungsadministrator muss diesen vertrauenswürdigen Token-Aussteller in der entsprechenden Konsole auswählen, um Benutzern den Zugriff auf die Anwendung über Anwendungen zu ermöglichen, die für die Weitergabe vertrauenswürdiger Identitäten konfiguriert sind.

Wie können Sie die Einstellungen für vertrauenswürdige Token-Aussteller in der IAM Identity Center-Konsole anzeigen oder bearbeiten

Nachdem Sie der IAM Identity Center-Konsole einen vertrauenswürdigen Token-Aussteller hinzugefügt haben, können Sie die entsprechenden Einstellungen anzeigen und bearbeiten.

Wenn Sie beabsichtigen, die Einstellungen des vertrauenswürdigen Token-Ausstellers zu bearbeiten, denken Sie daran, dass Benutzer dadurch den Zugriff auf alle Anwendungen verlieren können, die für die Verwendung des vertrauenswürdigen Token-Ausstellers konfiguriert sind. Um eine Unterbrechung des Benutzerzugriffs zu vermeiden, empfehlen wir, dass Sie sich mit den Administratoren aller Anwendungen abstimmen, die für die Verwendung des vertrauenswürdigen Token-Ausstellers konfiguriert sind, bevor Sie die Einstellungen bearbeiten.

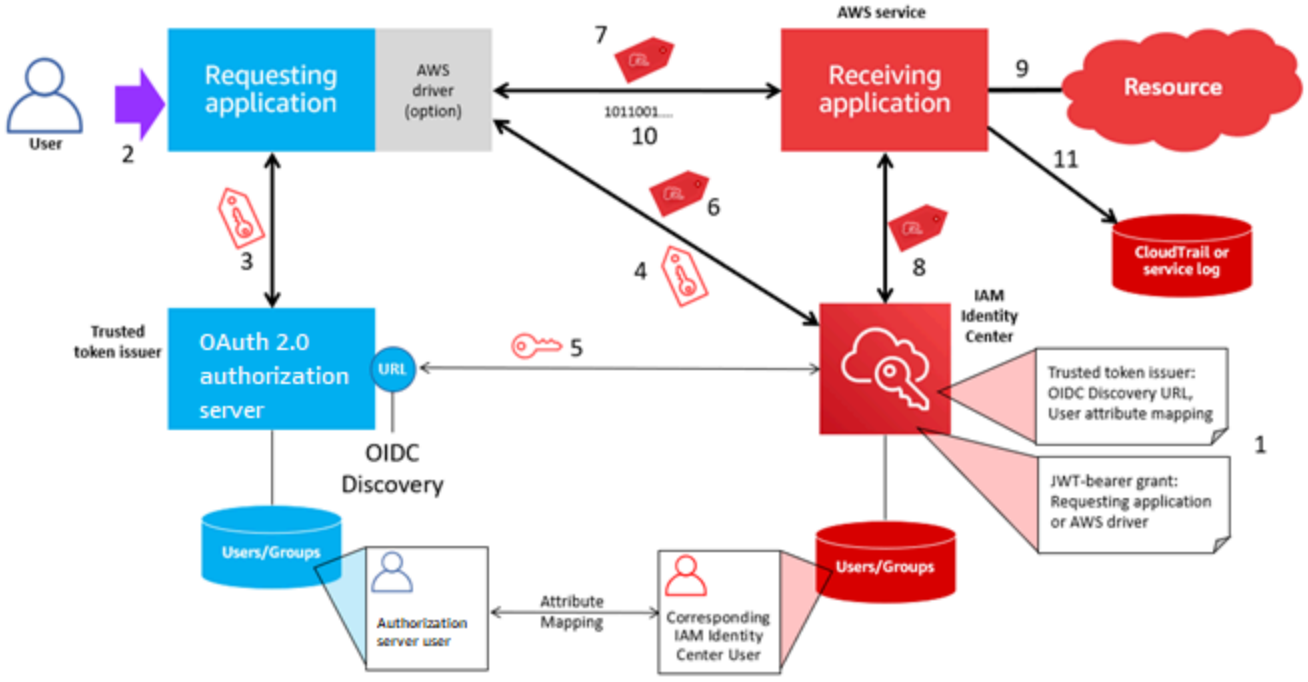
So können Sie die Einstellungen für vertrauenswürdige Token-Aussteller in der IAM Identity Center-Konsole anzeigen oder bearbeiten

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Authentifizierung.
4. Wählen Sie unter Vertrauenswürdige Token-Aussteller den vertrauenswürdigen Token-Aussteller aus, den Sie anzeigen oder bearbeiten möchten.
5. Wählen Sie Actions und anschließend Bearbeiten.

6. Auf der Seite Vertrauenswürdigen Token-Aussteller bearbeiten können Sie die Einstellungen nach Bedarf anzeigen oder bearbeiten. Sie können den Namen des vertrauenswürdigen Token-Ausstellers, die Attributzuordnungen und die Tags bearbeiten.
7. Wählen Sie Änderungen speichern aus.
8. Im Dialogfeld „Vertrauenswürdigen Token-Aussteller bearbeiten“ werden Sie aufgefordert, zu bestätigen, dass Sie Änderungen vornehmen möchten. Wählen Sie Bestätigen aus.

Einrichtungsprozess und Anforderungsablauf für Anwendungen, die einen vertrauenswürdigen Token-Aussteller verwenden

In diesem Abschnitt werden der Einrichtungsprozess und der Anforderungsablauf für Anwendungen beschrieben, die einen vertrauenswürdigen Token-Aussteller für die Weitergabe vertrauenswürdiger Identitäten verwenden. Das folgende Diagramm bietet einen Überblick über diesen Prozess.



Die folgenden Schritte bieten zusätzliche Informationen zu diesem Prozess.

1. Richten Sie das IAM Identity Center und die empfangende AWS verwaltete Anwendung so ein, dass sie einen vertrauenswürdigen Token-Aussteller verwenden. Weitere Informationen finden Sie unter Aufgaben zur Einrichtung eines vertrauenswürdigen Token-Emittenten.
2. Der Anforderungsablauf beginnt, wenn ein Benutzer die anfordernde Anwendung öffnet.

3. Die anfordernde Anwendung fordert vom vertrauenswürdigen Token-Aussteller ein Token an, um Anfragen an die empfangende AWS verwaltete Anwendung zu initiieren. Wenn sich der Benutzer noch nicht authentifiziert hat, löst dieser Prozess einen Authentifizierungsablauf aus. Das Token enthält die folgenden Informationen:
   - Der Betreff (Sub) des Benutzers.
   - Das Attribut, das IAM Identity Center verwendet, um den entsprechenden Benutzer in IAM Identity Center zu suchen.
   - Ein Zielgruppenanspruch (Aud), der einen Wert enthält, den der vertrauenswürdige Token-Aussteller der empfangenden AWS verwalteten Anwendung zuordnet. Wenn andere Ansprüche vorhanden sind, werden sie vom IAM Identity Center nicht verwendet.
4. Die anfordernde Anwendung oder der von ihr verwendete AWS Treiber leitet das Token an IAM Identity Center weiter und fordert den Austausch des Tokens gegen ein von IAM Identity Center generiertes Token an. Wenn Sie einen AWS Treiber verwenden, müssen Sie den Treiber möglicherweise für diesen Anwendungsfall konfigurieren. Weitere Informationen finden Sie in der Dokumentation der entsprechenden AWS verwalteten Anwendung.
5. IAM Identity Center verwendet den OIDC Discovery-Endpunkt, um den öffentlichen Schlüssel abzurufen, mit dem es die Authentizität des Tokens überprüfen kann. IAM Identity Center geht dann wie folgt vor:
   - Überprüft das Token.
   - Durchsucht das Identity Center-Verzeichnis. Zu diesem Zweck verwendet IAM Identity Center das zugeordnete Attribut, das im Token angegeben ist.
   - Überprüft, ob der Benutzer berechtigt ist, auf die empfangende Anwendung zuzugreifen. Wenn die AWS verwaltete Anwendung so konfiguriert ist, dass Zuweisungen an Benutzer und Gruppen erforderlich sind, muss der Benutzer über eine direkte oder gruppenbasierte Zuweisung zur Anwendung verfügen. Andernfalls wird die Anfrage abgelehnt. Wenn die AWS verwaltete Anwendung so konfiguriert ist, dass keine Benutzer- und Gruppenzuweisungen erforderlich sind, wird die Verarbeitung fortgesetzt.

> **Note**
>
> AWS Dienste verfügen über eine Standardeinstellungskonfiguration, die bestimmt, ob Zuweisungen für Benutzer und Gruppen erforderlich sind. Es wird empfohlen, die Einstellung „Zuweisungen erforderlich“ für diese Anwendungen nicht zu ändern, wenn Sie sie zusammen mit der Weitergabe vertrauenswürdiger Identitäten verwenden möchten. Selbst wenn Sie detaillierte Berechtigungen konfiguriert haben, die Benutzern

den Zugriff auf bestimmte Anwendungsressourcen ermöglichen, kann das Ändern der Einstellung „Zuweisungen erforderlich“ zu unerwartetem Verhalten führen, einschließlich einer Unterbrechung des Benutzerzugriffs auf diese Ressourcen.

- Überprüft, ob die anfordernde Anwendung so konfiguriert ist, dass sie gültige Bereiche für die empfangende verwaltete Anwendung verwendet. AWS

6. Wenn die vorherigen Überprüfungsschritte erfolgreich waren, erstellt IAM Identity Center ein neues Token. Das neue Token ist ein undurchsichtiges (verschlüsseltes) Token, das die Identität des entsprechenden Benutzers in IAM Identity Center, die Zielgruppe (Aud) der empfangenden AWS verwalteten Anwendung und die Bereiche enthält, die die anfordernde Anwendung verwenden kann, wenn sie Anfragen an die empfangende verwaltete Anwendung stellt. AWS
7. Die anfordernde Anwendung oder der von ihr verwendete Treiber initiiert eine Ressourcenanforderung an die empfangende Anwendung und leitet das von IAM Identity Center generierte Token an die empfangende Anwendung weiter.
8. Die empfangende Anwendung ruft das IAM Identity Center auf, um die Identität des Benutzers und die Bereiche zu ermitteln, die im Token kodiert sind. Es kann auch Anfragen zum Abrufen von Benutzerattributen oder Gruppenmitgliedschaften des Benutzers aus dem Identity Center-Verzeichnis stellen.
9. Die empfangende Anwendung verwendet ihre Autorisierungskonfiguration, um festzustellen, ob der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen.
10. Wenn der Benutzer berechtigt ist, auf die angeforderte Anwendungsressource zuzugreifen, beantwortet die empfangende Anwendung die Anfrage.
11. Die Identität des Benutzers, die in seinem Namen ausgeführten Aktionen und andere Ereignisse, die in den Protokollen und CloudTrail Ereignissen der empfangenden Anwendung aufgezeichnet wurden. Die spezifische Art und Weise, wie diese Informationen protokolliert werden, ist je nach Anwendung unterschiedlich.

IAM Identity Center-Zertifikate verwalten

IAM Identity Center verwendet Zertifikate, um eine SAML-Vertrauensstellung zwischen IAM Identity Center und dem Dienstanbieter Ihrer Anwendung einzurichten. Wenn Sie eine Anwendung in IAM Identity Center hinzufügen, wird während des Einrichtungsvorgangs automatisch ein IAM Identity Center-Zertifikat für die Verwendung mit dieser Anwendung erstellt. Dieses automatisch generierte IAM Identity Center-Zertifikat ist standardmäßig für einen Zeitraum von fünf Jahren gültig.

Als IAM Identity Center-Administrator müssen Sie gelegentlich ältere Zertifikate für eine bestimmte Anwendung durch neuere ersetzen. Beispielsweise müssen Sie möglicherweise ein Zertifikat ersetzen, wenn sich das Ablaufdatum des Zertifikats nähert. Der Vorgang, bei dem ein älteres Zertifikat durch ein neueres ersetzt wird, wird als Zertifikatsrotation bezeichnet.

Themen

Überlegungen vor der Rotation eines Zertifikats

Bevor Sie mit der Rotation eines Zertifikats in IAM Identity Center beginnen, sollten Sie Folgendes beachten:

- Der Zertifizierungsrotationsprozess erfordert, dass Sie das Vertrauen zwischen IAM Identity Center und dem Service Provider wiederherstellen. Verwenden Sie die unter beschriebenen Verfahren, um das Vertrauen wiederherzustellen. Wechseln Sie ein IAM Identity Center-Zertifikat
- Die Aktualisierung des Zertifikats mit dem Dienstanbieter kann zu einer vorübergehenden Dienstunterbrechung für Ihre Benutzer führen, bis das Vertrauen erfolgreich wiederhergestellt wurde. Planen Sie diesen Vorgang möglichst außerhalb der Spitzenzeiten sorgfältig.

Wechseln Sie ein IAM Identity Center-Zertifikat

Die Rotation eines IAM Identity Center-Zertifikats ist ein mehrstufiger Prozess, der Folgendes umfasst:

- Generieren eines neuen Zertifikats
- Hinzufügen des neuen Zertifikats zur Website des Dienstanbieters
- Das neue Zertifikat auf aktiv setzen
- Das inaktive Zertifikat wird gelöscht

Wenden Sie alle folgenden Verfahren in der folgenden Reihenfolge an, um den Zertifikatsrotationsprozess für eine bestimmte Anwendung abzuschließen.

Schritt 1: Generieren Sie ein neues Zertifikat.

Neue IAM Identity Center-Zertifikate, die Sie generieren, können so konfiguriert werden, dass sie die folgenden Eigenschaften verwenden:

- Gültigkeitszeitraum — Gibt die Zeit (in Monaten) an, bis ein neues IAM Identity Center-Zertifikat abläuft.
- Schlüsselgröße — Bestimmt die Anzahl der Bits, die ein Schlüssel mit seinem kryptografischen Algorithmus verwenden muss. Sie können diesen Wert entweder auf 1024-Bit-RSA oder 2048-Bit-RSA festlegen. Allgemeine Informationen zur Funktionsweise von Schlüsselgrößen in der Kryptografie finden Sie unter Schlüsselgröße.
- Algorithmus — Gibt den Algorithmus an, den IAM Identity Center beim Signieren der SAML-Assertion/-Antwort verwendet. Sie können diesen Wert entweder auf SHA-1 oder SHA-256 setzen. AWS empfiehlt, wenn möglich SHA-256 zu verwenden, es sei denn, Ihr Dienstanbieter verlangt SHA-1. Allgemeine Informationen zur Funktionsweise von Kryptografiealgorithmen finden Sie unter Kryptografie mit öffentlichen Schlüsseln.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen die Anwendung aus, für die Sie ein neues Zertifikat generieren möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Registerkarte Konfiguration aus. Wählen Sie unter IAM Identity Center-Metadaten die Option Zertifikat verwalten aus. Wenn Sie keine Registerkarte „Konfiguration“ haben oder die Konfigurationseinstellung nicht verfügbar ist, müssen Sie das Zertifikat für diese Anwendung nicht rotieren.
5. Wählen Sie auf der IAM Identity Center-Zertifikatsseite die Option Neues Zertifikat generieren aus.
6. Geben Sie im Dialogfeld Neues IAM Identity Center-Zertifikat generieren die entsprechenden Werte für Gültigkeitsdauer, Algorithmus und Schlüsselgröße an. Wählen Sie dann Generieren.

Schritt 2: Aktualisieren Sie die Website des Dienstanbieters.

Gehen Sie wie folgt vor, um die Vertrauensstellung mit dem Dienstanbieter der Anwendung wiederherzustellen.

> **Important**
>
> Wenn Sie das neue Zertifikat auf den Dienstanbieter hochladen, können sich Ihre Benutzer möglicherweise nicht authentifizieren. Um diese Situation zu korrigieren, legen Sie das neue Zertifikat wie im nächsten Schritt beschrieben als aktiv fest.

1. Wählen Sie in der IAM Identity Center-Konsole die Anwendung aus, für die Sie gerade ein neues Zertifikat generiert haben.
2. Wählen Sie auf der Seite mit den Anwendungsdetails die Option Konfiguration bearbeiten aus.
3. Wählen Sie Anweisungen anzeigen aus und folgen Sie dann den Anweisungen auf der Website Ihres jeweiligen Anwendungsdienstanbieters, um das neu generierte Zertifikat hinzuzufügen.

Schritt 3: Setzen Sie das neue Zertifikat auf aktiv.

Einer Anwendung können bis zu zwei Zertifikate zugewiesen werden. IAM Identity Center verwendet die als aktiv eingestellte Zertifizierung, um alle SAML-Assertionen zu signieren.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen Ihre Anwendung aus.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Registerkarte Konfiguration aus. Wählen Sie unter IAM Identity Center-Metadaten die Option Zertifikat verwalten aus.
5. Wählen Sie auf der IAM Identity Center-Zertifikatsseite das Zertifikat aus, das Sie als aktiv festlegen möchten, wählen Sie Aktionen und dann Als aktiv festlegen aus.
6. Vergewissern Sie sich im Dialogfeld Das ausgewählte Zertifikat als aktiv festlegen, dass Sie beim Aktivieren eines Zertifikats möglicherweise die Vertrauensstellung erneut herstellen müssen, und wählen Sie dann Make active aus.

Schritt 4: Löschen Sie das alte Zertifikat.

Gehen Sie wie folgt vor, um den Zertifikatsrotationsprozess für Ihre Bewerbung abzuschließen. Sie können nur ein Zertifikat löschen, das sich im Status Inaktiv befindet.

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).

3. Wählen Sie in der Liste der Anwendungen Ihre Anwendung aus.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Registerkarte Konfiguration aus. Wählen Sie unter IAM Identity Center-Metadaten die Option Zertifikat verwalten aus.
5. Wählen Sie auf der IAM Identity Center-Zertifikatsseite das Zertifikat aus, das Sie löschen möchten. Wählen Sie Actions und dann Delete aus.
6. Wählen Sie im Dialogfeld „Zertifikat löschen“ die Option Löschen aus.

Indikatoren für den Ablaufstatus des Zertifikats

Wenn Sie sich in den Eigenschaften einer Anwendung auf der Seite „Anwendungen“ befinden, sehen Sie möglicherweise farbige Statusanzeigesymbole. Diese Symbole werden in der Spalte Läuft ab neben jedem Zertifikat in der Liste angezeigt. Im Folgenden werden die Kriterien beschrieben, anhand derer IAM Identity Center bestimmt, welches Symbol für jedes Zertifikat angezeigt wird.

- Rot — Zeigt an, dass ein Zertifikat derzeit abgelaufen ist.
- Gelb — Zeigt an, dass ein Zertifikat in 90 Tagen oder weniger abläuft.
- Grün — Zeigt an, dass ein Zertifikat derzeit gültig ist und noch mindestens 90 Tage gültig bleibt.

Um den aktuellen Status eines Zertifikats zu überprüfen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Überprüfen Sie in der Liste der Anwendungen den Status der Zertifikate in der Liste, wie in der Spalte Läuft ab am angegeben.

Konfigurieren Sie die Anwendungseigenschaften in der IAM Identity Center-Konsole

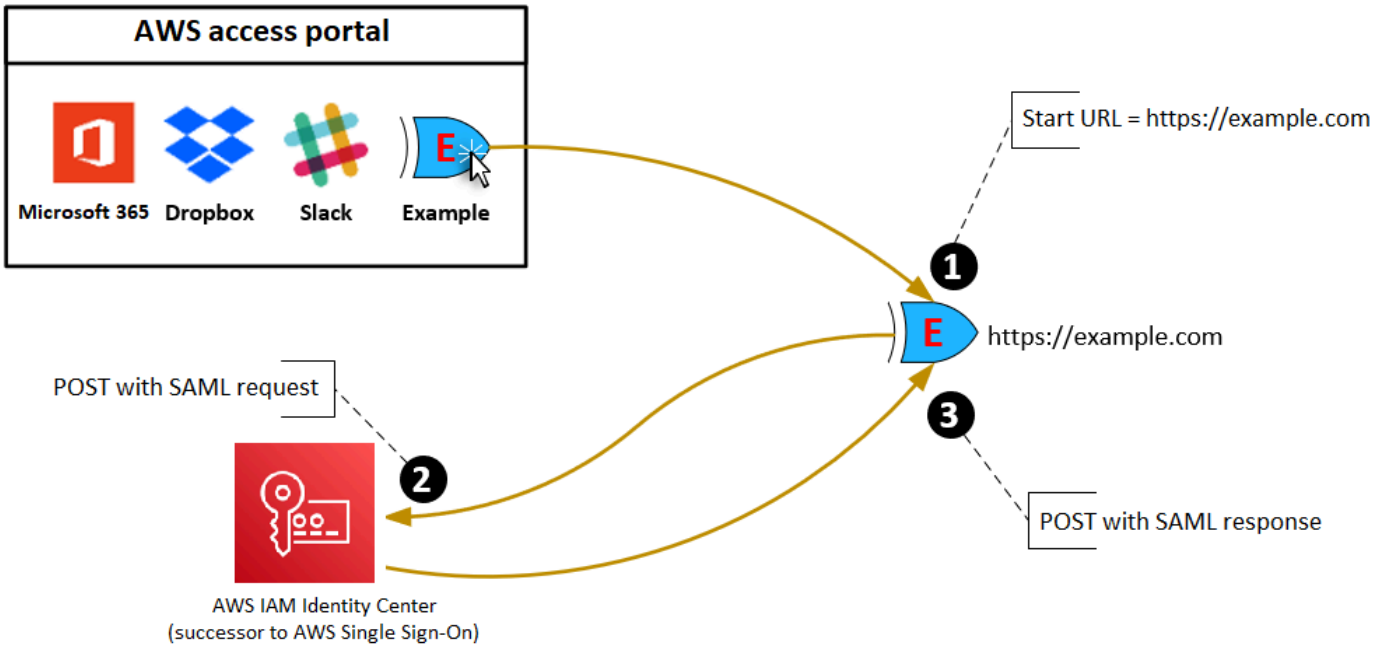
In IAM Identity Center können Sie die Benutzererfahrung anpassen, indem Sie die Start-URL der Anwendung, den Relay-Status und die Sitzungsdauer konfigurieren.

Start-URL der Anwendung

Sie verwenden eine Anwendungs-Start-URL, um den Verbundprozess mit Ihrer Anwendung zu starten. In der Regel wird sie für Anwendungen verwendet, die nur vom Service Provider (SP) initiierte Bindungen unterstützen.

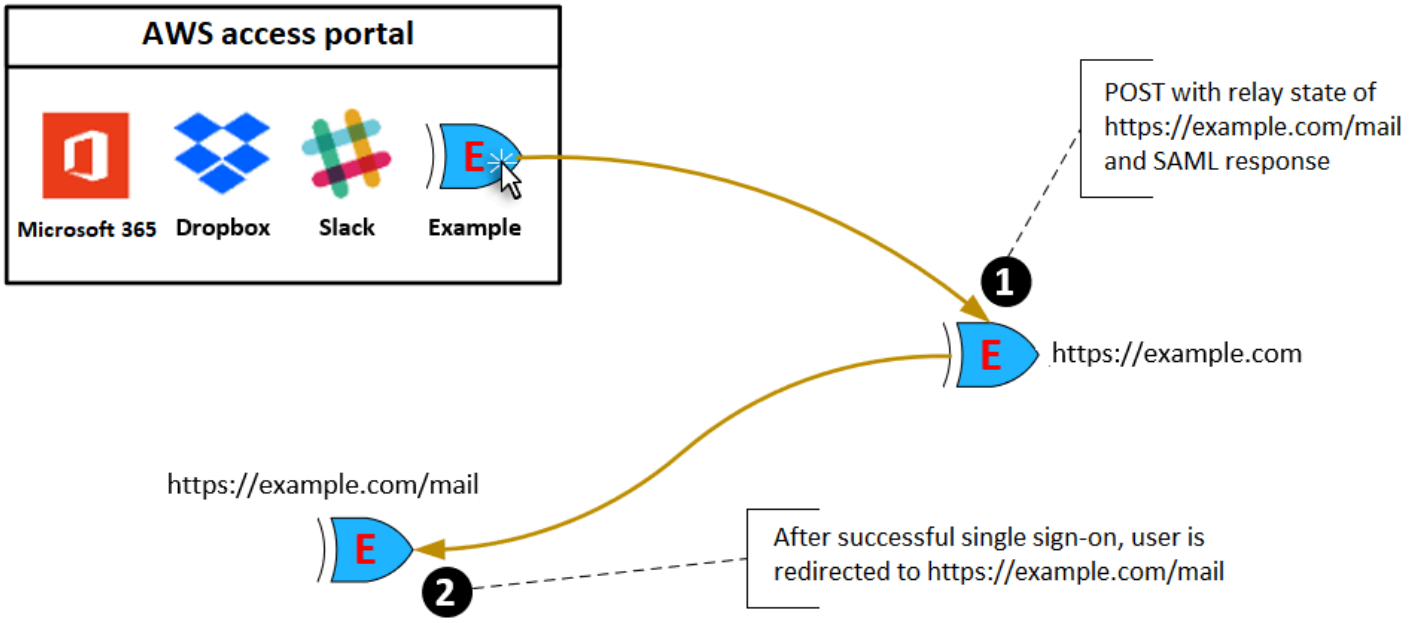
Die folgenden Schritte und das Diagramm veranschaulichen den Ablauf der URL-Authentifizierung beim Starten einer Anwendung, wenn ein Benutzer im AWS Access Portal eine Anwendung auswählt:

1. Der Browser des Benutzers leitet die Authentifizierungsanforderung anhand des Wertes für die Anwendungs-Start-URL (in diesem Fall https://example.com) um.
2. Die Anwendung sendet eine `HTML POST` mit a `SAMLRequest` an das IAM Identity Center.
3. IAM Identity Center sendet dann eine `HTML POST` mit einer `SAMLResponse` Rückseite an die Anwendung.



Relay-Status

Während des Verbund-Authentifizierungsprozesses leitet der Relais-Status Benutzer innerhalb der Anwendung um. Für SAML 2.0 wird dieser Wert unverändert an die Anwendung übergeben. Nachdem die Anwendungseigenschaften konfiguriert wurden, sendet IAM Identity Center den Relay-Status-Wert zusammen mit einer SAML-Antwort an die Anwendung.



Sitzungsdauer

Die Sitzungsdauer ist der Zeitraum, für den eine Anwendungsbenutzersitzung gültig ist. Für SAML 2.0 wird dies verwendet, um das `SessionNotOnOrAfter` Datum des Elements der SAML-Assertion festzulegen. `saml2:AuthNStatement`

Die Sitzungsdauer kann von Anwendungen auf eine der folgenden Arten interpretiert werden:

- Anwendungen können damit die maximale Zeit bestimmen, die für die Sitzung des Benutzers zulässig ist. Anwendungen können eine Benutzersitzung mit einer kürzeren Dauer generieren. Dies kann der Fall sein, wenn die Anwendung nur Benutzersitzungen mit einer Dauer unterstützt, die kürzer ist als die konfigurierte Länge der Sitzung ist.
- Anwendungen können sie als exakte Dauer ansehen und Administratoren möglicherweise nicht erlauben, den Wert zu konfigurieren. Dies kann der Fall sein, wenn die Anwendung nur eine bestimmte Sitzungsdauer unterstützt.

Weitere Informationen darüber, wie die Sitzungsdauer verwendet wird, finden Sie in der Dokumentation der betreffenden Anwendung.

Weisen Sie Benutzerzugriff auf Anwendungen in der IAM Identity Center-Konsole zu

Sie können Benutzern Single Sign-On-Zugriff auf SAML 2.0-Anwendungen im Anwendungskatalog oder auf benutzerdefinierte SAML 2.0-Anwendungen zuweisen.

Überlegungen zu Gruppenzuweisungen:

- Weisen Sie Gruppen den Zugriff direkt zu. Um die Verwaltung der Zugriffsberechtigungen zu vereinfachen, empfehlen wir, den Zugriff direkt Gruppen und nicht einzelnen Benutzern zuzuweisen. Mit Gruppen können Sie Benutzergruppen Berechtigungen gewähren oder verweigern, anstatt diese Berechtigungen jedem einzelnen Benutzer zuzuweisen. Wenn ein Benutzer in eine andere Organisation wechselt, verschieben Sie diesen Benutzer einfach in eine andere Gruppe. Der Benutzer erhält dann automatisch die Berechtigungen, die für die neue Organisation erforderlich sind.
- Verschachtelte Gruppen werden nicht unterstützt. Beim Zuweisen von Benutzerzugriff auf Anwendungen unterstützt IAM Identity Center nicht, dass Benutzer zu verschachtelten Gruppen hinzugefügt werden. Wenn ein Benutzer zu einer verschachtelten Gruppe hinzugefügt wird, erhält er bei der Anmeldung möglicherweise die Meldung „Sie haben keine Anwendungen“. Zuweisungen müssen für die unmittelbare Gruppe vorgenommen werden, deren Mitglied der Benutzer ist.

Um Benutzer- oder Gruppenzugriff auf Anwendungen zuzuweisen

> **Important**
>
> Bei AWS verwalteten Anwendungen müssen Sie Benutzer direkt aus den entsprechenden Anwendungskonsolen oder über die APIs hinzufügen.

1. Öffnen Sie die IAM Identity Center-Konsole.

   > **Note**
   >
   > Wenn Sie Benutzer in verwalten AWS Managed Microsoft AD, stellen Sie sicher, dass die IAM Identity Center-Konsole die AWS Region verwendet, in der sich Ihr AWS Managed Microsoft AD Verzeichnis befindet, bevor Sie den nächsten Schritt ausführen.

2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen den Namen der Anwendung aus, der Sie Zugriff zuweisen möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails im Abschnitt Zugewiesene Benutzer die Option Benutzer zuweisen aus.
5. Geben Sie im Dialogfeld „Benutzer zuweisen“ einen Benutzer- oder Gruppennamen ein. Sie können auch nach Benutzern und Gruppen suchen. Sie können mehrere Benutzer oder Gruppen angeben, indem Sie die entsprechenden Konten in den Suchergebnissen markieren.
6. Wählen Sie Assign users (Benutzer zuweisen) aus.

Entfernen Sie den Benutzerzugriff in der IAM Identity Center-Konsole

Gehen Sie wie folgt vor, um den Benutzerzugriff auf SAML 2.0-Anwendungen im Anwendungskatalog oder auf benutzerdefinierte SAML 2.0-Anwendungen zu entfernen.

So entfernen Sie den Benutzerzugriff auf eine Anwendung

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen die Anwendung aus, für die Sie den Benutzerzugriff entfernen möchten.
4. Wählen Sie auf der Seite mit den Anwendungsdetails im Abschnitt Zugewiesene Benutzer den Benutzer oder die Gruppe aus, den Sie entfernen möchten, und klicken Sie dann auf die Schaltfläche Zugriff entfernen.
5. Überprüfen Sie im Dialogfeld Remove access (Zugriff entfernen) den Benutzer- oder Gruppennamen. Klicken Sie abschließend auf Remove access (Zugriff entfernen).

Ordnen Sie Attribute in Ihrer Anwendung den IAM Identity Center-Attributen zu

Einige Service-Anbieter erfordern benutzerdefinierte SAML-Zusicherungen, um zusätzliche Daten zu Ihren Benutzeranmeldungen zu übergeben. Verwenden Sie in diesem Fall das folgende Verfahren,

um anzugeben, wie die Benutzerattribute Ihrer Anwendung den entsprechenden Attributen in IAM Identity Center zugeordnet werden sollen.

So ordnen Sie Anwendungsattribute Attributen in IAM Identity Center zu

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Applications (Anwendungen).
3. Wählen Sie in der Liste der Anwendungen diejenige aus, für die Attribute zugeordnet werden sollen.
4. Wählen Sie auf der Seite mit den Anwendungsdetails die Option Aktionen und dann Attributzuordnung bearbeiten aus.
5. Wählen Sie Neue Attributzuordnung hinzufügen aus.
6. Geben Sie im ersten Textfeld das Anwendungsattribut ein.
7. Geben Sie im zweiten Textfeld das Attribut in IAM Identity Center ein, das Sie dem Anwendungsattribut zuordnen möchten. Möglicherweise möchten Sie das Anwendungsattribut dem IAM Identity Center-Benutzerattribut zuordnen**`Username`**. **`email`** Eine Liste der zulässigen Benutzerattribute in IAM Identity Center finden Sie in der Tabelle unter. Attributzuordnungen für AWS Managed Microsoft AD das Verzeichnis
8. Wählen Sie in der dritten Spalte der Tabelle das entsprechende Format für das Attribut aus dem Menü aus.
9. Wählen Sie Save Changes.

Resilienzdesign und regionales Verhalten

Der IAM-Identity-Center-Service wird vollständig verwaltet und verwendet hochverfügbare und dauerhafte AWS Services wie Amazon S3 und Amazon EC2. Um die Verfügbarkeit im Falle einer Unterbrechung der Availability Zone sicherzustellen, arbeitet IAM Identity Center über mehrere Availability Zones hinweg. Informationen zu den Zielen des Verfügbarkeitsdesigns für IAM Identity Center finden Sie in Anhang A: Entwurf für Verfügbarkeit für ausgewählte AWS Services im Säulenhandbuch zur Zuverlässigkeit.

Sie aktivieren IAM Identity Center in Ihrem AWS Organizations Verwaltungskonto. Dies ist erforderlich, damit IAM Identity Center Rollen in allen Ihren bereitstellen, bereitstellen und aktualisieren kannAWS-Konten. Wenn Sie IAM Identity Center aktivieren, wird es in der bereitgestelltAWS-Region, die derzeit ausgewählt ist. Wenn Sie für eine bestimmte bereitstellen möchtenAWS-Region, ändern Sie die Regionsauswahl, bevor Sie IAM Identity Center aktivieren.

> **Note**
>
> IAM Identity Center steuert den Zugriff auf seine Berechtigungssätze und Anwendungen nur aus seiner primären Region. Wir empfehlen Ihnen, die mit der Zugriffskontrolle verbundenen Risiken zu berücksichtigen, wenn IAM Identity Center in einer einzigen Region arbeitet.

Obwohl IAM Identity Center den Zugriff aus der Region bestimmt, in der Sie den Service aktivieren, AWS-Konten sind global. Das bedeutet, dass Benutzer nach der Anmeldung bei IAM Identity Center in jeder Region arbeiten können, wenn sie AWS-Konten über IAM Identity Center auf zugreifen. Die meisten AWS SageMakerverwalteten Anwendungen wie Amazon müssen jedoch in derselben - Region wie IAM Identity Center installiert sein, damit Benutzer den Zugriff auf diese Anwendungen authentifizieren und zuweisen können. Informationen zu regionalen Einschränkungen bei der Verwendung einer Anwendung mit IAM Identity Center finden Sie in der Dokumentation für die Anwendung.

Sie können IAM Identity Center auch verwenden, um den Zugriff auf SAML-basierte Anwendungen zu authentifizieren und zu autorisieren, die über eine öffentliche URL erreichbar sind, unabhängig von der Plattform oder Cloud, auf der die Anwendung erstellt wird.

Wir empfehlen nicht, Kontoinstanzen von IAM Identity Center als Möglichkeit zu verwenden, um Ausfallsicherheit zu implementieren, da ein zweiter isolierter Kontrollpunkt erstellt wird, der nicht mit Ihrer Organisations-Instance verbunden ist.

Einrichten des Notfallzugriffs auf die AWS Management Console

IAM Identity Center basiert auf einer hochverfügbaren AWS Infrastruktur und verwendet eine Availability Zone-Architektur, um einzelne Fehlerpunkte zu vermeiden. Für eine zusätzliche Schutzebene im unwahrscheinlichen Fall einer AWS-Region Unterbrechung oder eines IAM Identity Center empfehlen wir Ihnen, eine Konfiguration einzurichten, mit der Sie temporären Zugriff auf die gewähren könnenAWS Management Console.

Inhalt

Übersicht

AWS ermöglicht Ihnen Folgendes:

- Verbinden Sie Ihren Drittanbieter-IdP mit IAM Identity Center .
- Verbinden Sie Ihren Drittanbieter-IdP mithilfe AWS-Konten des SAML-2.0-basierten Verbunds mit einzelnen .

Wenn Sie IAM Identity Center verwenden, können Sie diese Funktionen verwenden, um die in den folgenden Abschnitten beschriebene Notfallzugriffskonfiguration zu erstellen. Mit dieser Konfiguration können Sie IAM Identity Center als AWS-Konto Zugriffsmechanismus verwenden. Wenn IAM Identity Center unterbrochen wird, können sich Ihre Notfallbenutzer AWS Management Console über einen direkten Verbund bei der anmelden, indem sie dieselben Anmeldeinformationen verwenden, die sie

für den Zugriff auf ihre Konten verwenden. Diese Konfiguration funktioniert, wenn IAM Identity Center nicht verfügbar ist, aber die IAM-Datenebene und Ihr externer Identitätsanbieter (IdP) verfügbar sind.

> **Important**
>
> Wir empfehlen Ihnen, diese Konfiguration bereitzustellen, bevor eine Unterbrechung auftritt, da Sie die Konfiguration nicht erstellen können, wenn Ihr Zugriff zum Erstellen der erforderlichen IAM-Rollen ebenfalls unterbrochen wird. Testen Sie diese Konfiguration außerdem regelmäßig, um sicherzustellen, dass Ihr Team weiß, was zu tun ist, wenn IAM Identity Center unterbrochen wird.

Zusammenfassung der Notfallzugriffskonfiguration

Um den Notfallzugriff zu konfigurieren, müssen Sie die folgenden Aufgaben ausführen:

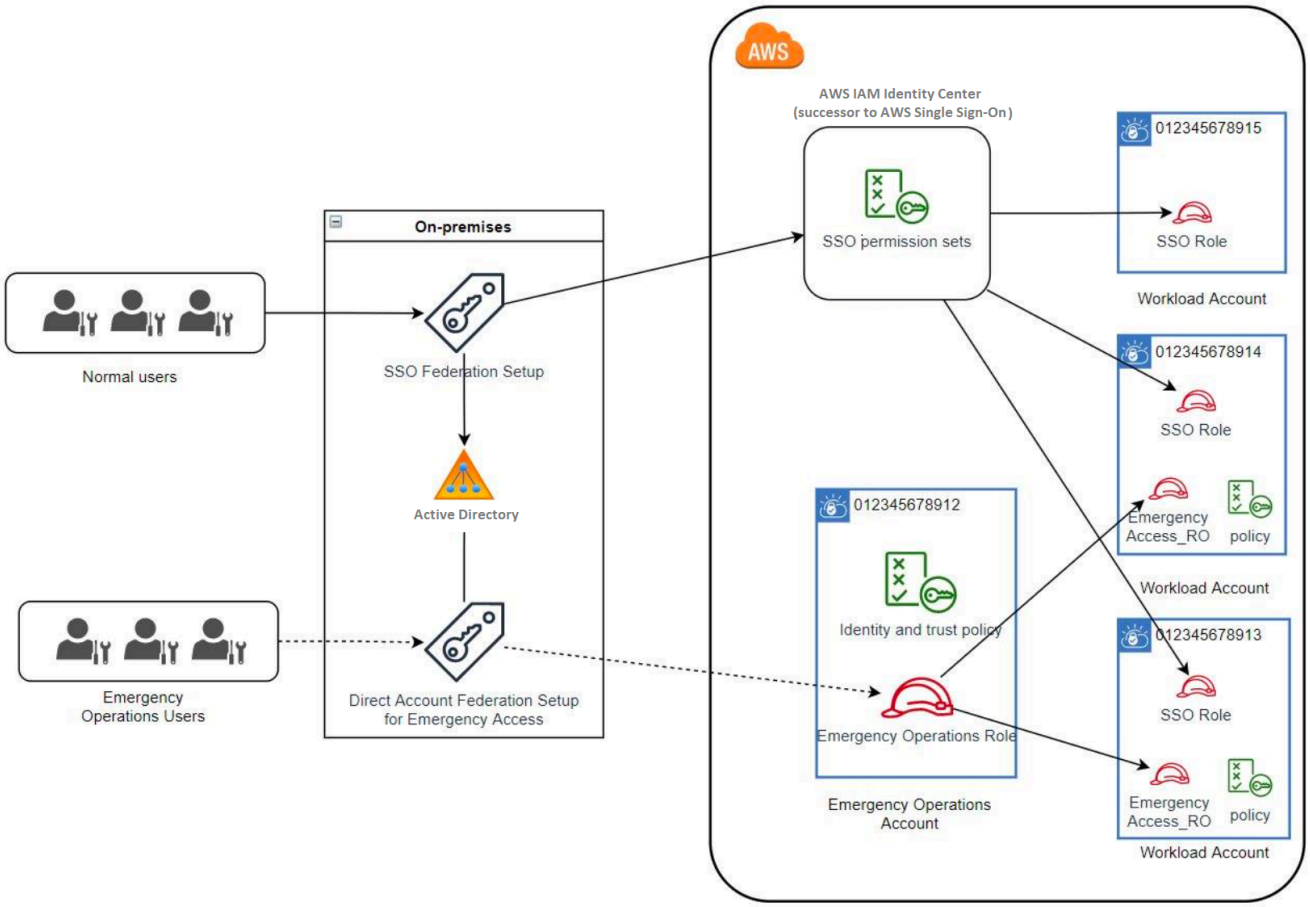
1. Erstellen Sie ein Notfallbetriebskonto in Ihrer Organisation in AWS Organizations.
2. Verbinden Sie Ihren IdP mit dem Notfallbetriebskonto mithilfe des SAML-2.0-basierten Verbunds .
3. Erstellen Sie im Konto für Notfalloperationen eine Rolle für den externen Identitätsanbieterverbund . Erstellen Sie außerdem in jedem Ihrer Workload-Konten eine Notfalloperationenrolle mit Ihren erforderlichen Berechtigungen.
4. Delegieren Sie den Zugriff auf Ihre Workload-Konten für die IAM-Rolle, die Sie im Konto für Notfalloperationen erstellt haben. Um den Zugriff auf Ihr Notfallbetriebskonto zu autorisieren, erstellen Sie eine Notfallbetriebsgruppe in Ihrem IdP ohne Mitglieder.
5. Aktivieren Sie die Notfalloperationengruppe in Ihrem IdP, um die Notfalloperationsrolle zu verwenden, indem Sie eine Regel in Ihrem IdP erstellen, die den SAML-2.0-Verbundzugriff auf die ermöglichtAWS Management Console.

Während des normalen Betriebs hat niemand Zugriff auf das Notfallbetriebskonto, da die Notfallbetriebsgruppe in Ihrem IdP keine Mitglieder hat. Im Falle einer Unterbrechung des IAM Identity Center verwenden Sie Ihren IdP, um der Notfalloperationsgruppe in Ihrem IdP vertrauenswürdige Benutzer hinzuzufügen. Diese Benutzer können sich dann bei Ihrem IdP anmelden, zur navigieren und die AWS Management ConsoleNotfalloperationenrolle im Notfalloperationenkonto übernehmen. Von dort aus können diese Benutzer Rollen zur Notfallzugriffsrolle in Ihren Workload-Konten wechseln, wo sie Vorgänge ausführen müssen.

So entwerfen Sie Ihre kritischen Betriebsrollen

Mit diesem Design konfigurieren Sie einen einzelnen , AWS-Konto in dem Sie sich über IAM verbinden, sodass Benutzer kritische Betriebsrollen übernehmen können. Die Rollen für kritische Vorgänge verfügen über eine Vertrauensrichtlinie, die es Benutzern ermöglicht, eine entsprechende Rolle in Ihren Workload-Konten zu übernehmen. Die Rollen in den Workload-Konten bieten die Berechtigungen, die Benutzer für die Ausführung wesentlicher Aufgaben benötigen.

Das folgende Diagramm bietet einen Überblick über das Design.



So planen Sie Ihr Zugriffsmodell

Bevor Sie den Notfallzugriff konfigurieren, erstellen Sie einen Plan für die Funktionsweise des Zugriffsmodells. Gehen Sie wie folgt vor, um diesen Plan zu erstellen.

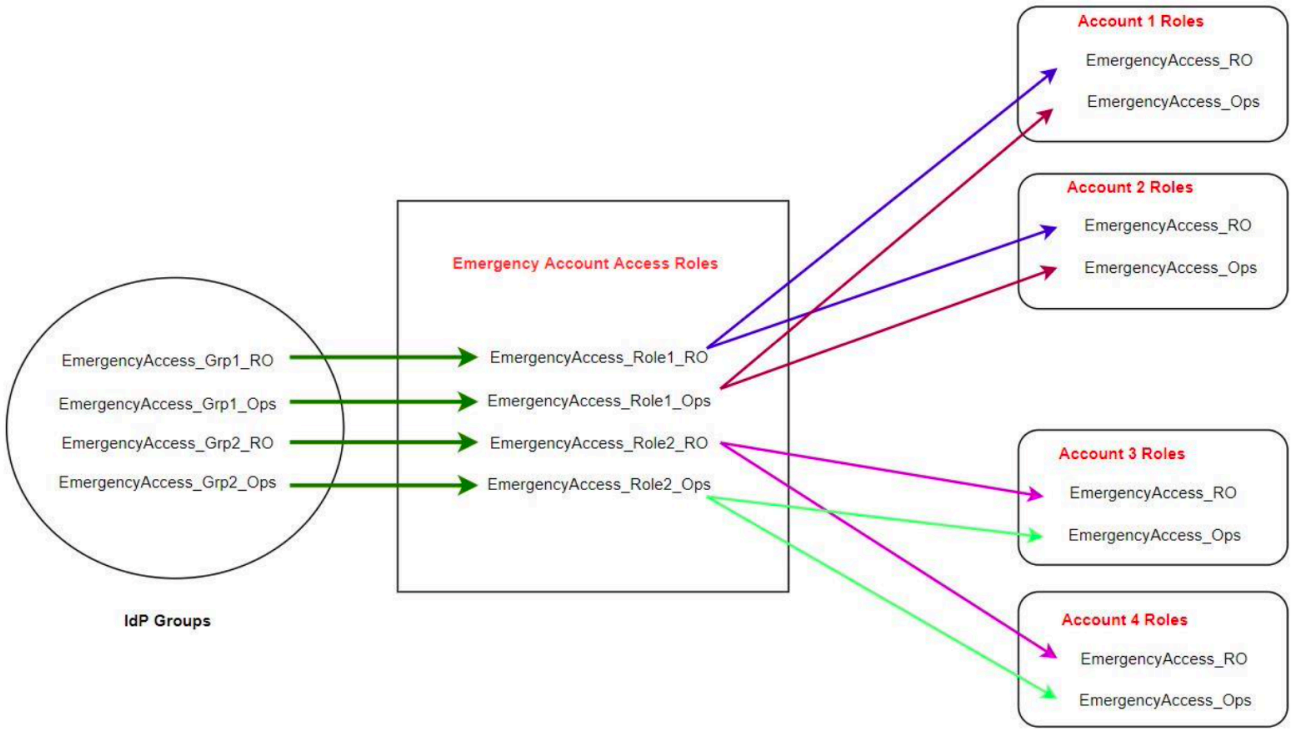
1. Identifizieren Sie die AWS-Konten, in der der Zugriff auf Notfalloperatoren während einer Unterbrechung des IAM Identity Center unerlässlich ist. Ihre Produktionskonten sind

beispielsweise wahrscheinlich von entscheidender Bedeutung, Ihre Entwicklungs- und Testkonten sind es jedoch möglicherweise nicht.

2. Identifizieren Sie für diese Sammlung von Konten die spezifischen kritischen Rollen, die Sie in Ihren Konten benötigen. Über diese Konten hinweg sollten Sie konsistent definieren, was die Rollen tun können. Dies vereinfacht die Arbeit in Ihrem Notfallzugriffskonto, in dem Sie kontoübergreifende Rollen erstellen. Wir empfehlen Ihnen, mit zwei unterschiedlichen Rollen in diesen Konten zu beginnen: Nur Lesen (RO) und Operationen (Ops). Bei Bedarf können Sie weitere Rollen erstellen und diese Rollen einer eindeutigeren Gruppe von Notfallzugriffsbenutzern in Ihrem Setup zuordnen.
3. Identifizieren und erstellen Sie Notfallzugriffsgruppen in Ihrem IdP Die Gruppenmitglieder sind die Benutzer, an die Sie den Zugriff auf Notfallzugriffsrollen delegieren.
4. Definieren Sie, welche Rollen diese Gruppen im Notfallzugriffskonto übernehmen können. Definieren Sie dazu Regeln in Ihrem IdP, die Ansprüche generieren, die auflisten, auf welche Rollen die Gruppe zugreifen kann. Diese Gruppen können dann Ihre schreibgeschützten oder Betriebsrollen im Notfallzugriffskonto übernehmen. Von diesen Rollen können sie entsprechende Rollen in Ihren Workload-Konten übernehmen.

So entwerfen Sie Notfallrollen-, Konto- und Gruppenzuordnungen

Das folgende Diagramm zeigt, wie Sie Ihre Notfallzugriffsgruppen Rollen in Ihrem Notfallzugriffskonto zuordnen. Das Diagramm zeigt auch die kontoübergreifenden Rollenvertrauensstellungen, die es Notfallzugriffskontorollen ermöglichen, auf entsprechende Rollen in Ihren Workload-Konten zuzugreifen. Wir empfehlen, dass Ihr Notfallplandesign diese Zuordnungen als Ausgangspunkt verwendet.



So erstellen Sie Ihre Notfallzugriffskonfiguration

Verwenden Sie die folgende Zuordnungstabelle, um Ihre Notfallzugriffskonfiguration zu erstellen. Diese Tabelle spiegelt einen Plan wider, der zwei Rollen in den Workload-Konten enthält: Nur Lesen (RO) und Operationen (Ops) mit entsprechenden Vertrauensrichtlinien und Berechtigungsrichtlinien. Die Vertrauensrichtlinien ermöglichen es den Notfallzugriffskontorollen, auf die einzelnen Workload-Kontorollen zuzugreifen. Die einzelnen Workload-Kontorollen verfügen auch über Berechtigungsrichtlinien für die Aktionen der Rolle im Konto. Die Berechtigungsrichtlinien können AWS verwaltete Richtlinien oder vom Kunden verwaltete Richtlinien sein.

Account	Zu erstellende Rollen	Vertrauensrichtlinie	Berechtigungsrichtlinie
Konto 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Konto 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator

Account	Zu erstellende Rollen	Vertrauensrichtlinie	Berechtigungsrichtlinie
Konto 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Konto 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Konto für Notfallzugriff	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole für Rollenressource im Konto

In diesem Zuordnungsplan enthält das Notfallzugriffskonto zwei schreibgeschützte Rollen und zwei Betriebsrollen. Diese Rollen vertrauen Ihrem IdP, um Ihre ausgewählten Gruppen zu authentifizieren und zu autorisieren, auf die Rollen zuzugreifen, indem sie die Namen der Rollen in Assertionen übergeben. In Workload-Konto 1 und Konto 2 gibt es entsprechende schreibgeschützte - und -Operationsrollen. Für Workload-Konto 1 vertraut die `EmergencyAccess_RO` Rolle der `EmergencyAccess_Role1_RO` Rolle, die sich im Notfallzugriffskonto befindet. Die Tabelle gibt ähnliche Vertrauensmuster zwischen den schreibgeschützten Workload-Konto- und Betriebsrollen und den entsprechenden Notfallzugriffsrollen an.

Notfallvorbereitungsaufgaben

Um Ihre Notfallzugriffskonfiguration vorzubereiten, empfehlen wir Ihnen, die folgenden Aufgaben auszuführen, bevor ein Notfall eintritt.

1. Richten Sie eine direkte IAM-Verbundanwendung in Ihrem IdP ein. Weitere Informationen finden Sie unter Einmalige Einrichtung einer direkten IAM-Verbundanwendung in Okta.

2. Erstellen Sie eine IdP-Verbindung im Notfallzugriffskonto, auf die während des Ereignisses zugegriffen werden kann.
3. Erstellen Sie Notfallzugriffsrollen in den Notfallzugriffskonten, wie in der obigen Zuordnungstabelle beschrieben.
4. Erstellen Sie temporäre Betriebsrollen mit Vertrauens- und Berechtigungsrichtlinien in jedem der Workload-Konten.
5. Erstellen Sie temporäre Betriebsgruppen in Ihrem IdP . Die Gruppennamen hängen von den Namen der temporären Operationsrollen ab.
6. Testen Sie den direkten IAM-Verbund.
7. Deaktivieren Sie die IdP-Verbundanwendung in Ihrem IdP, um eine regelmäßige Nutzung zu verhindern.

Notfall-Failover-Prozess

Wenn eine IAM-Identity-Center-Instance nicht verfügbar ist und Sie feststellen, dass Sie Notfallzugriff auf die -AWSManagementkonsole gewähren müssen, empfehlen wir den folgenden Failover-Prozess.

1. Der IdP-Administrator aktiviert die direkte IAM-Verbundanwendung in Ihrem IdP .
2. Benutzer fordern den Zugriff auf die temporäre Betriebsgruppe über Ihren vorhandenen Mechanismus an, z. B. eine E-Mail-Anfrage, einen Slack-Kanal oder eine andere Form der Kommunikation.
3. Benutzer, die Sie Ihren Notfallzugriffsgruppen hinzufügen, melden sich beim IdP an, wählen das Notfallzugriffskonto aus und die Benutzer wählen eine Rolle aus, die im Notfallzugriffskonto verwendet werden soll. Von diesen Rollen können sie Rollen in entsprechenden Workload-Konten übernehmen, die kontoübergreifende Vertrauensstellung mit der Notfallkontorolle haben.

Kehren Sie zum normalen Betrieb zurück

Überprüfen Sie das AWS Zustands-Dashboard, um zu bestätigen, wann der Zustand des IAM-Identity-Center-Service wiederhergestellt wird. Führen Sie die folgenden Schritte aus, um zum normalen Betrieb zurückzukehren.

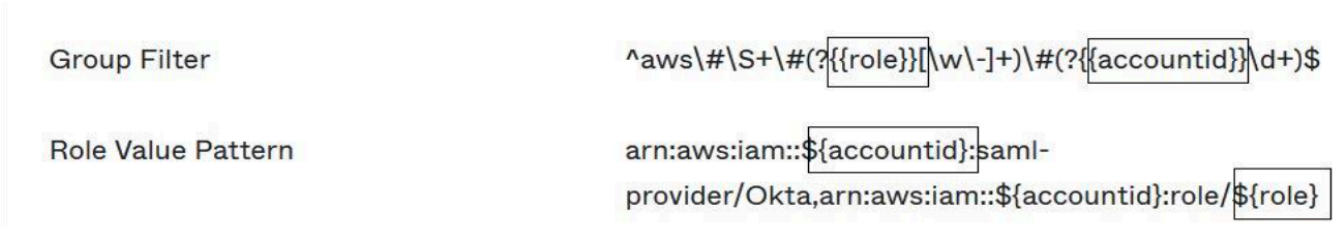
1. Nachdem das Statussymbol für den IAM-Identity-Center-Service anzeigt, dass der Service fehlerfrei ist, melden Sie sich beim IAM Identity Center an.

2. Wenn Sie sich erfolgreich bei IAM Identity Center anmelden können, teilen Sie den Notfallzugriffsbenutzern mit, dass IAM Identity Center verfügbar ist. Weisen Sie diese Benutzer an, sich abzumelden und das -AWSZugriffsportal zu verwenden, um sich wieder beim IAM Identity Center anzumelden.
3. Nachdem sich alle Notfallzugriffsbenutzer abgemeldet haben, deaktivieren Sie im IdP die IdP-Verbundanwendung. Wir empfehlen Ihnen, diese Aufgabe nach der Geschäftszeit auszuführen.
4. Entfernen Sie alle Benutzer aus der Notfallzugriffsgruppe im IdP .

Ihre Notfallzugriffsrolleninfrastruktur bleibt als Backup-Zugriffsplan bestehen, ist aber jetzt deaktiviert.

Einmalige Einrichtung einer direkten IAM-Verbundanwendung in Okta

1. Melden Sie sich als Benutzer mit Administratorberechtigungen bei Ihrem -OktaKonto an.
2. Wählen Sie in der Okta Admin-Konsole unter Anwendungen die Option Anwendungen aus.
3. Wählen Sie App Catalog durchsuchen aus. Suchen Sie nach und wählen Sie AWS Kontoverbund aus. Wählen Sie dann Integration hinzufügen aus.
4. Richten Sie den direkten IAM-Verbund mit ein, AWS indem Sie die Schritte unter So konfigurieren Sie SAML 2.0 für den AWS Kontoverbund befolgen.
5. Wählen Sie auf der Registerkarte Anmeldeoptionen SAML 2.0 aus und geben Sie Gruppenfilter- und Rollenwertmustereinstellungen ein. Der Name der Gruppe für das Benutzerverzeichnis hängt vom konfigurierten Filter ab.



   In der obigen Abbildung bezieht sich die `role` Variable auf die Rolle für den Notfallbetrieb in Ihrem Notfallzugriffskonto. Wenn Sie beispielsweise die `EmergencyAccess_Role1_R0` Rolle (wie in der Zuordnungstabelle beschrieben) in erstellen AWS-Konto `123456789012`und Ihre Gruppenfiltereinstellung wie in der Abbildung oben gezeigt konfiguriert ist, sollte Ihr Gruppenname lauten`aws#EmergencyAccess_Role1_R0#123456789012`.
6. Erstellen Sie in Ihrem Verzeichnis (z. B. Ihr Verzeichnis in Active Directory) die Notfallzugriffsgruppe und geben Sie einen Namen für das Verzeichnis an (z. B.

aws#EmergencyAccess_Role1_RO#123456789012). Weisen Sie Ihre Benutzer dieser Gruppe zu, indem Sie Ihren vorhandenen Bereitstellungsmechanismus verwenden.

7. Konfigurieren Sie im Notfallzugriffskonto eine benutzerdefinierte Vertrauensrichtlinie, die die Berechtigungen bereitstellt, die erforderlich sind, damit die Notfallzugriffsrolle während einer Unterbrechung übernommen werden kann. Im Folgenden finden Sie eine Beispielanweisung für eine benutzerdefinierte Vertrauensrichtlinie, die der EmergencyAccess_Role1_RO Rolle angefügt ist. Zur Veranschaulichung vgl. das Notfallkonto im Diagramm unter So entwerfen Sie Notfallrollen-, Konto- und Gruppenzuordnungen.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
      }
   ]
}
```

8. Im Folgenden finden Sie eine Beispielanweisung für eine Berechtigungsrichtlinie, die der EmergencyAccess_Role1_RO Rolle angefügt ist. Zur Veranschaulichung vgl. das Notfallkonto im Diagramm unter So entwerfen Sie Notfallrollen-, Konto- und Gruppenzuordnungen.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
```

```
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. Konfigurieren Sie für die Workload-Konten eine benutzerdefinierte Vertrauensrichtlinie. Im Folgenden finden Sie eine Beispielanweisung für eine Vertrauensrichtlinie, die der `EmergencyAccess_RO` Rolle angefügt ist. In diesem Beispiel `123456789012` ist das Konto das Notfallzugriffskonto. Zur Veranschaulichung siehe Workload-Konto im Diagramm unter So entwerfen Sie Notfallrollen-, Konto- und Gruppenzuordnungen.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> Die meisten IdPs ermöglichen es Ihnen, eine Anwendungsintegration bei Bedarf deaktiviert zu lassen. Wir empfehlen Ihnen, die direkte IAM-Verbundanwendung in Ihrem IdP deaktiviert zu lassen, bis sie für den Notfallzugriff erforderlich ist.

Sicherheit in AWS IAM Identity Center

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS IAM Identity Center, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von IAM Identity Center anwenden können. In den folgenden Themen erfahren Sie, wie Sie IAM Identity Center konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer IAM Identity Center-Ressourcen unterstützen.

Themen

Identitäts- und Zugriffsmanagement für IAM Identity Center

Für den Zugriff auf das IAM Identity Center sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen verfügen, z. B. für eine AWS verwaltete Anwendung.

Die Authentifizierung beim AWS Zugriffsportal wird durch das Verzeichnis gesteuert, das Sie mit dem IAM Identity Center verbunden haben. Die Autorisierung für die, AWS-Konten die Benutzern vom AWS Zugriffsportal aus zur Verfügung stehen, wird jedoch von zwei Faktoren bestimmt:

1. Wem wurde Zugriff auf die Dateien AWS-Konten in der IAM Identity Center-Konsole zugewiesen. Weitere Informationen finden Sie unter Single Sign-On-Zugriff auf AWS-Konten.
2. Welche Berechtigungsstufen wurden den Benutzern in der IAM Identity Center-Konsole gewährt, um ihnen den entsprechenden Zugriff darauf zu ermöglichen. AWS-Konten Weitere Informationen finden Sie unter Berechtigungssätze erstellen, verwalten und löschen.

In den folgenden Abschnitten wird erläutert, wie Sie als Administrator den Zugriff auf die IAM Identity Center-Konsole steuern oder den Administratorzugriff für day-to-day Aufgaben von der IAM Identity Center-Konsole aus delegieren können.

- Authentifizierung
- Zugriffskontrolle

Authentifizierung

Erfahren Sie, wie Sie AWS mithilfe von IAM-Identitäten darauf zugreifen können.

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen zu authentifizieren. Wenn Sie jedoch nicht über die entsprechenden Berechtigungen verfügen, können Sie keine IAM Identity Center-Ressourcen erstellen oder darauf zugreifen. Sie benötigen beispielsweise die erforderlichen Berechtigungen, um ein mit IAM Identity Center verbundenes Verzeichnis zu erstellen.

In den folgenden Abschnitten wird beschrieben, wie Sie Berechtigungen für IAM Identity Center verwalten. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen
- Beispiele für identitätsbasierte Richtlinien für IAM Identity Center
- Verwendung von serviceverknüpften Rollen für IAM Identity Center

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen

Jede AWS Ressource gehört einem AWS-Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen werden durch Berechtigungsrichtlinien geregelt. Um Zugriff zu gewähren, kann ein Kontoadministrator Berechtigungen für IAM-Identitäten (d. h. Benutzer, Gruppen und Rollen) hinzufügen. Einige Dienste (z. B. AWS Lambda) unterstützen auch das Hinzufügen von Berechtigungen zu Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Themen

- Ressourcen und Operationen von IAM Identity Center
- Grundlegendes zum Eigentum an Ressourcen
- Verwalten des Zugriffs auf Ressourcen
- Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipien
- Angeben von Bedingungen in einer Richtlinie

Ressourcen und Operationen von IAM Identity Center

In IAM Identity Center sind die primären Ressourcen Anwendungsinstanzen, Profile und Berechtigungssätze.

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist derjenige AWS-Konto , der eine Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist derjenige AWS-Konto der Hauptentität (das Konto, ein Benutzer oder eine

IAM-Rolle), die die Anfrage authentifiziert, mit der die Ressource erstellt wird. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn der eine IAM Identity Center-Ressource Root-Benutzer des AWS-Kontos erstellt, z. B. eine Anwendungsinstanz oder einen Berechtigungssatz, sind Sie AWS-Konto der Eigentümer dieser Ressource.
- Wenn Sie in Ihrem AWS Konto einen Benutzer erstellen und diesem Benutzer Berechtigungen zum Erstellen von IAM Identity Center-Ressourcen gewähren, kann der Benutzer dann IAM Identity Center-Ressourcen erstellen. Ihr AWS Konto, zu dem der Benutzer gehört, besitzt jedoch die Ressourcen.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Erstellen von IAM Identity Center-Ressourcen erstellen, kann jeder, der diese Rolle übernehmen kann, IAM Identity Center-Ressourcen erstellen. Ihnen AWS-Konto, zu der die Rolle gehört, gehören die IAM Identity Center-Ressourcen.

Verwalten des Zugriffs auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> In diesem Abschnitt wird die Verwendung von IAM im Kontext von IAM Identity Center beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Informationen über die Syntax und Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

An eine IAM-Identität angefügte Richtlinien werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet. An Ressourcen angehängte Richtlinien werden als ressourcenbasierte Richtlinien bezeichnet. IAM Identity Center unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Identitätsbasierte Richtlinien (IAM-Richtlinien)
- Ressourcenbasierte Richtlinien

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Sie können IAM-Identitäten Berechtigungen hinzufügen. Sie können z. B. Folgendes tun:

- Ordnen Sie einem Benutzer oder einer Gruppe in Ihrer Gruppe eine Berechtigungsrichtlinie zu AWS-Konto — Ein Kontoadministrator kann mithilfe einer Berechtigungsrichtlinie, die einem bestimmten Benutzer zugeordnet ist, diesem Benutzer Berechtigungen zum Hinzufügen einer IAM Identity Center-Ressource, z. B. einer neuen Anwendung, gewähren.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen.

  Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit beginne `List`. Diese Aktionen zeigen Informationen über eine IAM Identity Center-Ressource an, z. B. eine Anwendungsinstanz oder einen Berechtigungssatz. Beachten Sie, dass das Platzhalterzeichen (*) im `Resource` Element angibt, dass die Aktionen für alle IAM Identity Center-Ressourcen zulässig sind, die dem Konto gehören.

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

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit IAM Identity Center finden Sie unter. Beispiele für identitätsbasierte Richtlinien für IAM Identity Center Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Beispielsweise können Sie einem S3 Bucket eine Richtlinie zuweisen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. IAM Identity Center unterstützt keine ressourcenbasierten Richtlinien.

Spezifizierung von Richtlinienelementen: Aktionen, Auswirkungen, Ressourcen und Prinzipien

Für jede IAM Identity Center-Ressource (siehe Ressourcen und Operationen von IAM Identity Center) definiert der Service eine Reihe von API-Vorgängen. Um Berechtigungen für diese API-Operationen zu gewähren, definiert IAM Identity Center eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können. Zur Durchführung einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Die Berechtigung gewährt dem Benutzer beispielsweise die `sso:DescribePermissionsPolicies` Erlaubnis, den IAM Identity `DescribePermissionsPolicies` Center-Vorgang auszuführen.
- Auswirkung – Die von Ihnen festgelegte Auswirkung, wenn der Benutzer die jeweilige Aktion anfordert – entweder „allow“ (Zugriffserlaubnis) oder „deny“ (Zugriffsverweigerung). Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten ("Allow"), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. In ressourcenbasierten Richtlinien müssen Sie den Benutzer, das Konto, den Service oder die sonstige Entität angeben, die die Berechtigungen erhalten soll (gilt nur für ressourcenbasierte Richtlinien). IAM Identity Center unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax und zu Beschreibungen von IAM-Richtlinien finden Sie in der AWS -IAM-Richtlinienreferenz im IAM-Benutzerhandbuch.

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der Sprache der Zugriffsrichtlinie die Bedingungen angeben, die erfüllt werden müssen, damit die Richtlinie in Kraft tritt. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Es gibt keine spezifischen Bedingungsschlüssel für IAM Identity Center. Es gibt jedoch AWS Bedingungsschlüssel, die Sie je nach Bedarf verwenden können. Eine vollständige Liste der AWS Schlüssel finden Sie unter Verfügbare globale Bedingungsschlüssel im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für IAM Identity Center

Dieses Thema enthält Beispiele für IAM-Richtlinien, die Sie erstellen können, um Benutzern und Rollen Berechtigungen zur Verwaltung von IAM Identity Center zu gewähren.

> **Important**
>
> Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die grundlegenden Konzepte und Optionen erläutert werden, mit denen Sie den Zugriff auf Ihre IAM Identity Center-Ressourcen verwalten können. Weitere Informationen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre IAM Identity Center-Ressourcen.

Dieses Thema besteht aus folgenden Abschnitten:

- Beispiele für benutzerdefinierte Richtlinien
- Für die Verwendung der IAM Identity Center-Konsole sind Berechtigungen erforderlich

Beispiele für benutzerdefinierte Richtlinien

Dieser Abschnitt enthält Beispiele für gängige Anwendungsfälle, für die eine benutzerdefinierte IAM-Richtlinie erforderlich ist. Bei diesen Beispielrichtlinien handelt es sich um identitätsbasierte Richtlinien, die das Principal-Element nicht spezifizieren. Das liegt daran, dass Sie bei einer identitätsbasierten Richtlinie nicht den Prinzipal angeben, der die Erlaubnis erhält. Stattdessen fügen Sie die Richtlinie dem Prinzipal hinzu. Wenn Sie einer IAM-Rolle eine identitätsbasierte

Berechtigungsrichtlinie zuordnen, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen. Sie können identitätsbasierte Richtlinien in IAM erstellen und diese Benutzern, Gruppen und/oder Rollen zuordnen. Sie können diese Richtlinien auch auf IAM Identity Center-Benutzer anwenden, wenn Sie in IAM Identity Center einen Berechtigungssatz erstellen.

> **Note**
>
> Verwenden Sie diese Beispiele, wenn Sie Richtlinien für Ihre Umgebung erstellen, und stellen Sie sicher, dass Sie Tests sowohl auf positive („Zugriff gewährt“) als auch auf negative („Zugriff verweigert“) Testfälle durchführen, bevor Sie diese Richtlinien in Ihrer Produktionsumgebung bereitstellen. Weitere Informationen zum Testen von IAM-Richtlinien finden Sie unter Testen von IAM-Richtlinien mit dem IAM-Richtliniensimulator im IAM-Benutzerhandbuch.

Themen

Beispiel 1: Erlauben Sie einem Benutzer, IAM Identity Center aufzurufen

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer nur Leseberechtigungen, sodass er alle in IAM Identity Center konfigurierten Einstellungen und Verzeichnisinformationen einsehen kann.

> **Note**
>
> Diese Richtlinie dient nur zu Beispielzwecken. In einer Produktionsumgebung empfehlen wir, die `ViewOnlyAccess` AWS verwaltete Richtlinie für IAM Identity Center zu verwenden.

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

```
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel 2: Erlauben Sie einem Benutzer, seine Berechtigungen AWS-Konten in IAM Identity Center zu verwalten

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, die es einem Benutzer ermöglichen, Berechtigungssätze für Sie zu erstellen, zu verwalten und bereitzustellen. AWS-Konten

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

```
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
```

```
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> Die zusätzlichen Berechtigungen`"Sid": "IAMListPermissions"`, die in den `"Sid": "AccessToSSOProvisiondRoles"` Abschnitten und aufgeführt sind, sind nur erforderlich, damit der Benutzer Aufgaben im AWS Organizations Verwaltungskonto erstellen kann. In bestimmten Fällen müssen Sie diese Abschnitte möglicherweise auch erweiterniam:UpdateSAMLProvider.

Beispiel 3: Erlauben Sie einem Benutzer, Anwendungen in IAM Identity Center zu verwalten

Die folgende Berechtigungsrichtlinie gewährt Benutzern Berechtigungen zum Anzeigen und Konfigurieren von Anwendungen in IAM Identity Center, einschließlich vorintegrierter SaaS-Anwendungen aus dem IAM Identity Center-Katalog.

> **Note**
>
> Der im folgenden Richtlinienbeispiel verwendete `sso:AssociateProfile` Vorgang ist für die Verwaltung von Benutzer- und Gruppenzuweisungen zu Anwendungen erforderlich. Es ermöglicht einem Benutzer auch, AWS-Konten mithilfe vorhandener Berechtigungssätze Benutzer und Gruppen zuzuweisen. Wenn ein Benutzer den AWS-Konto Zugriff innerhalb von IAM Identity Center verwalten muss und die für die Verwaltung von Berechtigungssätzen erforderlichen Berechtigungen benötigt, finden Sie weitere Informationen unterBeispiel 2: Erlauben Sie einem Benutzer, seine Berechtigungen AWS-Konten in IAM Identity Center zu verwalten.

Seit Oktober 2020 sind viele dieser Operationen nur über die AWS Konsole verfügbar. Diese Beispielrichtlinie umfasst „Lesen“ -Aktionen wie „Auflisten“, „Abrufen“ und „Suchen“, die für den fehlerfreien Betrieb der Konsole in diesem Fall relevant sind.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Beispiel 4: Erlauben Sie einem Benutzer, Benutzer und Gruppen in Ihrem Identity Center-Verzeichnis zu verwalten

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer Berechtigungen, die es einem Benutzer ermöglichen, Benutzer und Gruppen in IAM Identity Center zu erstellen, anzuzeigen, zu ändern und zu löschen.

In einigen Fällen sind direkte Änderungen an Benutzern und Gruppen in IAM Identity Center eingeschränkt. Dies ist beispielsweise der Fall, wenn Active Directory oder ein externer Identitätsanbieter mit aktivierter automatischer Bereitstellung als Identitätsquelle ausgewählt wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Für die Verwendung der IAM Identity Center-Konsole sind Berechtigungen erforderlich

Damit ein Benutzer fehlerfrei mit der IAM Identity Center-Konsole arbeiten kann, sind zusätzliche Berechtigungen erforderlich. Wenn eine IAM-Richtlinie erstellt wurde, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktioniert die Konsole für Benutzer mit dieser Richtlinie nicht wie vorgesehen. Im folgenden Beispiel werden die Berechtigungen aufgeführt, die möglicherweise erforderlich sind, um einen fehlerfreien Betrieb innerhalb der IAM Identity Center-Konsole sicherzustellen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
```

```
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS verwaltete Richtlinien für IAM Identity Center

Die Erstellung von kundenverwalteten IAM-Richtlinien, die Ihrem Team nur die erforderlichen Berechtigungen gewähren, erfordert Zeit und Fachwissen. Um schnell loszulegen, können Sie AWS verwaltete Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS -Richtlinien finden Sie unter Verwaltete AWS -Richtlinien im IAM-Leitfaden.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

Neue Aktionen, mit denen Sie Benutzersitzungen auflisten und löschen können, sind unter dem neuen Namespace verfügbar. `identitystore-auth` Alle zusätzlichen Berechtigungen für Aktionen in diesem Namespace werden auf dieser Seite aktualisiert. Vermeiden Sie beim Erstellen Ihrer benutzerdefinierten IAM-Richtlinien die Verwendung von `*` after, `identitystore-auth` da dies für alle Aktionen gilt, die heute oder in future im Namespace existieren.

AWS verwaltete Richtlinie: AWSSSOMasterAccountAdministrator

Die `AWSSSOMasterAccountAdministrator` Richtlinie sieht die erforderlichen Verwaltungsmaßnahmen für die Schulleiter vor. Die Richtlinie richtet sich an Schulleiter, die die Rolle eines AWS IAM Identity Center Administrators ausüben. Im Laufe der Zeit wird die Liste der bereitgestellten Aktionen aktualisiert, sodass sie der vorhandenen Funktionalität von IAM Identity Center und den Aktionen entspricht, die als Administrator erforderlich sind.

Sie können die `AWSSSOMasterAccountAdministrator`-Richtlinie an Ihre IAM-Identitäten anfügen. Wenn Sie die `AWSSSOMasterAccountAdministrator` Richtlinie an eine Identität anhängen, gewähren Sie AWS IAM Identity Center Administratorberechtigungen. Principals mit dieser Richtlinie können innerhalb des AWS Organizations Verwaltungskontos und aller Mitgliedskonten auf IAM Identity Center zugreifen. Dieser Principal kann alle IAM Identity Center-Vorgänge vollständig verwalten, einschließlich der Möglichkeit, eine IAM Identity Center-Instanz, Benutzer, Berechtigungssätze und Zuweisungen zu erstellen. Der Principal kann diese Zuweisungen auch in allen Mitgliedskonten der AWS Organisation instanziieren und Verbindungen zwischen AWS Directory Service verwalteten Verzeichnissen und IAM Identity Center herstellen. Sobald neue Verwaltungsfunktionen veröffentlicht werden, erhält der Kontoadministrator diese Berechtigungen automatisch.

Gruppierungen von Berechtigungen

Diese Richtlinie ist in Anweisungen gruppiert, die auf den bereitgestellten Berechtigungen basieren.

- `AWSSSOMasterAccountAdministrator`— Ermöglicht es IAM Identity Center, die benannte Servicerolle `AWSServiceRoleforSSO` an IAM Identity Center weiterzuleiten, sodass es später die

Rolle übernehmen und Aktionen in ihrem Namen ausführen kann. Dies ist erforderlich, wenn die Person oder Anwendung versucht, IAM Identity Center zu aktivieren. Weitere Informationen finden Sie unter Zugriff verwalten auf AWS-Konten.

- `AWSSSOMemberAccountAdministrator`— Ermöglicht IAM Identity Center, Kontoadministratoraktionen in einer Umgebung mit mehreren AWS Konten durchzuführen. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AWSSSOMemberAccountAdministrator.
- `AWSSSOManageDelegatedAdministrator`— Ermöglicht IAM Identity Center die Registrierung und Deregistrierung eines delegierten Administrators für Ihre Organisation.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz zu AWSSSOMasterAccountAdministratorverwalteten AWS Richtlinien.

Zusätzliche Informationen zu dieser Richtlinie

Wenn IAM Identity Center zum ersten Mal aktiviert wird, erstellt der IAM Identity Center-Dienst eine dienstverknüpfte Rolle im AWS Organizations Verwaltungskonto (früher Hauptkonto), sodass IAM Identity Center die Ressourcen in Ihrem Konto verwalten kann. Die erforderlichen Aktionen sind `iam:CreateServiceLinkedRole` und`iam:PassRole`, die in den folgenden Codefragmenten dargestellt werden.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
```

```
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
}
```

AWS verwaltete Richtlinie: AWSSSOMemberAccountAdministrator

Die `AWSSSOMemberAccountAdministrator` Richtlinie sieht die erforderlichen Verwaltungsmaßnahmen für die Schulleiter vor. Die Richtlinie richtet sich an Principals, die die Rolle eines IAM Identity Center-Administrators ausüben. Im Laufe der Zeit wird die Liste der bereitgestellten Aktionen aktualisiert, sodass sie der bestehenden Funktionalität von IAM Identity Center und den Aktionen entspricht, die als Administrator erforderlich sind.

Sie können die `AWSSSOMemberAccountAdministrator`-Richtlinie an Ihre IAM-Identitäten anfügen. Wenn Sie die `AWSSSOMemberAccountAdministrator` Richtlinie an eine Identität anhängen, gewähren Sie AWS IAM Identity Center Administratorberechtigungen. Principals mit dieser Richtlinie können innerhalb des AWS Organizations Verwaltungskontos und aller Mitgliedskonten auf IAM Identity Center zugreifen. Dieser Principal kann alle IAM Identity Center-Vorgänge vollständig verwalten, einschließlich der Möglichkeit, Benutzer, Berechtigungssätze und Zuweisungen zu erstellen. Der Principal kann diese Zuweisungen auch in allen Mitgliedskonten der AWS Organisation instanziieren und Verbindungen zwischen AWS Directory Service verwalteten Verzeichnissen und IAM Identity Center herstellen. Sobald neue Verwaltungsfunktionen veröffentlicht werden, erhält der Kontoadministrator diese Berechtigungen automatisch.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSSSOMemberAccountAdministratorReferenz für AWS verwaltete Richtlinien.

Zusätzliche Informationen zu dieser Richtlinie

IAM Identity Center-Administratoren verwalten Benutzer, Gruppen und Passwörter in ihrem Identity Center-Verzeichnisspeicher (sso-Verzeichnis). Die Rolle des Kontoadministrators umfasst Berechtigungen für die folgenden Aktionen:

- `"sso:*"`

- `"sso-directory:*"`

IAM Identity Center-Administratoren benötigen eingeschränkte Berechtigungen für die folgenden AWS Directory Service Aktionen, um tägliche Aufgaben ausführen zu können.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`
- `"ds:AuthorizeApplication"`
- `“ds:CreateAlias”`

Diese Berechtigungen ermöglichen es IAM Identity Center-Administratoren, vorhandene Verzeichnisse zu identifizieren und Anwendungen zu verwalten, sodass sie für die Verwendung mit IAM Identity Center konfiguriert werden können. Weitere Informationen zu jeder dieser Aktionen finden Sie unter AWS Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen.

IAM Identity Center verwendet IAM-Richtlinien, um IAM Identity Center-Benutzern Berechtigungen zu gewähren. IAM Identity Center-Administratoren erstellen Berechtigungssätze und fügen ihnen Richtlinien hinzu. Der IAM Identity Center-Administrator muss berechtigt sein, die vorhandenen Richtlinien aufzulisten, sodass er auswählen kann, welche Richtlinien mit dem Berechtigungssatz verwendet werden sollen, den er gerade erstellt oder aktualisiert. Um sichere und funktionale Berechtigungen festzulegen, muss der IAM Identity Center-Administrator über die erforderlichen Berechtigungen verfügen, um die IAM Access Analyzer-Richtlinienvalidierung auszuführen.

- `"iam:ListPolicies"`
- `"access-analyzer:ValidatePolicy"`

IAM Identity Center-Administratoren benötigen eingeschränkten Zugriff auf die folgenden AWS Organizations Aktionen, um tägliche Aufgaben ausführen zu können:

- `"organizations:EnableAWSServiceAccess"`
- `"organizations:ListRoots"`
- `"organizations:ListAccounts"`
- `"organizations:ListOrganizationalUnitsForParent"`

- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

Diese Berechtigungen ermöglichen es IAM Identity Center-Administratoren, mit Unternehmensressourcen (Konten) für grundlegende IAM Identity Center-Verwaltungsaufgaben wie die folgenden zu arbeiten:

- Identifizieren des Verwaltungskontos, das zur Organisation gehört
- Identifizierung der Mitgliedskonten, die zur Organisation gehören
- Aktivieren des AWS Servicezugriffs für Konten
- Einen delegierten Administrator einrichten und verwalten

Weitere Informationen zur Verwendung eines delegierten Administrators mit IAM Identity Center finden Sie unter. Delegierte Verwaltung Weitere Informationen zur Verwendung dieser Berechtigungen mit AWS Organizations finden Sie unter Verwendung AWS Organizations mit anderen AWS Diensten.

AWS verwaltete Richtlinie: AWSSSODirectoryAdministrator

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

Diese Richtlinie gewährt Administratorberechtigungen für Benutzer und Gruppen von IAM Identity Center. Principals, denen diese Richtlinie zugewiesen ist, können alle Aktualisierungen für IAM Identity Center-Benutzer und -Gruppen vornehmen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz zu AWSSSODirectoryAdministrator AWSverwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSSSOReadOnly

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

Diese Richtlinie gewährt Benutzern nur Leseberechtigungen, die es Benutzern ermöglichen, Informationen in IAM Identity Center einzusehen. Principals, denen diese Richtlinie zugewiesen ist, können die Benutzer oder Gruppen von IAM Identity Center nicht direkt einsehen. Principals, denen diese Richtlinie zugewiesen ist, können keine Aktualisierungen in IAM Identity Center vornehmen. Principals mit diesen Berechtigungen können beispielsweise die IAM Identity Center-Einstellungen einsehen, aber keinen der Einstellungswerte ändern.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSSSOReadOnlyReferenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSSODirectoryReadOnly

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

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer und Gruppen in IAM Identity Center anzeigen können. Principals, denen diese Richtlinie zugewiesen ist, können IAM Identity Center-Zuweisungen, Berechtigungssätze, Anwendungen oder Einstellungen nicht einsehen. Principals, denen diese Richtlinie zugewiesen ist, können keine Aktualisierungen in IAM Identity Center vornehmen. Principals mit diesen Berechtigungen können beispielsweise IAM Identity Center-Benutzer anzeigen, aber sie können keine Benutzerattribute ändern oder MFA-Geräte zuweisen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz zu AWSSSODirectoryReadOnly AWSverwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSIdentitySyncFullAccess

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

Principals, denen diese Richtlinie beigefügt ist, verfügen über uneingeschränkte Zugriffsberechtigungen zum Erstellen und Löschen von Synchronisierungsprofilen, zum Zuordnen oder Aktualisieren eines Synchronisierungsprofils zu einem Synchronisierungsziel, zum Erstellen, Auflisten und Löschen von Synchronisationsfiltern sowie zum Starten oder Beenden der Synchronisation.

Einzelheiten zu den Berechtigungen

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz AWSIdentitySyncFullAccesszu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSIdentitySyncReadOnlyAccess

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

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer Informationen über das Identitätssynchronisierungsprofil, die Filter und die Zieleinstellungen einsehen können. Prinzipale, denen diese Richtlinie zugewiesen ist, können die Synchronisierungseinstellungen nicht aktualisieren. Prinzipale mit diesen Berechtigungen können beispielsweise Einstellungen für die Identitätssynchronisierung einsehen, aber keine Profil- oder Filterwerte ändern.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSIdentitySyncReadOnlyAccessReferenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSSSOServiceRolePolicy

Sie können die `AWSSSOServiceRolePolicy` Richtlinie nicht an Ihre IAM-Identitäten anhängen.

Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es IAM Identity Center ermöglicht, zu delegieren und durchzusetzen, welche Benutzer über Single Sign-On-Zugriff auf bestimmte Eingänge verfügen. AWS-Konten AWS Organizations Wenn Sie IAM aktivieren, wird in allen Bereichen Ihrer Organisation eine serviceverknüpfte Rolle erstellt. AWS-Konten IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen. Mit Diensten verknüpfte Rollen, die in den einzelnen Rollen erstellt werden, AWS-Konto sind benannt. `AWSServiceRoleForSSO` Weitere Informationen finden Sie unter Verwendung von serviceverknüpften Rollen für IAM Identity Center.

AWS verwaltete Richtlinie: AWSIAMIdentityCenterAllowListForIdentityContext

Wenn Sie eine Rolle mit dem IAM Identity Center-Identitätskontext übernehmen, hängt AWS Security Token Service (AWS STS) die `AWSIAMIdentityCenterAllowListForIdentityContext` Richtlinie automatisch an die Rolle an.

Diese Richtlinie enthält die Liste der Aktionen, die zulässig sind, wenn Sie Trusted Identity Propagation mit Rollen verwenden, für die der IAM Identity Center-Identitätskontext verwendet wird. Alle anderen Aktionen, die in diesem Kontext aufgerufen werden, sind blockiert. Der Identitätskontext wird als übergeben`ProvidedContext`.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Referenz AWSIAMIdentityCenterAllowListForIdentityContextzu AWS verwalteten Richtlinien.

IAM Identity Center aktualisiert AWS verwaltete Richtlinien

In der folgenden Tabelle werden die Aktualisierungen der AWS verwalteten Richtlinien für IAM Identity Center seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst beschrieben.

Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Dokumentenverlauf von IAM Identity Center.

Änderung	Beschreibung	Datum
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `elasticmapreduce:ListSteps` Aktionen`elasticmapreduce:AddJobFlowSteps` ,`elasticmapreduce:DescribeCluster` , `elasticmapreduce:CancelSteps` `elasticmapreduce:DescribeStep` , und zur Unterstützung der Verbreitung vertrauenswürdiger Identitäten in Amazon EMR.	17. Mai 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die`qapps:CreateQApp` ,,`qapps:PredictProblemStatementFromConversation` ,`qapps:PredictQAppFromProblemStatement` ,,`qapps:CopyQApp` ,`qapps:GetQApp` ,`qapps:ListQApps` ,`qapps:UpdateQApp` ,`qapps:DeleteQApp` ,`qapps:AssociateQAppWithUser` ,,`qapps:DisassociateQAppFromUser` ,`qapps:Imp`	30. April 2024

Änderung	Beschreibung	Datum
	`ortDocume ntToQApp` ,`qapps:Imp ortDocumentToQAppS ession` ,`qapps:Cre ateLibrar yItem` ,`qapps:Get LibraryItem` , `qapps:UpdateLibrar yItem` `qapps:Cre ateLibraryItemRevi ew` `qapps:ListLibraryI tems` `qapps:Cre ateSubscriptionTok en` `qapps:StartQAppSes sion` , und `qapps:Sto pQAppSession` Aktionen zur Unterstützung identität sbewusster Konsolens itzungen für AWS verwaltet e Anwendungen, die diese Sitzungen unterstützen.	
AWSSSOMasterAccoun tAdministrator	Diese Richtlinie umfasst jetzt die `signin:CreateTrust edIdentityPropagat ionApplicationForC onsole` und `signin:Li stTrustedIdentityP ropagationApplicat ionsForConsole` Aktionen zur Unterstützung identitätsbewusster Konsolens itzungen für AWS verwaltet e Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderung	Beschreibung	Datum
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt die `signin:CreateTrustedIdentityPropagationApplicationForConsole` und `signin:ListTrustedIdentityPropagationApplicationsForConsole` Aktionen zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSSSOReadOnly	Diese Richtlinie umfasst jetzt die `signin:ListTrustedIdentityPropagationApplicationsForConsole` Aktion zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `qbusiness:PutFeedback` Aktion zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	26. April 2024

Änderung	Beschreibung	Datum
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `q:UpdateTroubleshootingCommandResult` Aktionen `q:StartConversation`, `q:SendMessage`, `q:ListConversations`, `q:GetConversation` `q:StartTroubleshootingAnalysis` `q:GetTroubleshootingResults` `q:StartTroubleshootingResolutionExplanation`, und zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	24. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `sts:SetContext` Aktion zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	19. April 2024

Änderung	Beschreibung	Datum
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `qbusiness:DeleteConversation` Aktionen `qbusiness:Chat` ,, `qbusiness:ChatSync` `qbusiness:ListConversations` `qbusiness:ListMessages` , und zur Unterstützung identitätsbewusster Konsolensitzungen für AWS verwaltete Anwendungen, die diese Sitzungen unterstützen.	11. April 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie umfasst jetzt die `s3:GetDataAccess` Aktionen `s3:GetAccessGrantsInstanceForPrefix` und.	26. November 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Diese Richtlinie enthält die Liste der Aktionen, die zulässig sind, wenn Sie Trusted Identity Propagation mit Rollen verwenden, für die der IAM Identity Center-Identitätskontext verwendet wird.	15. November 2023

Änderung	Beschreibung	Datum
AWSSSODirectoryReadOnly	Diese Richtlinie umfasst jetzt den neuen Namespace `identitystore-auth` mit neuen Berechtigungen, die es Benutzern ermöglichen, Sitzungen aufzulisten und abzurufen.	21. Februar 2023
AWSSSOServiceRolePolicy	Diese Richtlinie ermöglicht nun, dass die `UpdateSAMLProvider` Aktion für das Verwaltungskonto ausgeführt wird.	20. Oktober 2022
AWSSSOMasterAccountAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace `identitystore-auth` mit neuen Berechtigungen, die es dem Administrator ermöglichen, Sitzungen für einen Benutzer aufzulisten und zu löschen.	20. Oktober 2022
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace `identitystore-auth` mit neuen Berechtigungen, die es dem Administrator ermöglichen, Sitzungen für einen Benutzer aufzulisten und zu löschen.	20. Oktober 2022

Änderung	Beschreibung	Datum
AWSSSODirectoryAdministrator	Diese Richtlinie umfasst jetzt den neuen Namespace `identitystore-auth` mit neuen Berechtigungen, die es dem Administrator ermöglichen, Sitzungen für einen Benutzer aufzulisten und zu löschen.	20. Oktober 2022
AWSSSOMasterAccountAdministrator	Diese Richtlinie umfasst jetzt neue `ListDelegatedAdministrators` Anrufberechtigungen. AWS Organizations Diese Richtlinie umfasst jetzt auch eine Teilmenge von BerechtigungenAWSSSOMan `ageDelegatedAdministrator` , zu der auch Anrufberechtigungen `RegisterDelegatedAdministrator` und `DeregisterDelegatedAdministrator` gehören.	16. August 2022

Änderung	Beschreibung	Datum
AWSSSOMemberAccountAdministrator	Diese Richtlinie umfasst jetzt neue ListDelegatedAdministrators_ Anrufberechtigungen. AWS Organizations Diese Richtlinie umfasst jetzt auch eine Teilmenge von BerechtigungenAWSSSOManageDelegatedAdministrator , zu der auch Anrufberechtigungen RegisterDelegatedAdministrator und DeregisterDelegatedAdministrator gehören.	16. August 2022
AWSSSOReadOnly	Diese Richtlinie umfasst jetzt neue ListDelegatedAdministrators Anrufberechtigungen. AWS Organizations	11. August 2022
AWSSSOServiceRolePolicy	Diese Richtlinie umfasst jetzt neue Anrufberechtigungen DeleteRolePermissionsBoundary undPutRolePermisionsBoundary .	14. Juli 2022

Änderung	Beschreibung	Datum
AWSSSOServiceRolePolicy	Diese Richtlinie umfasst jetzt neue Berechtigungen, die eingehende Anrufe ermöglichen `ListAWSServiceAccessForOrganization` and `ListDelegatedAdministrators` AWS Organizations.	11. Mai 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Fügen Sie IAM Access Analyzer-Berechtigungen hinzu, die es einem Prinzipal ermöglichen, die Richtlinienprüfungen zur Validierung zu verwenden.	28. April 2022
AWSSSOMasterAccountAdministrator	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen. Informationen zu den im IAM Identity Center Identity Store-Dienst verfügbaren Aktionen finden Sie in der IAM Identity Center Identity Store-API-Referenz.	29. März 2022
AWSSSOMemberAccountAdministrator	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen.	29. März 2022
AWSSSODirectoryAdministrator	Diese Richtlinie erlaubt jetzt alle IAM Identity Center Identity Store-Dienstaktionen.	29. März 2022

Änderung	Beschreibung	Datum
AWSSSODirectoryReadOnly	Diese Richtlinie gewährt jetzt Zugriff auf die Leseaktionen des IAM Identity Center Identity Store-Dienstes. Dieser Zugriff ist erforderlich, um Benutzer- und Gruppeninformationen aus dem IAM Identity Center Identity Store-Dienst abzurufen.	29. März 2022
AWSIdentitySyncFullAccess	Diese Richtlinie ermöglicht vollen Zugriff auf Berechtigungen zur Identitätssynchronisierung.	3. März 2022
AWSIdentitySyncReadOnlyAccess	Diese Richtlinie gewährt nur Leseberechtigungen, die es einem Prinzipal ermöglichen, Einstellungen zur Identitätssynchronisierung einzusehen.	3. März 2022
AWSSSOReadOnly	Diese Richtlinie gewährt Nur-Lese-Berechtigungen, die es einem Principal ermöglichen, die IAM Identity Center-Konfigurationseinstellungen einzusehen.	4. August 2021
IAM Identity Center hat mit der Nachverfolgung von Änderungen begonnen	IAM Identity Center begann, Änderungen für AWS verwaltete Richtlinien nachzuverfolgen.	4. August 2021

Verwendung von serviceverknüpften Rollen für IAM Identity Center

AWS IAM Identity Center verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit IAM Identity Center verknüpft ist. Sie ist von IAM Identity Center vordefiniert und umfasst alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen. Weitere Informationen finden Sie unter Service-verknüpfte Rollen.

Eine dienstbezogene Rolle erleichtert die Einrichtung von IAM Identity Center, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. IAM Identity Center definiert die Berechtigungen seiner dienstbezogenen Rolle, und sofern nicht anders definiert, kann nur IAM Identity Center diese Rolle übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für IAM Identity Center

IAM Identity Center verwendet die benannte dienstverknüpfte Rolle AWSServiceRoleForSSO, um IAM Identity Center Berechtigungen zur Verwaltung von AWS Ressourcen, einschließlich IAM-Rollen, Richtlinien und SAML-IdP, in Ihrem Namen zu gewähren.

Die AWSServiceRoleForSSO dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `IAM Identity Center`

Die Berechtigungsrichtlinie für AWSServiceRoleForSSO dienstbezogene Rollen ermöglicht es IAM Identity Center, für Rollen im Pfad „/aws-reserved/sso.amazonaws.com/“ und mit dem Namenspräfix „_“ Folgendes auszuführen: AWSReservedSSO

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam:DeleteRole`

- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

Die Richtlinie für AWSServiceRoleForSSO dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, bei SAML-Anbietern mit dem Namenspräfix „_“ Folgendes auszuführen: AWSSSO

- iam:CreateSAMLProvider
- iam:GetSAMLProvider
- iam:UpdateSAMLProvider
- iam:DeleteSAMLProvider

Die Richtlinie für AWSServiceRoleForSSO dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, in allen Organisationen Folgendes durchzuführen:

- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedAdministrators

Die Richtlinie für AWSServiceRoleForSSO dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, Folgendes für alle IAM-Rollen durchzuführen (*):

- iam:listRoles

Die Richtlinie für AWSServiceRoleForSSO dienstbezogene Rollenberechtigungen ermöglicht es IAM Identity Center, auf „arn:aws:iam: :*:role/ /sso.amazonaws.com/“ Folgendes auszuführen: aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

Die Richtlinie für Rollenberechtigungen ermöglicht es IAM Identity Center, die folgenden Aktionen an Ressourcen durchzuführen.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
```

```
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
```

```
        }
      }
    },
    {
      "Sid": "IAMSAMLProviderUpdateAction",
      "Effect": "Allow",
      "Action": [
        "iam:UpdateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
      ]
    },
    {
       "Sid":"IAMSAMLProviderCleanupActions",
       "Effect":"Allow",
       "Action":[
          "iam:DeleteSAMLProvider",
          "iam:GetSAMLProvider"
       ],
       "Resource":[
          "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ]
    },
    {
       "Effect":"Allow",
       "Action":[
          "organizations:DescribeAccount",
          "organizations:DescribeOrganization",
          "organizations:ListAccounts",
          "organizations:ListAWSServiceAccessForOrganization",
          "organizations:ListDelegatedAdministrators"
       ],
       "Resource":[
          "*"
       ]
    },
    {
       "Sid":"AllowUnauthAppForDirectory",
       "Effect":"Allow",
       "Action":[
          "ds:UnauthorizeApplication"
       ],
       "Resource":[
```

```
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
         "Effect":"Allow",
         "Action":[
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine dienstbezogene Rolle für IAM Identity Center erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Nach der Aktivierung erstellt IAM Identity Center eine serviceverknüpfte Rolle für alle Konten innerhalb der Organisation in AWS Organizations. IAM Identity Center erstellt außerdem dieselbe serviceverknüpfte Rolle in jedem Konto, das anschließend zu Ihrer Organisation hinzugefügt wird. Diese Rolle ermöglicht es IAM Identity Center, in Ihrem Namen auf die Ressourcen der einzelnen Konten zuzugreifen.

Hinweise

- Wenn Sie beim AWS Organizations Verwaltungskonto angemeldet sind, verwendet es Ihre aktuell angemeldete Rolle und nicht die dienstverknüpfte Rolle. Dadurch wird die Eskalation von Rechten verhindert.
- Wenn IAM Identity Center irgendwelche IAM-Operationen im AWS Organizations Verwaltungskonto ausführt, werden alle Vorgänge mit den Anmeldeinformationen des IAM-Prinzipals ausgeführt. Auf diese Weise können die Anmeldungen CloudTrail nachvollziehen, wer alle Berechtigungsänderungen im Verwaltungskonto vorgenommen hat.

Important

Wenn Sie den IAM Identity Center-Dienst vor dem 7. Dezember 2017 verwendet haben, als er begann, dienstbezogene Rollen zu unterstützen, dann hat IAM Identity Center die AWSServiceRoleForSSO Rolle in Ihrem Konto erstellt. Weitere Informationen finden Sie unter Eine neue Rolle ist in meinem IAM-Konto erschienen.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen.

Bearbeitung einer dienstbezogenen Rolle für IAM Identity Center

In IAM Identity Center können Sie die serviceverknüpfte Rolle nicht bearbeiten. AWSServiceRoleForSSO Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für IAM Identity Center

Sie müssen die Rolle nicht manuell löschen. AWSServiceRoleForSSO Wenn eine aus einer AWS Organisation entfernt AWS-Konto wird, bereinigt IAM Identity Center automatisch die Ressourcen und löscht die mit dem Dienst verknüpfte Rolle aus dieser Organisation. AWS-Konto

Sie können auch die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die serviceverknüpfte Rolle manuell zu löschen. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zuerst manuell bereinigen, bevor Sie diese manuell löschen können.

> **Note**
>
> Wenn der IAM Identity Center-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um IAM Identity Center-Ressourcen zu löschen, die von AWSServiceRoleForSSO

1. Entfernen Sie den Benutzer- und Gruppenzugrifffür alle Benutzer und Gruppen, die Zugriff auf die AWS-Konto haben.
2. Löschen Sie Berechtigungssätzedie Sie mit dem verknüpft haben AWS-Konto.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die IAM-CLI oder die IAM-API, um die serviceverknüpfte Rolle zu löschen. AWSServiceRoleForSSO Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Leitfaden.

IAM Identity Center-Konsole und API-Autorisierung

Bestehende IAM Identity Center-Konsolen-APIs unterstützen die duale Autorisierung, sodass Sie bestehende API-Operationen weiterhin verwenden können, wenn neuere APIs verfügbar sind. Wenn Sie über bestehende Instanzen von IAM Identity Center verfügen, die vor dem 15. November 2023 und dem 15. Oktober 2020 erstellt wurden, können Sie anhand der folgenden Tabellen ermitteln, welche API-Operationen nun neueren API-Vorgängen zugeordnet sind, die nach diesen Daten veröffentlicht wurden.

Themen

- API-Aktionen nach November 2023
- API-Aktionen nach Oktober 2020

API-Aktionen nach November 2023

Instanzen von IAM Identity Center, die vor dem 15. November 2023 erstellt wurden, berücksichtigen sowohl alte als auch neue API-Aktionen, sofern keine der Aktionen ausdrücklich verweigert wird. Instanzen, die nach dem 15. November 2023 erstellt wurden, verwenden neuere API-Aktionen für die Autorisierung in der IAM Identity Center-Konsole.

Name des Konsolenvorgangs, der vor dem 15. November 2023 verwendet wurde	API-Aktion, die nach dem 15. November 2023 verwendet wurde
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Name des Konsolenvorgangs, der vor dem 15. November 2023 verwendet wurde	API-Aktion, die nach dem 15. November 2023 verwendet wurde
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

API-Aktionen nach Oktober 2020

Instanzen von IAM Identity Center, die vor dem 15. Oktober 2020 erstellt wurden, berücksichtigen sowohl alte als auch neue API-Aktionen, sofern keine der Aktionen ausdrücklich verweigert wird. Instanzen, die nach dem 15. Oktober 2020 erstellt wurden, verwenden neuere API-Aktionen für die Autorisierung in der IAM Identity Center-Konsole.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS Bedingungskontextschlüssel für IAM Identity Center

Wenn ein Principal eine Anfrage an stellt AWS, AWS sammelt er die Anforderungsinformationen in einem Anforderungskontext, der zur Auswertung und Autorisierung der Anfrage verwendet wird. Sie können das `Condition`-Element einer JSON-Richtlinie verwenden, um Schlüssel im Anforderungskontext mit Schlüsselwerten zu vergleichen, die Sie in Ihrer Richtlinie angeben. Die Anforderungsinformationen werden von verschiedenen Quellen bereitgestellt, darunter dem Principal, der die Anfrage stellt, der Ressource, der Anfrage, gegen die sie gestellt wurde, und den Metadaten zur Anfrage selbst. Dienstspezifische Bedingungsschlüssel werden für die Verwendung mit einem einzelnen AWS Dienst definiert.

IAM Identity Center umfasst einen AWS STS Kontextanbieter, der AWS es verwalteten Anwendungen und Drittanbieteranwendungen ermöglicht, Werte für Bedingungsschlüssel hinzuzufügen, die von IAM Identity Center definiert werden. Diese Schlüssel sind in IAM-Rollen enthalten. Die Schlüsselwerte werden festgelegt, wenn eine Anwendung ein Token an AWS STSübergibt. Die Anwendung erhält das Token, an das sie weitergibt, AWS STS auf eine der folgenden Arten:

- Während der Authentifizierung mit IAM Identity Center.
- Nach dem Token-Austausch mit einem vertrauenswürdigen Token-Aussteller zur Weitergabe vertrauenswürdiger Identitäten. In diesem Fall erhält die Anwendung ein Token von einem vertrauenswürdigen Token-Aussteller und tauscht dieses Token gegen ein Token von IAM Identity Center aus.

Diese Schlüssel werden in der Regel von Anwendungen verwendet, die in die Verbreitung vertrauenswürdiger Identitäten integriert sind. In einigen Fällen können Sie, wenn Schlüsselwerte vorhanden sind, diese Schlüssel in IAM-Richtlinien verwenden, die Sie erstellen, um Berechtigungen zuzulassen oder zu verweigern.

Beispielsweise möchten Sie möglicherweise bedingten Zugriff auf eine Ressource gewähren, die auf dem Wert von basiert. `UserId` Dieser Wert gibt an, welcher IAM Identity Center-Benutzer die

Rolle verwendet. Das Beispiel ähnelt der Verwendung `SourceId` von. Im `SourceId` Gegensatz dazu `UserId` steht der Wert für jedoch für einen bestimmten, verifizierten Benutzer aus dem Identitätsspeicher. Dieser Wert ist in dem Token enthalten, das die Anwendung erhält und an das sie dann AWS STS weiterleitet. Es handelt sich nicht um eine Allzweckzeichenfolge, die beliebige Werte enthalten kann.

Themen

Identitätsspeicher: UserId

Dieser Kontextschlüssel ist der `UserId` des IAM Identity Center-Benutzers, der Gegenstand der von IAM Identity Center ausgegebenen Kontext-Assertion ist. Die Kontext-Assertion wird an übergeben. AWS STS Sie können diesen Schlüssel verwenden, um den Namen `UserId` des IAM Identity Center-Benutzers, in dessen Namen die Anfrage gestellt wird, mit der ID für den Benutzer zu vergleichen, den Sie in der Richtlinie angeben.

- Verfügbarkeit — Dieser Schlüssel wird in den Anforderungskontext aufgenommen, nachdem eine vom IAM Identity Center ausgegebene Kontext-Assertion festgelegt wurde, wenn eine Rolle mit einem beliebigen AWS STS `assume-role` Befehl in der Operation AWS CLI oder AWS STS `AssumeRole` der API übernommen wird.
- Datentyp — Zeichenfolge
- Werttyp - Einzelwertig

Identitätsspeicher: IdentityStoreArn

Dieser Kontextschlüssel ist der ARN des Identitätsspeichers, der an die Instanz von IAM Identity Center angehängt ist, die die Kontext-Assertion ausgegeben hat. Es ist auch der Identitätsspeicher, in dem Sie nach Attributen suchen können. `identitystore:UserID` Sie können diesen Schlüssel in Richtlinien verwenden, um festzustellen, ob er von einem erwarteten Identitätsspeicher-ARN `identitystore:UserID` stammt.

- Verfügbarkeit — Dieser Schlüssel wird in den Anforderungskontext aufgenommen, nachdem eine vom IAM Identity Center ausgegebene Kontext-Assertion festgelegt wurde, wenn eine Rolle mit einem beliebigen AWS STS `assume-role` Befehl in der AWS CLI oder AWS STS `AssumeRole` API-Operation übernommen wird.
- Datentyp — Arn, String
- Werttyp - Einzelwertig

Identitätszentrum: ApplicationArn

Dieser Kontextschlüssel ist der ARN der Anwendung, für die IAM Identity Center eine Kontext-Assertion ausgegeben hat. Sie können diesen Schlüssel in Richtlinien verwenden, um festzustellen, ob er von einer erwarteten Anwendung `identitycenter:ApplicationArn` stammt. Mithilfe dieses Schlüssels kann verhindert werden, dass eine unerwartete Anwendung auf eine IAM-Rolle zugreift.

- Verfügbarkeit — Dieser Schlüssel ist im Anforderungskontext eines AWS STS `AssumeRole` API-Vorgangs enthalten. Der Anforderungskontext umfasst eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- Datentyp — Arn, Zeichenfolge
- Werttyp - Einzelwertig

Identitätszentrum: CredentialId

Dieser Kontextschlüssel ist eine zufällige ID für die Anmeldeinformationen der Rolle mit erweiterter Identität und wird nur für die Protokollierung verwendet. Da dieser Schlüsselwert nicht vorhersehbar ist, empfehlen wir, ihn nicht für Kontext-Assertionen in Richtlinien zu verwenden.

- Verfügbarkeit — Dieser Schlüssel ist im Anforderungskontext eines AWS STS `AssumeRole` API-Vorgangs enthalten. Der Anforderungskontext umfasst eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- Datentyp — Zeichenfolge
- Werttyp - Einzelwertig

Identitätszentrum: InstanceArn

Dieser Kontextschlüssel ist der ARN der Instanz von IAM Identity Center, die die Kontext-Assertion für ausgegeben hat. `identitystore:UserID` Sie können diesen Schlüssel verwenden, um festzustellen, ob die `identitystore:UserID` und kontextbezogene Assertion von einem erwarteten ARN der IAM Identity Center-Instanz stammt.

- Verfügbarkeit — Dieser Schlüssel ist im Anforderungskontext eines AWS STS `AssumeRole` API-Vorgangs enthalten. Der Anforderungskontext umfasst eine vom IAM Identity Center ausgegebene Kontext-Assertion.
- Datentyp — Arn, Zeichenfolge
- Werttyp - Einzelwertig

Protokollierung und Überwachung im IAM Identity Center

Als bewährte Methode sollten Sie Ihre Organisation überwachen, um sicherzustellen, dass Änderungen protokolliert werden. Auf diese Weise können Sie sicherstellen, dass alle unerwarteten Änderungen untersucht und unerwünschte Änderungen rückgängig gemacht werden können. AWS IAM Identity Center unterstützt derzeit zwei AWS Dienste, mit denen Sie Ihr Unternehmen und die darin stattfindenden Aktivitäten überwachen können.

Themen

- Protokollieren von IAM Identity Center-API-Aufrufen mit AWS CloudTrail
- Amazon EventBridge
- Protokollierung von AD-Synchronisierungs- und konfigurierbaren AD-Synchronisierungsfehlern

Protokollieren von IAM Identity Center-API-Aufrufen mit AWS CloudTrail

AWS IAM Identity Center ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in IAM Identity Center ausgeführt wurden. CloudTrail erfasst API-Aufrufe für IAM Identity Center als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der IAM Identity Center-Konsole und Code-Aufrufe an die IAM Identity Center-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für IAM Identity Center. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der

von CloudTrail gesammelten Informationen können Sie die Anfrage an das IAM Identity Center, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Themen

- Informationen zum IAM Identity Center finden Sie unter CloudTrail
- Grundlegendes zu den Einträgen in der IAM Identity Center-Protokolldatei
- Grundlegendes zu den Anmeldeereignissen im IAM Identity Center

Informationen zum IAM Identity Center finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im IAM Identity Center Aktivitäten auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für IAM Identity Center, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS -Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

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

Wenn die CloudTrail Protokollierung in Ihrem aktiviert ist AWS-Konto, werden API-Aufrufe an IAM Identity Center-Aktionen in Protokolldateien aufgezeichnet. IAM Identity Center-Datensätze werden zusammen mit anderen AWS Servicedatensätzen in einer Protokolldatei geschrieben. CloudTrail

bestimmt anhand eines Zeitraums und der Dateigröße, wann eine neue Datei erstellt und in diese geschrieben werden soll.

Die folgenden IAM Identity CloudTrail Center-Operationen werden unterstützt:

API-Operationen für die Konsole	Öffentliche API-Operationen
AssociateDirectory	AttachManagedPolicyToPermissionSet
AssociateProfile	CreateAccountAssignment
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus

API-Operationen für die Konsole	Öffentliche API-Operationen
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource

API-Operationen für die Konsole	Öffentliche API-Operationen
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Weitere Informationen zu den öffentlichen API-Vorgängen von IAM Identity Center finden Sie im IAM Identity Center API-Referenzhandbuch.

Die folgenden IAM Identity Center Identity CloudTrail Store-Operationen werden unterstützt:

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory
- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration

- `UpdateExternalIdPConfigurationForDirectory`
- `UpdateGroup`
- `UpdateMfaDeviceForUser`
- `UpdatePassword`
- `UpdateUser`
- `VerifyEmail`

Die folgenden IAM Identity Center CloudTrail OIDC-Aktionen werden unterstützt:

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

Die folgenden IAM Identity Center CloudTrail Portal-Aktionen werden unterstützt:

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

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

- Ob die Anfrage mit Root-Benutzer- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Grundlegendes zu den Einträgen in der IAM Identity Center-Protokolldatei

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

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für einen Administrator (samadams@example.com), der in der IAM Identity Center-Konsole stattgefunden hat:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
```

```
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für eine Endbenutzeraktion (bobsmith@example.com), die im AWS Zugriffsportal stattgefunden hat:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für eine Endbenutzeraktion (bobsmith@example.com), die im IAM Identity Center OIDC stattgefunden hat:

```
{
      "eventVersion": "1.05",
      "userIdentity": {
```

```
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```


Grundlegendes zu den Anmeldeereignissen im IAM Identity Center

AWS CloudTrail protokolliert erfolgreiche und erfolglose Anmeldeereignisse für alle AWS IAM Identity Center Identitätsquellen. Native SSO- und Active Directory-basierte Identitäten (AD Connector und AWS Managed Microsoft AD) beinhalten zusätzliche Anmeldeereignisse, die

jedes Mal erfasst werden, wenn ein Benutzer aufgefordert wird, eine bestimmte Anmeldeanfrage oder einen bestimmten Faktor zu lösen, sowie den Status dieser speziellen Anfrage zur Überprüfung der Anmeldeinformationen. Erst wenn ein Benutzer alle erforderlichen Anmeldedaten abgefragt hat, wird der Benutzer angemeldet, was dazu führt, dass ein Ereignis protokolliert wird. `UserAuthentication`

In der folgenden Tabelle sind die Namen der einzelnen IAM Identity CloudTrail Center-Anmeldeereignisse, ihr Zweck und ihre Anwendbarkeit auf verschiedene Identitätsquellen aufgeführt.

Ereignisname	Zweck des Ereignisses	Anwendbarkeit der Identitätsquelle
`CredentialChallenge`	Wird verwendet, um zu benachrichtigen, dass IAM Identity Center den Benutzer aufgefordert hat, eine bestimmte Anmeldeinformationsabfrage zu lösen, und gibt an `CredentialType`, welche erforderlich war (z. B. PASSWORD oder TOTP).	Systemeigene IAM Identity Center-Benutzer, AD Connector und AWS Managed Microsoft AD
`CredentialVerification`	Wird verwendet, um zu benachrichtigen, dass der Benutzer versucht hat, eine bestimmte `CredentialChallenge` Anfrage zu lösen, und gibt an, ob diese Anmeldeinformationen erfolgreich waren oder nicht.	Systemeigene IAM Identity Center-Benutzer, AD Connector und AWS Managed Microsoft AD
`UserAuthentication`	Wird verwendet, um zu benachrichtigen, dass alle Authentifizierungsanforderungen, mit denen der Benutzer konfrontiert wurde, erfolgreich erfüllt wurden und dass	Alle Identitätsquellen

Ereignisname	Zweck des Ereignisses	Anwendbarkeit der Identitätsquelle
	der Benutzer erfolgreich angemeldet wurde. Wenn Benutzer die erforderlichen Anmeldedaten nicht erfolgreich abschließen, wird kein *UserAuthentication* Ereignis protokolliert.	

In der folgenden Tabelle werden zusätzliche nützliche Ereignisdatenfelder erfasst, die in bestimmten CloudTrail Anmeldeereignissen enthalten sind.

Ereignisname	Zweck des Ereignisses	Anwendbarkeit des Anmeldeereignisses	Beispielwerte
`AuthWorkflowID`	Wird verwendet, um alle Ereignisse zu korrelieren, die während einer gesamten Anmeldesequenz ausgelöst wurden. Für jede Benutzeranmeldung können mehrere Ereignisse vom IAM Identity Center ausgelöst werden.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	„AuthWorkflowID“: „9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Wird verwendet, um den Berechtigungsnachweis oder den Faktor anzugeben, der angefochten	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType„: „PASSWORD“ oder "CredentialType„: „PASSWORD, TOTP“ (mögliche Werte sind: PASSWORD,

Ereignisname	Zweck des Ereignisses	Anwendbarkeit des Anmeldeereignisses	Beispielwerte
	wurde. `UserAuthentication` Ereignisse umfassen alle `CredentialType` Werte, die in der Anmeldesequenz des Benutzers erfolgreich verifiziert wurden.		TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP)
`DeviceEnrollmentRequired`	Wird verwendet, um anzugeben, dass der Benutzer bei der Anmeldung ein MFA-Gerät registrieren musste und dass der Benutzer diese Anfrage erfolgreich abgeschlossen hat.	`UserAuthentication`	"DeviceEnrollmentRequired„: „wahr“
`LoginTo`	Wird verwendet, um den Umleitungsort nach einer erfolgreichen Anmeldesequenz anzugeben.	`UserAuthentication`	"LoginTo„:" https://mydirectory.awsapps.com/start/...“

Beispielereignisse für IAM Identity Center-Anmeldeszenarien

Die folgenden Beispiele zeigen die erwartete Reihenfolge von CloudTrail Ereignissen für verschiedene Anmeldeszenarien.

Themen

- Erfolgreiche Anmeldung bei Authentifizierung nur mit einem Passwort
- Erfolgreiche Anmeldung bei der Authentifizierung mit einem externen Identitätsanbieter

- Erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer TOTP-Authentifikator-App
- Eine erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer erzwungenen MFA-Registrierung ist erforderlich
- Fehlgeschlagene Anmeldung bei der Authentifizierung nur mit einem Passwort

Erfolgreiche Anmeldung bei Authentifizierung nur mit einem Passwort

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Anmeldung nur mit Passwort.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
```

```
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Erfolgreich CredentialVerification (Passwort)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Erfolgreich UserAuthentication (nur Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

Erfolgreiche Anmeldung bei der Authentifizierung mit einem externen Identitätsanbieter

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Anmeldung, wenn sie über das SAML-Protokoll mit einem externen Identitätsanbieter authentifiziert wurde.

Erfolgreich UserAuthentication (externer Identitätsanbieter)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
```

```
}
```

Erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer TOTP-Authentifikator-App

Die folgende Abfolge von Ereignissen zeigt ein Beispiel, bei dem bei der Anmeldung eine Multi-Faktor-Authentifizierung erforderlich war und sich der Benutzer erfolgreich mit einem Passwort und einer TOTP-Authentifikator-App angemeldet hat.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
```

```
   }
}
```

Erfolgreich CredentialVerification (Passwort)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

CredentialChallenge (TOTP)

```
{
```

```
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Erfolgreich CredentialVerification (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
```

```
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


Erfolgreich UserAuthentication (Passwort + TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
```

```
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Eine erfolgreiche Anmeldung bei der Authentifizierung mit einem Passwort und einer erzwungenen MFA-Registrierung ist erforderlich

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine erfolgreiche Kennwortanmeldung, aber der Benutzer musste ein MFA-Gerät registrieren und hat die Registrierung erfolgreich abgeschlossen, bevor er seine Anmeldung abgeschlossen hat.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
```

```
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Erfolgreich CredentialVerification (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
```

```
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


Erfolgreich UserAuthentication (Passwort + MFA-Registrierung erforderlich)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
```

```
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Fehlgeschlagene Anmeldung bei der Authentifizierung nur mit einem Passwort

Die folgende Abfolge von Ereignissen zeigt ein Beispiel für eine fehlgeschlagene Anmeldung nur mit Passwort.

CredentialChallenge (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
```

```
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


CredentialVerification Fehlgeschlagen (Passwort)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
```

```
    "awsRegion":"us-east-1",
    "sourceIPAddress":"203.0.113.0",
    "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
    "requestParameters":null,
    "responseElements":null,
    "additionalEventData":{
       "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
       "CredentialType":"PASSWORD"
    },
    "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
    "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
       "CredentialVerification":"Failure"
    }
}
```

Amazon EventBridge

IAM Identity Center kann mit Amazon zusammenarbeiten EventBridge , um Ereignisse auszulösen, wenn vom Administrator festgelegte Aktionen in einer Organisation stattfinden. Zum Beispiel möchten die meisten Administratoren, aufgrund der Vertraulichkeit solcher Aktionen, gewarnt werden, sobald jemand ein neues Konto in der Organisation erstellt oder wenn der Administrator eines Mitgliedskontos versucht, die Organisation zu verlassen. Sie können EventBridge Regeln konfigurieren, die nach diesen Aktionen suchen und die generierten Ereignisse dann an vom Administrator definierte Ziele senden. Ziele können ein Amazon-SNS-Thema sein, das E-Mails oder SMS-Nachrichten an Abonnenten verwendet. Sie könnten auch eine AWS Lambda Funktion erstellen, die die Details der Aktion für Ihre spätere Überprüfung protokolliert.

Weitere Informationen darüber EventBridge, einschließlich der Konfiguration und Aktivierung, finden Sie im EventBridge Amazon-Benutzerhandbuch.

Protokollierung von AD-Synchronisierungs- und konfigurierbaren AD-Synchronisierungsfehlern

Sie können die Protokollierung Ihrer Active Directory-Synchronisierung (AD) und konfigurierbare AD-Synchronisierungskonfigurationen aktivieren, um Protokolle mit Informationen zu Fehlern zu erhalten, die während des Synchronisierungsvorgangs auftreten können. Mit diesen Protokollen können Sie überwachen, ob ein Problem mit Ihrer AD-Synchronisierung und der konfigurierbaren AD-Synchronisierung vorliegt, und gegebenenfalls Maßnahmen ergreifen. Sie können Ihre Protokolle an eine Amazon CloudWatch Logs-Protokollgruppe, einen Amazon Simple Storage Service (Amazon S3) -Bucket oder eine Amazon Data Firehose senden, wobei die kontoübergreifende Zustellung für Amazon S3-Buckets und Firehose unterstützt wird.

Weitere Informationen zu Einschränkungen, Berechtigungen und versendeten Protokollen finden Sie unter Aktivieren der Protokollierung von. AWS-Services

> **Note**
>
> Die Protokollierung wird Ihnen in Rechnung gestellt. Weitere Informationen finden Sie unter Vending Logs auf der Seite mit den CloudWatch Amazon-Preisen.

Um AD-Synchronisierung und konfigurierbare AD-Sync-Fehlerprotokolle zu aktivieren

1. Melden Sie sich bei der IAM Identity Center-Konsole an.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, dann Aktionen und anschließend Protokolle verwalten aus.
4. Wählen Sie „Protokollzustellung hinzufügen“ und einen der folgenden Zieltypen aus.
    a. Wählen Sie To Amazon CloudWatch Logs. Wählen Sie dann die Zielprotokollgruppe aus oder geben Sie sie ein.
    b. Wählen Sie Zu Amazon S3. Wählen Sie dann den Ziel-Bucket aus oder geben Sie ihn ein.
    c. Wählen Sie To Firehose. Wählen Sie dann den Ziel-Lieferstream aus oder geben Sie ihn ein.
5. Wählen Sie Absenden aus.

Um die AD-Synchronisierung und die konfigurierbaren AD-Synchronisierungsfehlerprotokolle zu deaktivieren

1. Melden Sie sich bei der IAM Identity Center-Konsole an.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie auf der Seite Einstellungen die Registerkarte Identitätsquelle, dann Aktionen und anschließend Protokolle verwalten aus.
4. Wählen Sie Entfernen für das Ziel, das Sie entfernen möchten.
5. Wählen Sie Absenden aus.

AD-Synchronisierung und konfigurierbare Protokollfelder für AD-Synchronisierungsfehler

In der folgenden Liste finden Sie mögliche Fehlerprotokollfelder.

`sync_profile_name`

Der Name des Synchronisierungsprofils.

`error_code`

Der Fehlercode, der angibt, welche Art von Fehler aufgetreten ist.

`error_message`

Eine Meldung, die detaillierte Informationen über den aufgetretenen Fehler enthält.

`sync_source`

Die Synchronisierungsquelle ist der Ort, von dem aus Entitäten synchronisiert werden. Für IAM Identity Center ist dies ein Active Directory (AD), das von verwaltet wird. AWS Directory Service Die Synchronisierungsquelle enthält die Domain und den ARN des betroffenen Verzeichnisses.

`sync_target`

Das Synchronisierungsziel ist das Ziel, an dem Entitäten gespeichert werden. Für IAM Identity Center ist dies ein Identity Store. Das Synchronisierungsziel enthält den betroffenen Identity Store-ARN.

`source_entity_id`

Eine eindeutige Kennung für die Entität, die den Fehler verursacht. Für IAM Identity Center ist dies die SID der Entität.

`source_entity_type`

Der Typ der Entität, die den Fehler verursacht hat. Dabei kann es sich um den Wert `USER` oder `GROUP` handeln.

`eventTimestamp`

Der Zeitstempel, zu dem der Fehler aufgetreten ist.

Beispiele für AD-Synchronisierung und konfigurierbare AD-Synchronisierungsfehlerprotokolle

Beispiel 1: Ein Fehlerprotokoll für ein abgelaufenes Passwort für ein AD-Verzeichnis

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

Beispiel 2: Ein Fehlerprotokoll für einen Benutzer mit einem nicht eindeutigen Benutzernamen

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "sync_target": {
```

```
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

Konformitätsprüfung für IAM Identity Center

Externe Prüfer bewerten die Sicherheit und Konformität von AWS-Services z. AWS IAM Identity Center B. im Rahmen mehrerer AWS Compliance-Programme.

Um zu erfahren, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

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

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

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

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

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.

- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Unterstützte Compliance-Standards

IAM Identity Center wurde nach den folgenden Standards geprüft und kann als Teil von Lösungen verwendet werden, für die Sie eine Konformitätszertifizierung benötigen.

AWS hat sein Compliance-Programm nach dem Health Insurance Portability and Accountability Act (HIPAA) um das IAM Identity Center als HIPAA-fähigen Service erweitert.

AWS bietet ein Whitepaper mit Fokus auf HIPAA für Kunden, die mehr darüber erfahren möchten, wie sie Gesundheitsinformationen verarbeiten und speichern können. AWS-Services Weitere Informationen finden Sie unter HIPAA-Compliance.

Das Information Security Registered Assessors Program (IRAP) ermöglicht es australischen Regierungskunden, sicherzustellen, dass angemessene Compliance-Kontrollen vorhanden sind, und das geeignete Verantwortungsmodell für die Erfüllung der Anforderungen des vom Australian Cyber Security Centre (ACSC) herausgegebenen Informationssicherheitshandbuch (ISM) der australischen Regierung festzulegen. Weitere Informationen finden Sie unter IRAP Resources.

Das IAM Identity Center verfügt über eine Konformitätsbescheinigung für den Payment Card Industry (PCI) Data Security Standard (DSS) Version 3.2 auf Service Provider Level 1.

Kunden, die AWS Produkte und Dienste zur Speicherung, Verarbeitung oder Übertragung von Karteninhaberdaten verwenden, können die folgenden Identitätsquellen in IAM Identity Center verwenden, um ihre eigene PCI-DSS-Konformitätszertifizierung zu verwalten:

- Active Directory
- Externer Identitätsanbieter

Die IAM Identity Center-Identitätsquelle ist derzeit nicht mit PCI DSS kompatibel.

	Weitere Informationen zu PCI DSS, einschließlich der Möglichkeit, eine Kopie des AWS PCI Compliance Package anzufordern, finden Sie unter PCI DSS Level 1.
	Bei den SOC-Berichten (System & Organization Control) handelt es sich um unabhängige Prüfungsberichte von Drittanbietern, die belegen, wie IAM Identity Center wichtige Compliance-Kontrollen und -Ziele erreicht. Diese Berichte helfen Ihnen und Ihren Prüfern zu verstehen, wie Kontrollen den Betrieb und die Einhaltung von Vorschriften unterstützen. Es gibt drei Arten von SOC-Berichten: • AWS SOC 1-Bericht — Mit AWS Artifact herunterladen • AWS SOC 2: Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit — Mit AWS Artifact herunterladen • AWS SOC 3: Bericht zu Sicherheit, Verfügbarkeit und Vertraulichkeit IAM Identity Center ist für AWS SOC 1-, SOC 2- und SOC 3-Berichte vorgesehen. Weitere Informationen finden Sie unter SOC-Compliance.

Ausfallsicherheit im IAM Identity Center

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Weitere Informationen zur AWS IAM Identity Center Ausfallsicherheit finden Sie unterResilienzdesign und regionales Verhalten.

Infrastruktursicherheit im IAM Identity Center

Als verwalteter Dienst AWS IAM Identity Center ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf IAM Identity Center zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Markieren von AWS IAM Identity Center-Ressourcen

Ein Tag ist eine benutzerdefinierte Attributskennzeichnung, die Sie zu einer AWS-Ressource hinzufügen, damit sich Ressourcen einfacher identifizieren, organisieren und finden lassen. Jedes Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Tag-Schlüssel können bis zu 128 Zeichen lang sein und berücksichtigen die Groß-/Kleinschreibung.
- Einem Tag-Wert (z. B. `111122223333` oder `Production`). Tag-Werte können bis zu 256 Zeichen lang sein und wie bei Tag-Schlüsseln muss die Groß-/Kleinschreibung beachtet werden. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht Null festlegen. Ein nicht angegebener Tag-Wert entspricht einer leeren Zeichenfolge.

Tags helfen Ihnen, Ihre AWS-Ressourcen zu identifizieren und zu organisieren. Viele AWS-Services unterstützen das Markieren mit Tags (kurz: Tagging). So können Ressourcen aus verschiedenen Services dasselbe Tag zuweisen, um anzugeben, dass die Ressourcen verbunden sind. Sie können dasselbe Tag beispielsweise einem bestimmten Berechtigungssatz in Ihrer IAM Identity Center-Instanz zuweisen. Weitere Informationen zu Tagging-Strategien finden Sie unter Tagging AWS Resources im Allgemeine AWS-ReferenzGuide und Best Practices für Tagging.

Neben der Identifizierung, Organisation und Nachverfolgung Ihrer AWS Ressourcen mithilfe von Tags können Sie mithilfe von Tags in IAM-Richtlinien steuern, wer Ihre Ressourcen einsehen und mit ihnen interagieren kann. Weitere Informationen zur Verwendung von Tags zur Zugriffskontrolle finden Sie im IAM-Benutzerhandbuch unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags. Sie können einem Benutzer beispielsweise erlauben, einen IAM Identity Center-Berechtigungssatz zu aktualisieren, aber nur, wenn der IAM Identity Center-Berechtigungssatz ein `owner` Tag mit dem Wert des Benutzernamens enthält.

Derzeit können Sie Tags nur auf Berechtigungssätze anwenden. Sie können keine Tags auf die entsprechenden Rollen anwenden, in AWS-Konten denen IAM Identity Center erstellt. Sie können die IAM Identity Center-Konsole AWS CLI oder die IAM Identity Center-APIs verwenden, um Tags für einen Berechtigungssatz hinzuzufügen, zu bearbeiten oder zu löschen.

In den folgenden Abschnitten finden Sie weitere Informationen zu Tags für IAM Identity Center.

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags auf IAM Identity Center-Ressourcen:

- Die maximale Anzahl von Tags, die Sie einer Ressource zuweisen können, beträgt 50.
- Die maximale Schlüssellänge beträgt 128 Unicode-Zeichen.
- Die maximale Wertlänge beträgt 256 Unicode-Zeichen.
- Gültige Zeichen für einen Tag-Schlüssel und -Wert sind:

  a-z, A-Z, 0-9, Leerzeichen und die folgenden Zeichen: _.:/= + - und @
- Bei Schlüsseln und Werten wird die Groß-/Kleinschreibung berücksichtigt.
- Verwenden Sie nicht `aws:` als Präfix für Schlüssel. Dieses Präfix ist für AWS reserviert.

Verwalten Sie Tags mithilfe der IAM Identity Center-Konsole

Sie können die IAM Identity Center-Konsole verwenden, um Tags hinzuzufügen, zu bearbeiten und zu entfernen, die Ihrer Instanz oder Ihren Berechtigungssätzen zugeordnet sind.

Um Berechtigungssätze und Tags für eine IAM Identity Center-Konsole zu verwalten

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Berechtigungssätze aus.
3. Wählen Sie den Namen des Berechtigungssatzes, der die Tags enthält, die Sie verwalten möchten.
4. Führen Sie auf der Registerkarte Berechtigungen unter Tags eine der folgenden Aktionen aus, und fahren Sie dann mit dem nächsten Schritt fort:

   a. Wenn diesem Berechtigungssatz bereits Tags zugewiesen wurden, wählen Sie Tags bearbeiten aus.

   b. Wenn diesem Berechtigungssatz keine Tags zugewiesen sind, wählen Sie Tags hinzufügen aus.
5. Geben Sie für jedes neue Tag die Werte in die Spalten Schlüssel und Wert (optional) ein. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

Um ein Tag zu entfernen, wählen Sie das X in der Spalte Entfernen neben dem Tag, das Sie entfernen möchten.

Um Tags für eine Instanz von IAM Identity Center zu verwalten

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie Settings (Einstellungen) aus.
3. Wählen Sie die Registerkarte Tags aus.
4. Geben Sie für jedes Tag die Werte in die Felder Schlüssel und Wert (optional) ein. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche Neues Tag hinzufügen.

Um ein Tag zu entfernen, klicken Sie auf die Schaltfläche Entfernen neben dem Tag, das Sie entfernen möchten.

Beispiele für AWS CLI

Das AWS CLI enthält Befehle, mit denen Sie die Tags verwalten können, die Sie Ihrem Berechtigungssatz zuweisen.

Zuweisen von Tags

Verwenden Sie die folgenden Befehle, um Ihrem Berechtigungssatz Tags zuzuweisen.

Example **`tag-resource`**Befehl für einen Berechtigungssatz

Weisen Sie einem Berechtigungssatz Tags zu, indem Sie `tag-resource`innerhalb des `sso` Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Dieser Befehl enthält die folgenden Parameter:

- `instance-arn`— Der Amazon-Ressourcenname (ARN) der IAM Identity Center-Instance, unter der der Vorgang ausgeführt wird.

- `resource-arn`— Der ARN der Ressource mit den aufgelisteten Tags.
- `tags` – Die Schlüssel-Wert-Paare der Tags.

Wenn Sie mehrere Tags auf einmal zuweisen möchten, geben Sie sie in eine durch Kommata getrennte Liste ein:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Anzeigen von Tags

Verwenden Sie die folgenden Befehle, um die Tags anzuzeigen, die Sie Ihrem Berechtigungssatz zugewiesen haben.

Example **`list-tags-for-resource`**Befehl für einen Berechtigungssatz

Zeigen Sie die Tags an, die einem Berechtigungssatz zugewiesen sind, indem Sie `list-tags-for-resource`innerhalb des `sso` Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Entfernen von Tags

Verwenden Sie die folgenden Befehle, um Tags aus einem Berechtigungssatz zu entfernen.

Example **`untag-resource`**Befehl für einen Berechtigungssatz

Entfernen Sie Tags aus einem Berechtigungssatz, indem Sie `untag-resource`innerhalb des `sso` Befehlssatzes Folgendes verwenden:

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Geben Sie für den `--tag-keys`-Parameter einen oder mehrere Tag-Schlüssel ohne Tag-Werte an.

Anwenden von Tags beim Erstellen eines Berechtigungssatzes

Verwenden Sie die folgenden Befehle, um Tags zuzuweisen, sobald Sie einen Berechtigungssatz erstellen.

Example **`create-permission-set`**-Befehl mit Tags

Wenn Sie mithilfe des `create-permission-set`Befehls einen Berechtigungssatz erstellen, können Sie Tags mit dem `--tags` Parameter angeben:

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Tags mithilfe der IAM Identity Center-API verwalten

Sie können die folgenden Aktionen in der IAM Identity Center-API verwenden, um die Tags für Ihren Berechtigungssatz zu verwalten.

API-Aktionen für IAM Identity Center-Instanz-Tags

Verwenden Sie die folgenden API-Aktionen, um Tags für einen Berechtigungssatz oder eine Instanz von IAM Identity Center zuzuweisen, anzuzeigen und zu entfernen.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

Integration vonAWSCLI mit IAM Identity Center

AWSDie Integration der Befehlszeilenschnittstelle (CLI) Version 2 in IAM Identity Center vereinfacht den Anmeldevorgang. Entwickler können sich direkt bei derAWS CLImit denselben Active Directory- oder IAM Identity Center-Anmeldeinformationen, die sie normalerweise verwenden, um sich bei IAM Identity Center anzumelden und auf die ihnen zugewiesenen Konten und Rollen zuzugreifen. Nachdem ein Administrator beispielsweise IAM Identity Center für die Verwendung von Active Directory für die Authentifizierung konfiguriert hat, kann sich ein Entwickler bei derAWS CLIdirekt mit ihren Active Directory-Anmeldeinformationen.

AWSDie CLI-Integration mit IAM Identity Center bietet die folgenden Vorteile:

- Unternehmen können ihren Entwicklern ermöglichen, sich mit Anmeldeinformationen von IAM Identity Center oder Active Directory anzumelden, indem sie IAM Identity Center überAWS Directory Serviceaus.
- Entwickler können sich für einen schnelleren Zugriff über die CLI anmelden.
- Entwickler können Konten und Rollen auflisten und zwischen ihnen wechseln, denen sie Zugriff zugewiesen haben.
- Entwickler können benannte Rollenprofile in ihrer CLI-Konfiguration automatisch generieren und speichern und sie in der CLI referenzieren, um Befehle in den gewünschten Konten und Rollen auszuführen.
- Die CLI verwaltet kurzfristige Anmeldeinformationen automatisch, sodass Entwickler sicher und ohne Unterbrechung in der CLI starten und dort bleiben und lang laufende Skripts ausführen können.

Funktionsweise der -IntegrationAWSCLI mit IAM Identity Center

So verwenden Sie denAWSCLI-Integration mit IAM Identity Center, Sie müssen herunterladen, installieren und konfigurierenAWS Command Line InterfaceVersion 2 Detaillierte Anweisungen zum Herunterladen und -Integrieren derAWS CLImit IAM Identity Center finden Sie unterKonfigurieren vonAWSCLI zur Verwendung von IAM Identity CenterimAWS Command Line InterfaceBenutzerhandbuchaus.

AWS IAM Identity Center Verfügbarkeit in der Region

IAM Identity Center ist in verschiedenen gängigen AWS-Regionen Versionen verfügbar. Diese Verfügbarkeit erleichtert Ihnen die Konfiguration des Benutzerzugriffs auf mehrere AWS-Konten Geschäftsanwendungen. Wenn sich Ihre Benutzer beim AWS Zugriffsportal anmelden, können sie auswählen, AWS-Konto für welche sie berechtigt sind, und dann auf das zugreifen AWS Management Console. Eine vollständige Liste der AWS-Regionen von IAM Identity Center unterstützten Geräte finden Sie unter IAM Identity Center-Endpunkte und Kontingente.

Daten zur IAM Identity Center-Region

Wenn Sie IAM Identity Center zum ersten Mal aktivieren, werden alle Daten, die Sie in IAM Identity Center konfigurieren, in der Region gespeichert, in der Sie sie konfiguriert haben. Zu diesen Daten gehören Verzeichniskonfigurationen, Berechtigungssätze, Anwendungsinstanzen und Benutzerzuweisungen zu AWS-Konto Anwendungen. Wenn Sie den IAM Identity Center-Identitätsspeicher verwenden, werden alle Benutzer und Gruppen, die Sie in IAM Identity Center erstellen, ebenfalls in derselben Region gespeichert. Wir empfehlen, IAM Identity Center in einer Region zu installieren, die Sie für Benutzer verfügbar halten möchten, und nicht in einer Region, die Sie möglicherweise deaktivieren müssen.

AWS Organizations unterstützt AWS-Region jeweils nur eine. Um IAM Identity Center in einer anderen Region zu aktivieren, müssen Sie zuerst Ihre aktuelle IAM Identity Center-Konfiguration löschen. Wenn Sie zu einer anderen Region wechseln, ändert sich auch die URL für das AWS Zugriffsportal, und Sie müssen alle Berechtigungssätze und Zuweisungen neu konfigurieren.

Regionsübergreifende Anrufe

IAM Identity Center verwendet Amazon Simple Email Service (Amazon SES), um E-Mails an Endbenutzer zu senden, wenn diese versuchen, sich mit einem Einmalpasswort (OTP) als zweitem Authentifizierungsfaktor anzumelden. Diese E-Mails werden auch für bestimmte Ereignisse zur Identitäts- und Anmeldeinformationsverwaltung gesendet, z. B. wenn der Benutzer aufgefordert wird, ein erstes Passwort einzurichten, eine E-Mail-Adresse zu verifizieren und sein Passwort zurückzusetzen. Amazon SES ist in einer Teilmenge der von AWS-Regionen IAM Identity Center unterstützten Optionen verfügbar.

IAM Identity Center ruft lokale Amazon SES-Endpunkte auf, wenn Amazon SES lokal in einem verfügbar ist. AWS-Region Wenn Amazon SES nicht lokal verfügbar ist, ruft IAM Identity Center

Amazon SES SES-Endpunkte auf einem anderen Weg auf AWS-Region, wie in der folgenden Tabelle angegeben.

Die Amazon SES SES-Regionscodes sind in der folgenden Tabelle aufgeführt.

Regionalcode für das IAM Identity Center	Name der Region für das IAM Identity Center	Amazon SES SES-Regionalcode	Name der Amazon SES SES-Region
us-gov-east-1	AWS GovCloud (USA-Ost)	us-gov-west-1	AWS GovCloud (US-West)
ap-east-1	Asien-Pazifik (Hongkong)	ap-northeast-2	Asien-Pazifik (Seoul)
ap-southeast-4	Asien-Pazifik (Melbourne)	ap-southeast-2	Asien-Pazifik (Sydney)
ap-south-2	Asien-Pazifik (Hyderabad)	ap-south-1	Asien-Pazifik (Mumbai)
eu-central-2	Europa (Zürich)	eu-central-1	Europa (Frankfurt)
eu-south-2	Europa (Spain)	eu-west-3	Europa (Paris)
me-central-1	Naher Osten (VAE)	eu-central-1	Europa (Frankfurt)

Bei diesen regionsübergreifenden Aufrufen sendet IAM Identity Center möglicherweise die folgenden Benutzerattribute:

- E-Mail-Adresse
- Vorname
- Nachname
- Konto in AWS Organizations
- AWS Portal-URL aufrufen
- Username
- Verzeichnis-ID

- Benutzer-ID

Verwaltung des IAM Identity Center in einer Opt-in-Region (Region, die standardmäßig deaktiviert ist)

Die meisten AWS-Regionen sind standardmäßig für den Betrieb in allen AWS Diensten aktiviert. Diese Regionen werden automatisch für die Verwendung mit IAM Identity Center aktiviert. Bei den folgenden Regionen AWS-Regionen handelt es sich um Opt-in-Regionen, die Sie aktivieren müssen:

- Afrika (Kapstadt)
- Asia Pacific (Hongkong)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Hyderabad)
- Europa (Milan)
- Europa (Zürich)
- Europa (Spain)
- Israel (Tel Aviv)
- Naher Osten (Bahrain)
- Naher Osten (VAE)

Wenn Sie IAM Identity Center für ein Verwaltungskonto in einem Opt-In aktivieren AWS-Region, werden die folgenden IAM Identity Center-Metadaten für alle Mitgliedskonten in der Region gespeichert.

- Konto-ID
- Account name (Kontoname)
- Konto-E-Mail
- Amazon-Ressourcennamen (ARNs) der IAM-Rollen, die IAM Identity Center im Mitgliedskonto erstellt

Wenn Sie eine Region deaktivieren, in der IAM Identity Center installiert ist, wird IAM Identity Center ebenfalls deaktiviert. Nachdem IAM Identity Center in einer Region deaktiviert wurde, haben

Benutzer in dieser Region keinen Single Sign-On-Zugriff auf Anwendungen. AWS-Konten AWS bewahrt die Daten in Ihrer IAM Identity Center-Konfiguration für mindestens 10 Tage auf. Wenn Sie IAM Identity Center innerhalb dieses Zeitraums erneut aktivieren, sind Ihre IAM Identity Center-Konfigurationsdaten weiterhin in der Region verfügbar.

Um IAM Identity Center im Opt-In wieder zu aktivieren AWS-Regionen, müssen Sie die Region erneut aktivieren. Da IAM Identity Center alle unterbrochenen Ereignisse erneut verarbeiten muss, kann die erneute Aktivierung von IAM Identity Center einige Zeit dauern.

> **Note**
>
> IAM Identity Center kann nur den Zugriff auf diejenigen verwalten, die für AWS-Konten die Verwendung in einem aktiviert sind. AWS-Region Um den Zugriff für alle Konten in Ihrer Organisation zu verwalten, aktivieren Sie IAM Identity Center im Verwaltungskonto eines Kontos, das automatisch für AWS-Region die Verwendung mit IAM Identity Center aktiviert wird.

Weitere Informationen zur Aktivierung und Deaktivierung AWS-Regionen finden Sie AWS-Regionen in der AWS allgemeinen Referenz unter Verwaltung.

Löschen Sie Ihre IAM Identity Center-Konfiguration

Wenn eine IAM Identity Center-Konfiguration gelöscht wird, werden alle Daten in dieser Konfiguration gelöscht und können nicht wiederhergestellt werden. In der folgenden Tabelle wird beschrieben, welche Daten basierend auf dem Verzeichnistyp gelöscht werden, der derzeit in IAM Identity Center konfiguriert ist.

Welche Daten werden gelöscht	Verbundenes Verzeichnis (AWS Managed Microsoft AD oder AD Connector)	IAM Identity Center-Identitätsspeicher
Alle Berechtigungssätze, für die Sie konfiguriert haben AWS-Konten	✓	✓

Welche Daten werden gelöscht	Verbundenes Verzeichnis (AWS Managed Microsoft AD oder AD Connector)	IAM Identity Center-Identitätsspeicher
Alle Anwendungen, die Sie in IAM Identity Center konfiguriert haben	✓	✓
Alle Benutzerzuweisungen, für die Sie konfiguriert haben, AWS-Konten und alle Anwendungen	✓	✓
Alle Benutzer und Gruppen im Verzeichnis oder Speicher	N/A	✓

Gehen Sie wie folgt vor, wenn Sie Ihre aktuelle IAM Identity Center-Konfiguration löschen müssen.

Um Ihre IAM Identity Center-Konfiguration zu löschen

1. Öffnen Sie die IAM Identity Center-Konsole.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Seite „Einstellungen“ die Registerkarte „Verwaltung“.
4. Wählen Sie im Abschnitt „IAM Identity Center-Konfiguration löschen“ die Option Löschen aus.
5. Aktivieren Sie im Dialogfeld „IAM Identity Center-Konfiguration löschen“ jedes der Kontrollkästchen, um zu bestätigen, dass Sie damit einverstanden sind, dass Ihre Daten gelöscht werden. Geben Sie Ihre IAM Identity Center-Instanz in das Textfeld ein und wählen Sie dann Bestätigen aus.

AWS IAM Identity Center -Kontingente

In den folgenden Tabellen werden die Kontingente in IAM Identity Center beschrieben. Anfragen zur Erhöhung des Kontingents müssen von einem Verwaltungs- oder delegierten Administratorkonto stammen. Informationen zum Erhöhen eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung.

> **Note**
>
> Wir empfehlen die Verwendung der AWS CLI und APIs, APIs wenn Sie mehr als 50.000 Benutzer, 10.000 Gruppen oder 500 Berechtigungssätze haben. Weitere Informationen zur CLI finden Sie unter Integration vonAWSCLI mit IAM Identity Center. Weitere Informationen zu APIs finden Sie unterWillkommen in der API-Referenz zu IAM Identity Center.

Anwendungskontingente

Ressource	Standardkontingent	Kann erhöht werden
Dateigröße der SAML-Zertifikate vom Service-Anbieter (im PEM-Format)	2 KB	Nein
SAML-Assertion-Limit	50 000 Zeichen	Nein
Dateigrößenbeschränkung des in IAM Identity Center hochgeladenen IdP	2 500 (UTF-8) Zeichen	Nein
Zugriffsbereiche pro Anwendung	25	Nein

AWS-Konto -Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl der in IAM Identity Center zulässigen Berechtigungssätze	2000	Ja
Anzahl der zulässigen bereitgestellten Berechtigungssätze pro AWS-Konto	250	Ja
Anzahl der eingebundenen Richtlinien pro Berechtigungssatz	1	Nein
Anzahl der AWS von verwalteten und vom Kunden verwalteten Richtlinien pro Berechtigungssatz	20[1]	Nein
Maximale Größe der eingebundenen Richtlinie pro Berechtigungssatz	32 768 Byte. Die maximale Größe von Zeichen, die keine Leerzeichen sind, in der Inline-Richtlinie pro Berechtigungssatz beträgt 10.240 Byte.	Nein
Anzahl der IAM-Rollen (Berechtigungssätze) in der AWS-Konto , die gleichzeitig aktualisiert werden können	1	Nein

[1]AWS Identity and Access Management (IAM) legt ein Kontingent von 10 verwalteten Richtlinien pro Rolle fest. Um dieses Kontingent zu nutzen, fordern Sie eine Erhöhung der verwalteten

IAM-Kontingentrichtlinien an, die einer IAM-Rolle in der Service-Quotas-Konsole für jede an, AWS-Konto in der Sie den Berechtigungssatz bereitstellen möchten. Service Quotas

> **Note**
>
> Berechtigungssätze werden in AWS-Konten als IAM-Rollen bereitgestellt oder verwenden vorhandene IAM-Rollen in AWS-Kontenund befolgen daher IAM-Kontingente. Weitere Informationen zu Kontingenten, die IAM-Rollen zugeordnet sind, finden Sie unter IAM- und STS-Kontingente.

Active-Directory-Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl der gleichzeitig möglichen verbundenen Verzeichnisse	1	Nein

IAM Identity Center-Identitätsspeicher-Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Anzahl unterstützter Benutzer in IAM Identity Center	100000	Ja
Anzahl unterstützter Gruppen in IAM Identity Center	100000	Nein
Anzahl der eindeutigen Gruppen, die zum Auswerten der Berechtigungen für einen Benutzer verwendet werden können	1000	Nein

Drossel-Limits für IAM Identity Center

Ressource	Standardkontingent
IAM-Identity-Center-APIs	IAM-Identity-Center-APIs haben ein kollektiv es Drosselungsmaximum von 20 Transakti onen pro Sekunde (TPS). Die CreateAcc ountAssignment hat eine maximale Rate von 10 ausstehenden asynchronen Aufrufen. Diese Kontingente können nicht geändert werden.

Zusätzliche Kontingente

Ressource	Standardkontingent	Kann erhöht werden
Gesamtzahl der - AWS-Konte n oder -Anwendungen, die konfiguriert werden können*	3000	Ja
Gesamtzahl der Instances von IAM Identity Center pro Konto	1	Nein
Gesamtzahl der vertrauen swürdigen Token-Aussteller	10	Nein

* Es werden bis zu 3 000 AWS-Konten Anwendungen (zusammen) unterstützt. Sie können beispielsweise 2 750 Konten und 250 Anwendungen konfigurieren, was insgesamt 3 000 Konten und Anwendungen ergibt.

Behebung von Problemen mit IAM Identity Center

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Einrichtung oder Verwendung der IAM Identity Center-Konsole auftreten können.

Probleme beim Erstellen einer Kontoinstanz von IAM Identity Center

Bei der Erstellung einer Kontoinstanz von IAM Identity Center können mehrere Einschränkungen gelten. Wenn Sie keine Kontoinstanz über die IAM Identity Center-Konsole oder die Einrichtung einer unterstützten AWS verwalteten Anwendung erstellen können, überprüfen Sie die folgenden Anwendungsfälle:

- Klicken Sie AWS-Regionen in der Instanz, AWS-Konto in der Sie versuchen, die Kontoinstanz zu erstellen, auf andere Instanzen. Sie sind auf eine Instanz von IAM Identity Center pro AWS-Konto Instanz beschränkt. Um die Anwendung zu aktivieren, wechseln Sie entweder zu der AWS-Region mit der Instanz von IAM Identity Center oder zu einem Konto ohne eine Instanz von IAM Identity Center.
- Wenn Ihre Organisation IAM Identity Center vor dem 14. September 2023 aktiviert hat, muss sich Ihr Administrator möglicherweise für die Erstellung einer Kontoinstanz anmelden. Arbeiten Sie mit Ihrem Administrator zusammen, um die Erstellung von Kontoinstanzen über die IAM Identity Center-Konsole im Verwaltungskonto zu aktivieren.
- Ihr Administrator hat möglicherweise eine Service Control-Richtlinie erstellt, um die Erstellung von Kontoinstanzen von IAM Identity Center einzuschränken. Arbeiten Sie mit Ihrem Administrator zusammen und fügen Sie Ihr Konto zur Zulassungsliste hinzu.

Sie erhalten eine Fehlermeldung, wenn Sie versuchen, die Liste der Cloud-Anwendungen aufzurufen, die für die Verwendung mit IAM Identity Center vorkonfiguriert sind

Der folgende Fehler tritt auf, wenn Sie eine Richtlinie haben, die andere IAM Identity Center-APIs zulässt, `sso:ListApplications` aber nicht. Aktualisieren Sie Ihre Richtlinie, um diesen Fehler zu beheben.

Die `ListApplications` Erlaubnis autorisiert mehrere APIs:

- Die `ListApplications` API.
- Eine interne API, die der in der IAM Identity Center-Konsole verwendeten `ListApplicationProviders` API ähnelt.

Um Duplikate zu vermeiden, autorisiert die interne API jetzt auch die Verwendung der Aktion. `ListApplicationProviders` Um die öffentliche `ListApplications` API zuzulassen, die interne API jedoch abzulehnen, muss Ihre Richtlinie eine Erklärung enthalten, die die Aktion ablehnt: `ListApplicationProviders`

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Um die interne API zuzulassen, aber abzulehnen`ListApplications`, muss die Richtlinie nur `ListApplicationProviders` zulassen. Die `ListApplications` API wird verweigert, wenn sie nicht ausdrücklich erlaubt ist.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

Wenn Ihre Richtlinien aktualisiert werden, wenden Sie sich an uns, AWS Support um diese proaktive Maßnahme entfernen zu lassen.

Probleme mit dem Inhalt von SAML-Assertionen, die von IAM Identity Center erstellt wurden

IAM Identity Center bietet eine webbasierte Debug-Oberfläche für die von IAM Identity Center erstellten und gesendeten SAML-Assertions, einschließlich der Attribute in diesen Assertionen, beim Zugriff auf SAML-Anwendungen über das Zugriffsportal. AWS-Konten AWS Gehen Sie wie folgt vor, um die Details einer von IAM Identity Center generierten SAML-Assertion zu sehen.

1. Melden Sie sich beim Zugangsportal an AWS .
2. Halten Sie die Umschalttaste gedrückt, während Sie im Portal angemeldet sind, wählen Sie die Anwendungskachel aus, und lassen Sie dann die Umschalttaste los.
3. Überprüfen Sie die Informationen auf der Seite mit dem Titel You are now in administrator mode (Sie befinden sich jetzt im Administratormodus). Um diese Informationen zum future Nachschlagen aufzubewahren, wählen Sie „XML kopieren“ und fügen Sie den Inhalt an einer anderen Stelle ein.
4. Wählen Sie Senden an, <application>um fortzufahren. Diese Option sendet die Assertion an den Dienstanbieter.

> **Note**
>
> Einige Browserkonfigurationen und Betriebssysteme unterstützen dieses Verfahren möglicherweise nicht. Dieses Verfahren wurde unter Windows 10 mit den Browsern Firefox, Chrome und Edge getestet.

Bestimmte Benutzer können sich von einem externen SCIM-Anbieter nicht mit dem IAM Identity Center synchronisieren

Wenn die SCIM-Synchronisierung für eine Teilmenge von Benutzern, die in Ihrem IdP für die Bereitstellung im IAM Identity Center konfiguriert sind, erfolgreich ist, für andere jedoch fehlschlägt, wird möglicherweise ein Fehler angezeigt, der dem Ihres Identitätsanbieters ähnelt. `'Request is unparsable, syntactically incorrect, or violates schema'` Möglicherweise finden Sie auch detaillierte Fehlermeldungen bei der Bereitstellung unter. AWS CloudTrail

Dieses Problem weist häufig darauf hin, dass der Benutzer in Ihrem IdP auf eine Weise konfiguriert ist, die IAM Identity Center nicht unterstützt. Vollständige Informationen zur SCIM-Implementierung von IAM Identity Center, einschließlich der Spezifikationen der erforderlichen, optionalen und verbotenen Parameter und Operationen für Benutzerobjekte, finden Sie im IAM Identity Center SCIM Implementation Developer Guide. Der SCIM Developer Guide sollte als maßgebend für Informationen zu den SCIM-Anforderungen angesehen werden. Im Folgenden sind jedoch einige häufige Gründe für diesen Fehler aufgeführt:

1. Dem Benutzerobjekt im IdP fehlt ein Vorname (Vorname), ein Nachname (Familien) und/oder ein Anzeigename.

   - Lösung: Fügen Sie einen Vornamen (angegeben), einen Nachnamen (Familie) und einen Anzeigenamen für das Benutzerobjekt hinzu. Stellen Sie außerdem sicher, dass die SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP so konfiguriert sind, dass sie nicht leere Werte für all diese Attribute senden.

2. Es wird mehr als ein Wert für ein einzelnes Attribut an den Benutzer gesendet (auch als „Attribute mit mehreren Werten“ bezeichnet). Beispielsweise kann der Benutzer sowohl eine geschäftliche als auch eine private Telefonnummer im IdP angegeben haben oder mehrere E-Mails oder physische Adressen, und Ihr IdP ist so konfiguriert, dass er versucht, mehrere oder alle Werte für dieses Attribut zu synchronisieren.

   - Lösungsoptionen:

     i. Aktualisieren Sie Ihre SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP, sodass nur ein einziger Wert für ein bestimmtes Attribut gesendet wird. Konfigurieren Sie beispielsweise eine Zuordnung, die nur die geschäftliche Telefonnummer für jeden Benutzer sendet.

     ii. Wenn die zusätzlichen Attribute sicher aus dem Benutzerobjekt am IdP entfernt werden können, können Sie die zusätzlichen Werte entfernen, sodass entweder ein oder kein Wert für dieses Attribut für den Benutzer festgelegt bleibt.

     iii. Wenn das Attribut für keine Aktionen in benötigt wird AWS, entfernen Sie die Zuordnung für dieses Attribut aus den SCIM-Bereitstellungszuordnungen für Benutzerobjekte bei Ihrem IdP.

3. Ihr IdP versucht, Benutzer im Ziel (in diesem Fall IAM Identity Center) anhand mehrerer Attribute zuzuordnen. Da Benutzernamen innerhalb einer bestimmten IAM Identity Center-Instanz garantiert eindeutig sind, müssen Sie nur das für den `username` Abgleich verwendete Attribut angeben.

- Lösung: Stellen Sie sicher, dass Ihre SCIM-Konfiguration in Ihrem IdP nur ein einziges Attribut für den Abgleich mit Benutzern in IAM Identity Center verwendet. Beispielsweise ist die Zuordnung `username` oder `userPrincipalName` im IdP zum `userName` Attribut in SCIM für die Bereitstellung im IAM Identity Center korrekt und für die meisten Implementierungen ausreichend.

Benutzer können sich nicht anmelden, wenn ihr Benutzername im UPN-Format ist

Benutzer können sich aufgrund des Formats, das sie für die Eingabe ihres Benutzernamens auf der Anmeldeseite verwenden, möglicherweise nicht beim AWS Access-Portal anmelden. In den meisten Fällen können sich Benutzer entweder mit ihrem einfachen Benutzernamen, ihrem untergeordneten Anmeldenamen (DOMAIN\UserName) oder ihrem UPN-Anmeldenamen () beim Benutzerportal anmelden. `UserName@Corp.Example.com` Die Ausnahme ist, wenn IAM Identity Center ein verbundenes Verzeichnis verwendet, das mit MFA aktiviert wurde und der Bestätigungsmodus entweder auf Kontextsensitiv oder Always-on eingestellt wurde. In diesem Szenario müssen sich Benutzer mit ihrem untergeordneten Anmeldenamen (DOMAIN\) anmelden. UserName Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung für Identity Center-Benutzer. Allgemeine Informationen zu Benutzernamenformaten, die für die Anmeldung bei Active Directory verwendet werden, finden Sie unter Benutzernamenformate auf der Microsoft-Dokumentationswebsite.

Beim Ändern einer IAM-Rolle erhalte ich die Fehlermeldung „Der Vorgang kann mit der geschützten Rolle nicht ausgeführt werden“

Bei der Überprüfung der IAM-Rollen in einem Konto fallen Ihnen möglicherweise Rollennamen auf, die mit '_' beginnen. AWSReservedSSO Dies sind die Rollen, die der IAM Identity Center-Dienst für das Konto erstellt hat. Sie stammen aus der Zuweisung eines Berechtigungssatzes für das Konto. Der Versuch, diese Rollen von der IAM-Konsole aus zu ändern, führt zu dem folgenden Fehler:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Diese Rollen können nur über die IAM Identity Center-Administratorkonsole geändert werden, die sich im Verwaltungskonto von befindet. AWS Organizations Nach der Änderung können Sie die Änderungen dann auf die AWS Konten übertragen, denen sie zugewiesen sind.

Verzeichnisbenutzer können ihr Passwort nicht zurücksetzen

Wenn ein Verzeichnisbenutzer sein Passwort mit der Option Passwort vergessen zurücksetzt? Bei der Anmeldung am AWS Zugriffsportal muss das neue Passwort den standardmäßigen Passwortrichtlinien entsprechen, wie unter beschrieben. Passwortanforderungen bei der Verwaltung von Identitäten im IAM Identity Center

Wenn ein Benutzer ein Passwort eingibt, das der Richtlinie entspricht, und dann die Fehlermeldung erhält`We couldn't update your password`, überprüfen Sie, ob der Fehler AWS CloudTrail aufgezeichnet wurde. Suchen Sie dazu in der Konsole „Event History“ nach oder CloudTrail verwenden Sie den folgenden Filter:

```
"UpdatePassword"
```

Wenn in der Nachricht Folgendes steht, müssen Sie sich möglicherweise an den Support wenden:

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Eine weitere mögliche Ursache für dieses Problem liegt in der Benennungskonvention, die auf den Benutzernamenwert angewendet wurde. Benennungskonventionen müssen bestimmten Mustern wie „Surname.GivenName“ folgen. Einige Benutzernamen können jedoch sehr lang sein oder Sonderzeichen enthalten, was dazu führen kann, dass Zeichen im API-Aufruf weggelassen werden, was zu einem Fehler führen kann. Möglicherweise möchten Sie auf dieselbe Weise versuchen, das Passwort mit einem Testbenutzer zurückzusetzen, um zu überprüfen, ob dies der Fall ist.

Wenn das Problem weiterhin besteht, wenden Sie sich an das AWS Support Center.

Mein Benutzer wird in einem Berechtigungssatz referenziert, kann aber nicht auf die zugewiesenen Konten oder Anwendungen zugreifen

Dieses Problem kann auftreten, wenn Sie das System for Cross-Domain Identity Management (SCIM) für die automatische Bereitstellung mit einem externen Identitätsanbieter verwenden. Insbesondere wenn ein Benutzer oder die Gruppe, der der Benutzer angehörte, gelöscht und dann mit demselben Benutzernamen (für Benutzer) oder Namen (für Gruppen) im Identitätsanbieter neu

erstellt wird, wird eine neue eindeutige interne Kennung für den neuen Benutzer oder die neue Gruppe in IAM Identity Center erstellt. IAM Identity Center hat jedoch immer noch einen Verweis auf die alte ID in seiner Berechtigungsdatenbank, sodass der Name des Benutzers oder der Gruppe immer noch in der Benutzeroberfläche angezeigt wird, der Zugriff jedoch fehlschlägt. Das liegt daran, dass die zugrunde liegende Benutzer- oder Gruppen-ID, auf die sich die Benutzeroberfläche bezieht, nicht mehr existiert.

Um den AWS-Konto Zugriff in diesem Fall wiederherzustellen, können Sie den Zugriff für den alten Benutzer oder die alte Gruppe aus AWS-Konto denjenigen entfernen, denen er ursprünglich zugewiesen wurde, und dann den Zugriff wieder dem Benutzer oder der Gruppe zuweisen. Dadurch wird der Berechtigungssatz mit der richtigen ID für den neuen Benutzer oder die neue Gruppe aktualisiert. Um den Anwendungszugriff wiederherzustellen, können Sie auf ähnliche Weise den Zugriff für den Benutzer oder die Gruppe aus der Liste der zugewiesenen Benutzer für diese Anwendung entfernen und den Benutzer oder die Gruppe dann wieder hinzufügen.

Sie können auch überprüfen, ob der Fehler AWS CloudTrail aufgezeichnet wurde, indem Sie Ihre CloudTrail Protokolle nach SCIM-Synchronisierungsereignissen durchsuchen, die auf den Namen des betreffenden Benutzers oder der betreffenden Gruppe verweisen.

Ich kann meine Anwendung nicht korrekt aus dem Anwendungskatalog konfigurieren

Wenn Sie eine Anwendung aus dem Anwendungskatalog in IAM Identity Center hinzugefügt haben, beachten Sie, dass jeder Dienstanbieter seine eigene ausführliche Dokumentation bereitstellt. Sie können auf diese Informationen über die Registerkarte Konfiguration für die Anwendung in der IAM Identity Center-Konsole zugreifen.

Wenn das Problem mit der Einrichtung der Vertrauensstellung zwischen der Anwendung des Dienstanbieters und IAM Identity Center zusammenhängt, sollten Sie die Anweisungen zur Fehlerbehebung in der Bedienungsanleitung nachlesen.

Fehler „Ein unerwarteter Fehler ist aufgetreten“, wenn ein Benutzer versucht, sich mit einem externen Identitätsanbieter anzumelden

Dieser Fehler kann aus mehreren Gründen auftreten, ein häufiger Grund ist jedoch eine Nichtübereinstimmung zwischen den in der SAML-Anfrage enthaltenen Benutzerinformationen und den Informationen für den Benutzer in IAM Identity Center.

Damit sich ein IAM Identity Center-Benutzer erfolgreich anmelden kann, wenn er einen externen IdP als Identitätsquelle verwendet, muss Folgendes zutreffen:

- Das SAML-NameID-Format (bei Ihrem Identitätsanbieter konfiguriert) muss „E-Mail“ lauten
- Der NameID-Wert muss eine ordnungsgemäß (RFC2822) formatierte Zeichenfolge sein (user@domain.com)
- Der NameID-Wert muss exakt mit dem Benutzernamen eines vorhandenen Benutzers in IAM Identity Center übereinstimmen (es spielt keine Rolle, ob die E-Mail-Adresse in IAM Identity Center übereinstimmt oder nicht — der eingehende Abgleich basiert auf dem Benutzernamen)
- Die IAM Identity Center-Implementierung des SAML 2.0-Verbunds unterstützt nur eine Assertion in der SAML-Antwort zwischen dem Identitätsanbieter und IAM Identity Center. Verschlüsselte SAML-Assertionen werden nicht unterstützt.
- Die folgenden Aussagen gelten, wenn die Option in Ihrem IAM Identity Center-Konto aktiviert Attribute für Zugriffskontrolle ist:
  - Die Anzahl der in der SAML-Anfrage zugewiesenen Attribute muss 50 oder weniger betragen.
  - Die SAML-Anfrage darf keine mehrwertigen Attribute enthalten.
  - Die SAML-Anfrage darf nicht mehrere Attribute mit demselben Namen enthalten.
  - Das Attribut darf kein strukturiertes XML als Wert enthalten.
  - Das Namensformat muss ein in SAML spezifiziertes Format sein, kein generisches Format.

> **Note**
>
> IAM Identity Center führt keine Just-in-Time-Erstellung von Benutzern oder Gruppen für neue Benutzer oder Gruppen über einen SAML-Verbund durch. Das bedeutet, dass der Benutzer entweder manuell oder über automatische Bereitstellung vorab in IAM Identity Center erstellt werden muss, um sich bei IAM Identity Center anmelden zu können.

Dieser Fehler kann auch auftreten, wenn der in Ihrem Identitätsanbieter konfigurierte Assertion Consumer Service (ACS) -Endpunkt nicht mit der von Ihrer IAM Identity Center-Instanz bereitgestellten ACS-URL übereinstimmt. Stellen Sie sicher, dass diese beiden Werte exakt übereinstimmen.

Darüber hinaus können Sie Anmeldefehler bei externen Identitätsanbietern weiter beheben, indem Sie zum Ereignisnamen ExternalIdP DirectoryLogin wechseln AWS CloudTrail und nach diesem filtern.

Fehler „Die Attribute für die Zugriffskontrolle konnten nicht aktiviert werden“

Dieser Fehler kann auftreten, wenn der Benutzer, der ABAC aktiviert, nicht über die für die Aktivierung `iam:UpdateAssumeRolePolicy` erforderlichen Berechtigungen verfügt. Attribute für Zugriffskontrolle

Ich erhalte die Meldung „Browser wird nicht unterstützt“, wenn ich versuche, ein Gerät für MFA zu registrieren

WebAuthn wird derzeit in den Webbrowsern Google Chrome, Mozilla Firefox, Microsoft Edge und Apple Safari sowie in Windows 10- und Android-Plattformen unterstützt. Einige Komponenten der WebAuthn Unterstützung können unterschiedlich sein, z. B. die Unterstützung von Plattformauthentifikatoren in macOS- und iOS-Browsern. Wenn Benutzer versuchen, WebAuthn Geräte in einem Browser oder einer Plattform zu registrieren, die nicht unterstützt werden, werden bestimmte Optionen ausgegraut angezeigt, die nicht unterstützt werden, oder sie erhalten eine Fehlermeldung, dass nicht alle unterstützten Methoden unterstützt werden. In diesen Fällen finden Sie weitere Informationen zur Browser-/Plattformunterstützung unter FIDO2: Web Authentication (WebAuthn). Weitere Informationen zu WebAuthn in IAM Identity Center finden Sie unter. FIDO2-Authentifikatoren

Die Active Directory-Gruppe „Domänenbenutzer“ wird nicht ordnungsgemäß mit dem IAM Identity Center synchronisiert

Die Active Directory-Domänenbenutzergruppe ist die standardmäßige „primäre Gruppe“ für AD-Benutzerobjekte. Primäre Active Directory-Gruppen und ihre Mitgliedschaften können vom IAM Identity Center nicht gelesen werden. Verwenden Sie bei der Zuweisung von Zugriff auf IAM Identity Center-Ressourcen oder -Anwendungen andere Gruppen als die Gruppe Domänenbenutzer (oder andere Gruppen, die als primäre Gruppen zugewiesen wurden), damit die Gruppenmitgliedschaft im IAM Identity Center-Identitätsspeicher korrekt wiedergegeben wird.

Fehler mit ungültigen MFA-Anmeldeinformationen

Dieser Fehler kann auftreten, wenn ein Benutzer versucht, sich mit einem Konto eines externen Identitätsanbieters (z. B. Okta oderMicrosoft Entra ID) bei IAM Identity Center anzumelden, bevor sein Konto mithilfe des SCIM-Protokolls vollständig für IAM Identity Center bereitgestellt wurde. Nachdem das Benutzerkonto für IAM Identity Center bereitgestellt wurde, sollte dieses Problem behoben sein. Vergewissern Sie sich, dass das Konto für IAM Identity Center bereitgestellt wurde. Falls nicht, überprüfen Sie die Bereitstellungsprotokolle des externen Identitätsanbieters.

Ich erhalte die Meldung „Ein unerwarteter Fehler ist aufgetreten“, wenn ich versuche, mich mit einer Authenticator-App zu registrieren oder anzumelden

Zeitbasierte Einmalkennwortsysteme (TOTP), wie sie beispielsweise von IAM Identity Center in Kombination mit codebasierten Authentifikator-Apps verwendet werden, basieren auf der Zeitsynchronisierung zwischen dem Client und dem Server. Stellen Sie sicher, dass das Gerät, auf dem Ihre Authenticator-App installiert ist, korrekt mit einer zuverlässigen Zeitquelle synchronisiert ist, oder stellen Sie die Uhrzeit auf Ihrem Gerät manuell so ein, dass sie mit einer zuverlässigen Quelle wie NIST (https://www.time.gov/) oder anderen lokalen/regionalen Entsprechungen übereinstimmt.

Ich erhalte die Fehlermeldung „Nicht du, es sind wir“, wenn ich versuche, mich im IAM Identity Center anzumelden

Dieser Fehler weist auf ein Einrichtungsproblem mit Ihrer Instanz von IAM Identity Center oder dem externen Identitätsanbieter (IdP) hin, den IAM Identity Center als Identitätsquelle verwendet. Wir empfehlen Ihnen, Folgendes zu überprüfen:

- Überprüfen Sie die Datums- und Uhrzeiteinstellungen auf dem Gerät, mit dem Sie sich anmelden. Wir empfehlen Ihnen, Datum und Uhrzeit so einzustellen, dass sie automatisch eingestellt werden. Wenn dies nicht verfügbar ist, empfehlen wir, Datum und Uhrzeit mit einem bekannten NTP-Server (Network Time Protocol) zu synchronisieren.
- Stellen Sie sicher, dass das in IAM Identity Center hochgeladene IdP-Zertifikat mit dem von Ihrem IdP bereitgestellten Zertifikat übereinstimmt. Sie können das Zertifikat von der IAM Identity Center-Konsole aus überprüfen, indem Sie zu Einstellungen navigieren. Wählen Sie auf der Registerkarte

Identitätsquelle Aktion und dann Authentifizierung verwalten aus. Wenn die IdP- und IAM Identity Center-Zertifikate nicht übereinstimmen, importieren Sie ein neues Zertifikat in IAM Identity Center.

- Stellen Sie sicher, dass das NameID-Format in der Metadatendatei Ihres Identity Providers wie folgt lautet:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Wenn Sie AD Connector von AWS Directory Service als Identitätsanbieter verwenden, stellen Sie sicher, dass die Anmeldeinformationen für das Dienstkonto korrekt und nicht abgelaufen sind. Weitere Informationen finden Sie unter Aktualisieren der Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos in AWS Directory Service.

Meine Benutzer erhalten keine E-Mails von IAM Identity Center

Alle vom IAM Identity Center-Dienst gesendeten E-Mails stammen entweder von der Adresse `no-reply@signin.aws` oder. `no-reply@login.awsapps.com` Ihr E-Mail-System muss so konfiguriert sein, dass es E-Mails von diesen Absender-E-Mail-Adressen akzeptiert und sie nicht als Junk oder Spam behandelt.

Fehler: Sie können die im Verwaltungskonto bereitgestellten Berechtigungssätze nicht löschen/ändern/entfernen/ihnen keinen Zugriff zuweisen

Diese Meldung weist darauf hin, dass die Delegierte Verwaltung Funktion aktiviert wurde und dass der Vorgang, den Sie zuvor versucht haben, nur von jemandem erfolgreich ausgeführt werden kann, der über Verwaltungskontoberechtigungen für verfügt. AWS Organizations Um dieses Problem zu beheben, melden Sie sich als Benutzer an, der über diese Berechtigungen verfügt, und versuchen Sie erneut, die Aufgabe auszuführen, oder weisen Sie diese Aufgabe einer Person zu, die über die richtigen Berechtigungen verfügt. Weitere Informationen finden Sie unter Registrieren Sie ein Mitgliedskonto.

Fehler: Das Sitzungstoken wurde nicht gefunden oder ist ungültig

Dieser Fehler kann auftreten, wenn ein Client, z. B. ein Webbrowser AWS Toolkit, versucht AWS CLI, eine Sitzung zu verwenden, die serverseitig gesperrt oder ungültig gemacht wurde. Um dieses Problem zu beheben, kehren Sie zur Client-Anwendung oder Website zurück und versuchen Sie es

erneut. Melden Sie sich auch erneut an, wenn Sie dazu aufgefordert werden. Dies kann manchmal erforderlich sein, dass Sie auch ausstehende Anfragen stornieren müssen, z. B. einen ausstehenden Verbindungsversuch AWS Toolkit von Ihrer IDE aus.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Ergänzungen der AWS IAM Identity Center Dokumentation beschrieben. Wir aktualisieren die Dokumentation regelmäßig, um das Feedback, das Sie uns senden, einzuarbeiten.

- Letzte wichtige Aktualisierung der Dokumentation: 23. September 2022

Änderung	Beschreibung	Datum
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	17. Mai 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	30. April 2024
Updates für die AWS verwaltete Richtlinie	Die Berechtigungen für die `AWSSSOMasterAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSSSOMemberAccountAdministrator` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024

Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSSSOReadOnly` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	26. April 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	24. April 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	19. April 2024
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	11. April 2024

Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie wurden aktualisiert.	26. November 2023
Neues Thema für AWS verwaltete Richtlinien	Es wurden Details für die `AWSIAMIdentityCenterAllowListForIdentityContext` AWS verwaltete Richtlinie hinzugefügt.	15. November 2023
Verbesserte Anleitung für die ersten Schritte mit IAM Identity Center	Es wurden neue Inhalte für die ersten Schritte mit IAM Identity Center und die Erstellung eines Administratorbenutzers hinzugefügt	23. September 2022
Benutzer und Gruppen in der Identity Center API-Referenz wurden aktualisiert	Dieses Update enthält Verweise auf die neuen APIs zum Erstellen, Aktualisieren und Löschen von APIs im Identity Center API-Referenzhandbuch.	31. August 2022

AWS Single Sign-On (AWS SSO) wurde in AWS IAM Identity Center umbenannt	AWS führt ein. AWS IAM Identity Center IAM Identity Center erweitert die Funktionen von AWS Identity and Access Management (IAM), sodass Sie die Konten und den Zugriff auf Anwendungen für die Benutzer Ihrer Belegschaft zentral verwalten können. Zu den Funktionen von IAM Identity Center gehören Anwendungszuweisungen, Berechtigungen für mehrere Konten und ein Zugriffsportal. AWS	26. Juli 2022
Support für Berechtigungsgrenzen und vom Kunden verwaltete Richtlinien in Berechtigungssätzen	Es wurden Inhalte für die Verwendung von AWS verwalteten und vom Kunden verwalteten AWS Identity and Access Management (IAM) Richtlinien mit Berechtigungssätzen hinzugefügt.	14. Juli 2022
Support für manuell aktivierte AWS Regionen	Es wurden Inhalte für die Verwendung von IAM Identity Center in manuell aktivierten Regionen hinzugefügt.	15. Juni 2022
Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSSSOServiceRolePolicy` AWS verwaltete Richtlinie wurden aktualisiert.	11. Mai 2022
Support für delegierte Administration	Inhalt für die Funktion zur delegierten Verwaltung hinzugefügt.	11. Mai 2022

Updates für AWS verwaltete Richtlinien	Die Berechtigungen für die `AWSSSOMasterAccountAdministrator` `AWSSSOMemberAccountAdministrator` , und `AWSSSOReadOnly` AWS verwalteten Richtlinien wurden aktualisiert.	28. April 2022
Support für konfigurierbare AD-Synchronisierung	Inhalt für die konfigurierbare AD-Synchronisierungsfunktion hinzugefügt.	14. April 2022
Neues Thema für AWS verwaltete Richtlinien	Es wurden Details für die `AWSSSOMasterAccountAdministrator` AWS verwaltete Richtlinie hinzugefügt.	4. August 2021
Aktualisierungen für Kontingente	Anpassungen der Quotentabellen.	21. Dezember 2020
Neue Beispielrichtlinien	Dem Abschnitt „Erforderliche Berechtigungen“ wurden neue Beispiele für vom Kunden verwaltete Richtlinien und Aktualisierungen hinzugefügt.	21. Dezember 2020
Support für attributebasierte Zugriffskontrolle (ABAC)	Inhalt für die ABAC-Funktion hinzugefügt.	24. November 2020
Support für die erzwungene MFA-Registrierung	Updates, sodass Benutzer bei der Anmeldung ein MFA-Gerät registrieren müssen.	23. November 2020
Support für WebAuthn	Inhalt für neue WebAuthn Funktion hinzugefügt.	20. November 2020

Support für Ping Identity	Als unterstützter externer Identitätsanbieter wurden Inhalte zur Integration in Ping Identity Produkte hinzugefügt.	26. Oktober 2020
Support für OneLogin	Inhalt zur Integration OneLogin als unterstützter externer Identitätsanbieter hinzugefügt.	31. Juli 2020
Unterstützung fü Okta	Inhalt zur Integration Okta als unterstützter externer Identität sanbieter hinzugefügt.	28. Mai 2020
Support für externe Identität sanbieter	Die Verweise vom Verzeichn is zur Identitätsquelle wurden geändert und Inhalte zur Unterstützung externer Identitätsanbieter hinzugefügt.	26. November 2019
Neue MFA-Einstellungen	Das Thema zur Bestätigung in zwei Schritten wurde entfernt und stattdessen ein neues MFA-Thema hinzugefügt.	24. Oktober 2019
Neue Einstellung zum Hinzufügen der Bestätigung in zwei Schritten	Es wurden Inhalte zur Aktivierung der Bestätigung in zwei Schritten für Benutzer hinzugefügt.	16. Januar 2019
Support für die Sitzungsdauer auf AWS Konten	Es wurden Inhalte zur Festlegung der Sitzungsdauer für ein AWS Konto hinzugefü gt.	30. Oktober 2018

Neue Option zur Verwendung des Identity Center-Verzeichnisses	Es wurden Inhalte hinzugefügt, mit denen Sie entweder das Identity Center-Verzeichnis auswählen oder eine Verbindung zu einem vorhandenen Verzeichnis in Active Directory herstellen können.	17. Oktober 2018
Support für Relay-Status und Sitzungsdauer bei Anwendungen	Es wurden Inhalte zum Relay-Status und zur Sitzungsdauer für Anwendungen hinzugefügt.	10. Oktober 2018
Zusätzliche Unterstützung für neue Anwendungen	Hinzugefügt 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, und UserEcho zum Anwendungskatalog hinzugefügt.	3. August 2018
Support für den Zugriff mehrerer Konten auf Verwaltungskonten	Es wurden Inhalte zur Delegierung des Zugriffs mit mehreren Konten an Benutzer in einem Verwaltungskonto hinzugefügt.	9. Juli 2018

Support für neue Anwendungen	Hinzugefügt DocuSign, Keeper Security, und SugarCRM zum Anwendungskatalog hinzugefügt.	16. März 2018
Holen Sie sich temporäre Anmeldeinformationen für den CLI-Zugriff	Es wurden Informationen zum Abrufen temporärer Anmeldeinformationen für die Ausführung von AWS CLI Befehlen hinzugefügt.	22. Februar 2018
Neues Handbuch	Dies ist die erste Version des IAM Identity Center-Benutzerhandbuchs.	7. Dezember 2017

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.